



MARIN COUNTY | NAPA COUNTY | UNINCORPORATED CONTRA COSTA COUNTY | UNINCORPORATED SOLANO COUNTY  
BENICIA | CONCORD | DANVILLE | EL CERRITO | FAIRFIELD | LAFAYETTE | MARTINEZ | MORAGA | OAKLEY  
PINOLE | PITTSBURG | PLEASANT HILL | RICHMOND | SAN PABLO | SAN RAMON | VALLEJO | WALNUT CREEK

Technical Committee Meeting  
Friday, June 2, 2023  
10:00 A.M.

Charles F. McGlashan Board Room, 1125 Tamalpais Avenue, San Rafael, CA 94901  
Mt. Diablo Room, 2300 Clayton Road, Suite 1150, Concord, CA 94920

Members of the public who wish to observe the meeting and/or offer public comment may do so telephonically via the following teleconference call-in number and meeting ID:

For Viewing Access Join Zoom Meeting:

<https://us02web.zoom.us/j/89373348901?pwd=bDlpYkg0bzJQWkRvS205UHNwejlOdz09>

Dial: 1-669-900-9128  
Webinar ID: 893 7334 8901  
Passcode: 193748

Agenda Page 1 of 2

1. Roll Call/Quorum
2. Board Announcements (Discussion)
3. Public Open Time (Discussion)
4. Report from Chief Executive Officer (Discussion)
5. Consent Calendar (Discussion/Action)
  - C.1 Approval of 2.2.23 Meeting Minutes
6. National Energy Infrastructure Fund Offer for Virtual Power Plant Pilot Participants (Discussion/Action)
7. Peak FLEX Update (Discussion)

8. Committee Matters & Staff Matters (Discussion)
9. Adjourn

*The Technical Committee may discuss and/or take action on any or all of the items listed on the agenda irrespective of how the items are described.*

*This Committee may be attended by Board Members who do not serve on this Committee. In the event that a quorum of the entire Board is present, this Committee shall act as a Committee of the Whole. Any item acted upon by the Committee of the Whole will be considered advisory to the Board of Directors and require consideration and action by the Board of Directors at a noticed Board meeting before adoption or approval of the item.*

DISABLED ACCOMMODATION: If you are a person with a disability which requires an accommodation or an alternative format, please call MCE at 1 (888) 632-3674 at least 72 hours before the meeting start time to ensure arrangements for accommodation.

**DRAFT****MCE TECHNICAL COMMITTEE MEETING MINUTES**

Thursday, February 2, 2023

8:30 A.M.

The Technical Committee Meeting was conducted pursuant to the requirements of Assembly Bill No. 361 (September 16, 2021) which allows a public agency to use teleconferencing during a Governor-proclaimed state of emergency without meeting usual Ralph M. Brown Act teleconference requirements. Committee Members, staff and members of the public were able to participate in the Committee Meeting via teleconference.

---

**Present:** Gina Dawson, City of Lafayette  
 Kevin Haroff, City of Larkspur  
 Devin Murphy, City of Pinole  
 Scott Perkins, City of San Ramon  
 Katie Rice, County of Marin

**Absent:** John Gioia, Contra Costa County

**Staff  
& Others:** Jessica Brooks, Board Clerk  
 Darlene Jackson, Lead Board Clerk  
 Vicken Kasarjian, Chief Operating Officer  
 Paul Krebs, Power Procurement Manager  
 Justin Kudo, Senior Strategic Analysis and Rates Manager  
 Catalina Murphy, Associate General Counsel  
 Daniel Settlemyer, Internal Operations Coordinator  
 Jamie Tuckey, Chief of Staff  
 Dawn Weisz, Chief Executive Officer

1. **Roll Call**

Chair Murphy called the regular Technical Committee meeting to order at 8:30 a.m. with quorum established by roll call.

2. **Board Announcements (Discussion)**

There were no announcements.

3. **Public Open Time (Discussion)**

Chair Murphy opened the public comment period and there were comments from member of the public, Howdy Goudey.

4. **Resolution No. 2023-01 Authorizing Remote Teleconferencing Meetings for the Technical Committee Pursuant to Government Code Section 54953(e) (Discussion/Action)**

Catalina Murphy, Associate General Counsel, presented this item and addressed questions from Committee members.

**DRAFT**

Chair Murphy opened the public comment period and there were no comments.

Action: It was M/S/C (Perkins/Dawson) to **adopt proposed Resolution No. 2023-01 Authorizing Remote Teleconference Meetings for the Technical Committee Pursuant to Government Code Section 54953(e).**

Motion carried by unanimous roll call vote. (Absent: Director Gioia).

**5. Report from Chief Executive Officer (Discussion)**

Dawn Weisz, CEO, introduced this item and addressed questions from Board members.

Chair Murphy opened the public comment period and there were no comments.

**6. Consent Calendar (Discussion/Action)**

C.1 Approval of 11.3.22 Meeting Minutes

Chair Murphy opened the public comment period and there were no comments.

Action: It was M/S/C (Perkins/Dawson) to **approve Consent Calendar C.1.**

Motion carried by unanimous roll call vote. (Absent: Director Gioia).

**7. Renewable Power Purchase Agreement with Wind Power Partners 1993, LLC. (Discussion/Action)**

Paul Krebs, Power Procurement Manager, presented this item and addressed questions from Committee members.

Chair Murphy opened the public comment period and there were comments from member of the public, Daniel Segedin.

Action: It was M/S/C (Rice/Perkins) to **authorize execution of the Renewable Power Purchase Agreement with Wind Power Partners 1993, LLC.** Motion carried by unanimous roll call vote. (Absent: Gioia).

**8. Adjustments to MCE Net Surplus Compensation (Discussion/Action)**

Justin Kudo, Senior Strategic Analysis and Rates Manager, presented this item and addressed questions from Committee members.

Chair Murphy opened the public comment period and there were comments from member of the public Howdy Goudey.

**DRAFT**

Action: It was M/S/C (Dawson/Haroff) to **adopt the amended MCE Net Energy Metering Tariff provided in the Attachment.** Motion carried by unanimous roll call vote. (Absent: Gioia).

**9. Committee Matters & Staff Matters (Discussion)**

There were comments made by Directors Perkins and Dawson.

**10. Adjournment**

Chair Murphy adjourned the meeting at 9:35 a.m. to the next scheduled Technical Committee Meeting on March 2, 2023.

---

Devin Murphy, Chair

Attest:

---

Dawn Weisz, Secretary



June 2, 2023

TO: MCE Technical Committee

FROM: Garth Salisbury, Chief Financial Officer & Treasurer  
Alexandra McGee, Director of Strategic Initiatives

RE: National Energy Infrastructure Fund Offer for Virtual Power  
Plant Pilot Participants (Agenda Item #06)

ATTACHMENTS: A. Loan Origination and Servicing Agreement by and between  
NEIF and MCE  
B. First Amendment to Loan Origination and Servicing  
Agreement by and between NEIF and MCE

Dear Technical Committee Members:

**Summary:**

In April 2021, the Technical Committee unanimously approved staff to work with the National Energy Infrastructure Fund (NEIF), a certified B-Corp, non-bank financial institution, to offer loans with a mix of market and below-market interest rates to residential customers to finance home battery energy storage systems. MCE allocated \$4M in reserves for the loans with the understanding that higher-income participants with higher-interest loans would offset the loan losses and fees and cover any subsidies to lower-income customers, thereby making the loans self-sustaining and allowing staff to use it as a revolving loan fund.

In May 2021, the Technical Committee authorized staff to execute the Loan Origination and Servicing Agreement and Exhibits which designated NEIF as the lender. As approved, staff was directed to offer three categories of loans.

1. Lower-income customers qualify for a 10 year, 0% interest loan;
2. Customers on medical baseline or who live in high-fire threat districts qualify for a 10-year, 2.5% interest loan;
3. All other eligible customers qualify for a 5-year, 5.5% interest loan.

Since this authorization, the market has shifted significantly. These interest rates are now extremely affordable compared to other financing options available to residential

customers. MCE will adjust the interest rates as necessary to offer competitive, market-based interest rate offerings to higher-income borrowers.

MCE staff set up a system where \$400,000 is held by NEIF at any given time, with the ability to replenish funds when needed. MCE's installation partners are trained to apply for loan funds via a Developer Portal to upload the necessary customer documents before loan funds are dispersed.

**Proposed Transition of NEIF Loan Program to MCE Virtual Power Plant:** At the September 2022 Technical Committee meeting, staff presented on the development of MCE's Richmond Virtual Power Plant (VPP) pilot project. Staff underscored the importance of this pilot in demonstrating the unique value that MCE can harness and share with our VPP customers. While currently limited to the City of Richmond, this pilot is building the infrastructure necessary for scaling to all MCE member counties and cities, if successful.

Many of the necessary aspects of the VPP program have been developed, so as residential customers are now being engaged and enrolled in the pilot VPP, staff proposes using NEIF financing to ensure that the pilot is sensitive to and supports the financial limitations of eligible customers. However, since it is an explicit priority of this pilot to benefit lower-income customers, staff anticipates there to be more participants who qualify for the lower interest tiers. Without an equivalent number of higher-interest participants, it is anticipated that over time the fund will not be self-sustaining as originally approved.

Staff anticipates that higher interest rate loans will eventually be offered to higher-income customers when the VPP project scales up, but the timeline for the stabilization of this fund is pending.

**Fiscal Impacts:**

NEIF's origination and servicing fees would continue to be paid out of the previously approved \$4M revolving loan fund. Adjustments to the loan program to facilitate primarily low-income borrowers may deplete the fund over time, unless a larger percentage of the loans are originated with customers who qualify for higher-interest loans.

**Recommendation:**

Authorize staff to execute an amendment and/or other necessary documents to the Loan Origination and Servicing Agreement to facilitate offering NEIF financing to pilot VPP participants to support lower-income customers' access to battery storage resources.

## LOAN ORIGINATION AND SERVICING AGREEMENT

### Energy Storage Loans

**THIS LOAN ORIGINATION AND SERVICING AGREEMENT** (the “Agreement”) is made and entered into as of this 6th day of May, 2021, by and between NATIONAL ENERGY IMPROVEMENT FUND, LLC, a Pennsylvania limited liability benefit company, with its principal office located at 1005 Brookside Road, Suite 200, Allentown, PA, 18106 (“**NEIF**”), and Marin Clean Energy, a California joint powers authority located at 1125 Tamalpais Avenue, San Rafael CA, 94901, (“**BUYER**”).

WHEREAS, NEIF desires to originate and service certain Energy Storage Loans for Buyer, as defined below, subject to the terms and conditions of this Agreement; and

WHEREAS, BUYER desires to engage NEIF to originate, service and administer the Energy Storage Loans on behalf of BUYER, and NEIF desires to originate, service and administer such Energy Storage Loans on behalf of BUYER, each upon the terms and subject to the conditions of this Agreement; and

WHEREAS, NEIF, by virtue of its substantial experience and expertise in energy lending has developed and has as part of NEIF’s corporate assets substantially all the information, processes, and systems necessary to successfully fulfill its responsibilities outlined under this Agreement.

NOW, THEREFORE, in consideration of these premises, and of the mutual agreements contained herein and other good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, BUYER and NEIF hereby agree as follows:

### ARTICLE I DEFINITIONS

**Section 1.01 Definitions.** The following terms shall have the following meanings for all purposes of this Agreement.

“*Account*” means an account owned by NEIF with funds held in trust solely for the benefit of BUYER and Obligors for the purposes of this Agreement.

“*Agreement*” means this Loan Origination and Servicing Agreement entered into by and between BUYER and NEIF, and all exhibits, amendments and supplements hereto.

“*Blanket Assignment*” means upon Loan funding, the Loan is immediately purchased and assigned to Buyer under terms of this agreement without recourse to NEIF.



*“Business Day”* means any day of the week other than Saturday, Sunday or a day which is a legal holiday in the state in which the principal office of BUYER or NEIF is located, or a day on which national banking institutions are authorized or obligated by Law, executive order or government decree to be closed.

*“Code”* means the Internal Revenue Code of 1986, as it may be amended from time to time, and any successor statutes thereto.

*“Confidential Information”* means any proprietary, confidential or non-public information in any form obtained by either NEIF or BUYER, including without limitation, identifiable non-public information regarding any Obligor under any Loan, or any guarantor or surety thereof or any grantor of any mortgage or other security thereunder. Confidential Information shall not include information that is: (i) in or becomes part of the public domain other than by disclosure by a party in violation of this Agreement; (ii) demonstrably known to a party previously, without a duty of confidentiality; (iii) independently developed by a party outside of this Agreement; (iv) rightfully obtained by a party from third parties without a duty of confidentiality; or (v) required to be publicly disclosed by Law.

*“Due Date”* means, with respect to each Loan, the date in each month on which payments of principal and interest are due.

*“Due Period”* means the period between and including the first day of each month and the last calendar day of the calendar month for which payments of principal and interest are due on a given Due Date.

*“Fee Schedule”* means Exhibit 2 attached hereto.

*“File”* means the documents related to a Loan maintained in the possession of BUYER or NEIF.

*“Independent Contractor”* means any Person that would be an "independent contractor" with respect to BUYER within the meaning of Section 856(d)(3) of the Code or such other Person as may be approved by BUYER.

*“Law”* means all applicable statutes, laws, ordinances, regulations, orders, writs, injunctions or decrees of the United States or any agency thereof, or any state or political subdivision thereof, or any court of competent jurisdiction thereof.

*“Loan”* means any loan:

- (a) made by NEIF in compliance with Law;
- (b) complying with the Loan Criteria and any other additional or different terms or program guidelines as BUYER may establish from time to time upon notice to NEIF, including but not limited to those pertaining to Energy Efficiency and Energy Storage Loans; and

(c) purchased by and assigned to BUYER pursuant to Blanket Assignment.

*“Loan Amount”* means the principal amount of the originated Loan.

*“Loan Criteria”* means the eligibility and underwriting requirements established by BUYER from time to time applicable to the Energy Storage Loans, the initial requirements of which are attached hereto as Exhibit 1.

*“Loan Documents”* means: The original of each document evidencing or entered into in connection with a Loan, properly executed and dated as required by Obligor(s), including without limitation (a) all notes, loan agreements, security agreements, guarantees, and any other document evidencing or entered into in connection with a Loan; (b) the original credit application completed and signed by the Obligor(s); (c) all documentation submitted by the Obligor(s) in connection with the credit application; and (d) all notices or disclosure forms required by Law.

*“Monthly Cut-Off Date”* means the last calendar day of any calendar month.

*“Monthly Payment”* means, with respect to any Loan and any Due Period, the payment of principal and interest due in such Due Period from the Obligor.

*“Nonpublic Personal Information”* means any information that would otherwise be considered Confidential Information and that is or relates to personally-identifiable financial information provided by individual consumers or customers of either party or their affiliates and any list, description or other grouping of consumers or customers that is derived using any such information. To the extent permitted by Law, any Nonpublic Personal Information shall remain confidential in all circumstances.

*“Notice Address”* means, unless each party is notified otherwise:

if to BUYER:

Dawn Weisz  
1125 Tamalpais Avenue  
San Rafael, CA 94901  
Email: dweisz@mceCleanEnergy.org  
cc: contracts@mceCleanEnergy.org

if to NEIF:

Matthew H. Brown  
National Energy Improvement Fund, LLC  
1005 Brookside Road, Suite 200  
Allentown, Pennsylvania 18106  
Email: mbrown@neifund.org

*“Obligor”* means a Person who is indebted under a Loan, as maker or co-maker of any note.

*“Payments”* means all moneys received by NEIF representing principal, interest and other amounts received on a Loan, including, without limitation, Principal Prepayments, amounts

received as a result of collection or collateral liquidation, and any proceeds from condemnation awards with respect to the Property.

*“Person”* means an individual, corporation, limited liability company, partnership, association, joint-stock company, trust, unincorporated organization or joint venture; or a government or any agency or political subdivision thereof; or other legal entity.

*“Principal Prepayment”* means any Obligor payment or other receipt of principal on a Loan paid in addition to a Monthly Payment that is received in advance of the scheduled maturity date of such Loan.

*“Program Setup Services”* means services set forth in Exhibit 8 provided by NEIF related to the design and set-up of the various financing mechanisms that Buyer will use to support financing elements of Buyer’s residential and commercial energy storage programs.

*“Property”* means any real property to be improved with Loan proceeds.

*“Servicing Record”* means the books and records established pursuant to Section 5.06 to record all Payments received in respect of any Loan, among other things.

*“Energy Storage loans”* means any Loan:

- (a) made by NEIF in compliance with Law;
- (b) complying with specified Energy Efficiency or Energy Storage Loans terms or any other additional or different terms as BUYER may establish from time to time upon notice to NEIF; and
- (d) purchased by and assigned to BUYER pursuant to Blanket Assignment.

**Section 1.02. Interpretation.** Unless the context requires otherwise, words of the masculine gender shall be construed to include correlative words of the feminine and neuter genders and vice versa, and words of the singular number shall be construed to include correlative words of the plural number and vice versa. The terms of this Agreement shall be liberally construed to effect the purposes set forth herein and to sustain the validity of this Agreement.

## **ARTICLE II REPRESENTATIONS, WARRANTIES AND COVENANTS**

**Section 2.01. Representations, Warranties and Covenants of BUYER.** BUYER hereby represents and warrants to, and covenants with, NEIF as of the date hereof and as of each date a Loan is purchased hereunder, that:

BUYER has power and authority to execute and deliver this Agreement and to perform in accordance herewith; the execution, delivery and performance of this Agreement by BUYER and the consummation of the transactions contemplated hereby have been duly and validly authorized by all necessary action; and this Agreement evidences the valid, binding obligation of BUYER.

**Section 2.02. Representations, Warranties and Covenants of NEIF.** NEIF represents and warrants to, and covenants with, BUYER throughout the term of this Agreement, that:

(a) NEIF is a limited liability benefit company duly organized, validly existing and in good standing under the laws of the jurisdiction of its formation and has and will maintain all approvals and licenses required by Law to carry on its business as now being conducted, and is licensed, qualified and in good standing in each state where any Property is located if the laws of such state require licensing or qualification in order to conduct business of the type conducted by NEIF and perform its obligations hereunder and will maintain such licensing and qualifications; NEIF has corporate power and authority to execute and deliver this Agreement and to perform in accordance herewith; the execution, delivery and performance of this Agreement by NEIF and the consummation of the transactions contemplated hereby have been duly and validly authorized by all necessary corporate action; this Agreement evidences the valid, binding and enforceable obligation of NEIF, and all requisite corporate action has been taken by NEIF to make this Agreement valid, binding and enforceable upon NEIF in accordance with its terms.

(b) NEIF does not believe, nor does it have any reason or cause to believe, that it cannot perform in a reasonable manner its obligations as set forth in this Agreement, and without limitation, NEIF has adequate staff and experience to perform such obligations.

(c) NEIF is solvent and will not be rendered insolvent as a result of the performance of its obligations pursuant to this Agreement.

(d) NEIF shall originate, assign and service each Loan in accordance with the terms of this Agreement, all requirements of Law relating to such Loans, and all reasonable instructions of BUYER not in conflict with any of the foregoing.

(e) NEIF is a lender that actively provides origination, closing and servicing of loans and the transactions contemplated by this Agreement are in the ordinary course of business of NEIF.

(f) Subject to the terms and conditions set forth herein, NEIF shall at all times act in good faith in a commercially reasonable manner to originate, process, close, service and administer the Loans in accordance with applicable Law, this Agreement, and the terms of the respective Loans, and, to the extent consistent with the foregoing, in the same manner in which it services and administers similar loans, or other loans of any nature whatsoever, as applicable, for its own portfolio in accordance with customary and usual standards of practice of prudent lending institutions, and with a view to the maximization of timely recovery of principal and interest on the Loans.

(g) Subject to the terms and conditions set forth herein, applicable Law, and of the respective Loans, NEIF shall have full power and authority to do or cause to be done any and all things in connection with such servicing and administration which it may deem necessary or desirable without the consent or approval of BUYER, unless any such consent or approval is expressly required hereunder or under applicable Law. NEIF shall provide to the Obligor under the Loans all notices, Loan Document copies, disclosure statements and similar documents and any other reports required by Law to be provided to them. BUYER shall execute any powers of attorney and other documents required by Law to enable NEIF to carry out its servicing and administrative duties hereunder and necessary to maintain a lien; provided, however, that NEIF shall indemnify BUYER for any loss to BUYER resulting from any negligence with respect to, or misuse of, any such power of attorney by NEIF.

(h) NEIF has or shall acquire and shall maintain appropriate insurance coverage as provided in Exhibit 7, including but not limited to fidelity or banker's bonds, from insurers with an A.M. Best rating of A- or better, in form and substance reasonably satisfactory to BUYER. If any such policy is written on a claims-made basis, NEIF shall maintain such insurance for two (2) years after expiration or termination of this Agreement. Such insurance coverage shall be primary to any other coverage available to BUYER, and shall not be deemed to limit NEIF's liability under this Agreement. NEIF shall promptly notify the BUYER if any required insurance lapses or is otherwise modified and cease performance of this Agreement unless otherwise directed by the BUYER. In such case, the BUYER may procure insurance or self insure the risk and charge NEIF for such costs and any and all damages resulting therefrom, by way of set-off from any sums owed NEIF.

(i) NEIF is not aware of any suit, action, arbitration or legal or administrative or other proceeding pending or threatened against it by any regulatory authority or that would affect its ability to perform its obligations under this Agreement.

(j) Each offer of a Loan to BUYER shall be complete, truthful and accurate, shall be deemed to be a warranty that the proposed Loan described therein has been originated, underwritten and closed in compliance with Law.

(k) All Loan Documents submitted to BUYER shall be genuine and complete in all respects, and enforceable against Obligor in accordance with their terms. All other representations as to each such Loan shall be true and correct and meet the requirements and specifications of all parts of this Agreement;

(m) NEIF shall perform its services in accordance with the MCE Residential Energy Storage Loan Program Origination and Servicing Operation Details, as updated from time to time by BUYER and included by reference as Exhibit 9.

### **Section 2.03. Notice to BUYER.**

(a) If, at any time, any representation or warranty of NEIF set forth in this Agreement is not true and correct in any material respect as of the time made, NEIF shall promptly notify

BUYER of such fact in writing and provide a full and accurate explanation thereof. Without limitation, NEIF shall notify BUYER of any pending or threatened action, by way of a proceeding or otherwise, to revoke or limit any license, permit, authorization or approval issued or granted by any federal, state or local government or quasi-governmental body, or any agency or instrumentality thereof, necessary for NEIF to conduct its business, or to impose any penalty or other disciplinary action in connection therewith, or any other sanction that would materially affect NEIF's business. BUYER shall have all rights and remedies available under this Agreement and applicable Law in the event NEIF is in breach of any representation or warranty.

(b) NEIF shall furnish BUYER and its representatives with any necessary information and data concerning the affairs of NEIF, as BUYER may reasonably request, including information regarding the status of its licenses, permits, authorizations and approvals necessary for the conduct of its business as well as copies of such documents, and shall advise BUYER, in writing within three (3) Business Days, of any inquiries by any regulatory agencies with respect to any Loan.

(c) NEIF shall notify BUYER within five (5) Business Days of any corporate changes (such as those relating to contact personnel, or organizational or legal structure) that would have a material impact on NEIF's performance, management or administration of its duties and functions under this Agreement.

### **ARTICLE III ASSIGNMENT OF AGREEMENT**

**Section 3.01. *Assignment by BUYER.*** BUYER may assign its right, title and interest, and delegate its duties under this Agreement to any successor. BUYER agrees it shall not otherwise assign its right, title or interest in this Agreement with respect to one or more Loans without the prior written consent of NEIF, which consent shall not be unreasonably withheld; provided that any assignment or transfer caused by the operation of Law shall not require the consent of NEIF.

**Section 3.02. *Assignment by NEIF.*** NEIF may not assign any of its rights or privileges hereunder or make or enter into any delegation, subcontract, authorization or appointment with respect to any of its duties, liabilities or obligations hereunder to any third party, or any subsidiary or affiliate of NEIF without the prior written consent of BUYER, which consent shall not be unreasonably withheld.

## **ARTICLE IV FURTHER COOPERATION; CONFLICTS**

**Section 4.01. *Review of Reports.*** In the event any records or reports pertaining to any Loan are, in the reasonable judgment of BUYER, defective in accordance with the terms of this Agreement or applicable Law, NEIF shall cure such defects as expeditiously as circumstances will allow.

**Section 4.02. *Conflicts.*** Nothing in this Agreement shall preclude NEIF, in its individual capacity, from entering into other loans or other financial transactions with any Obligor, provided that all such transactions are subordinate in payment and collection to a Loan with the Obligor, and further provided that NEIF does not use or disclose any Confidential Information acquired under this Agreement.

**Section 4.03. *Inspections; Other Assistance.***

(a) NEIF shall allow BUYER's representatives at any reasonable time and from time to time, during normal business hours, with reasonable notice, reasonable access to NEIF's premises where services in respect of the Loans are being provided to examine NEIF's performance under this Agreement. NEIF shall provide to representatives of BUYER reasonable access (i) to the Loan Documents and all other documents related to NEIF's services under this Agreement, and to those employees of NEIF who are liable for the performance of NEIF's duties hereunder; (ii) to the books of account, records, reports and other papers of NEIF (including without limitation the Servicing Record) including, without limitation, for audit purposes; (iii) any other necessary information and data concerning the affairs of NEIF, as BUYER may reasonably request, including information regarding the status of its licenses, permits, authorizations and approvals necessary for the conduct of its business as well as copies of such documents, and (iv) any complaints or legal notices and any material questions or other communications relating to a Loan.

(b) If either party receives any complaints or legal notices relating to a Loan, it shall notify the other party within three (3) Business Days of receipt of such complaint or legal notice.

(c) NEIF shall cooperate and provide assistance as BUYER may from time to time request in connection with any inquiries or requirements of any regulatory authority in connection with a Loan, including using its best efforts to provide BUYER with any information or documentation that a regulatory authority may request in connection with any regulatory proceeding or otherwise, within the timeframes required.

**ARTICLE V**  
**NEIF AND BUYER DUTIES WITH RESPECT TO LOANS**

**Section 5.01. *NEIF's Duties with Respect to Origination and Assignment of All Loans.***

NEIF shall, in each case in compliance with all Law:

- (i) maintain call center functionality to field inquiries regarding prospective Obligors;
- (ii) maintain website with links to and from BUYER with program information, applications, forms and documents, relating to prospective Loans, for use by prospective Obligors;
- (iii) provide Loan program information, applications, disclosures, forms and related documents relating to prospective Loans to potential Obligors upon request;
- (iv) receive and process Loan applications to determine general eligibility of potential Obligor and Property for a Loan;
- (v) promptly communicate with potential Obligors and solicit Obligor and Property information required to complete underwriting analysis necessary to make a Loan under the applicable Law and Loan Criteria;
- (vi) promptly perform such underwriting analysis on potential Loans pursuant to this Agreement and applicable Law and determine Loan application approval or denial;
- (vii) prepare and ensure proper execution of Loan Documents for approved Loans, using forms for the applicable loan program developed by NEIF and approved by BUYER but in any event in compliance with Law;
- (viii) hold Loan proceeds and any other funds provided for closing in trust for Obligor and BUYER in the Account and protect the Account from claims, liens, process, and encumbrances by NEIF's creditors and other third parties;
- (ix) debit the Account for the Loan Amount for each Loan, coordinate and conduct Loan closings, and coordinate and cause disbursement of proceeds in accordance with Law; and
- (x) immediately after closing each Loan assign such Loan to Buyer using Blanket Assignment (Exhibit 3), and retain secure possession of all original Loan Documents.

**Section 5.02. *Underwriting Guidelines.*** NEIF shall observe the underwriting guidelines and other Loan Criteria as may be established by BUYER in originating Loans under this Agreement. BUYER may, by written notice to NEIF, alter the underwriting guidelines at any time. NEIF shall implement all such changes to the underwriting guidelines as soon as reasonably



possible, but no later than within fourteen (14) days of BUYER's notice, unless extended by BUYER through written notice to NEIF, which extension of time may be granted or withheld in BUYER's complete and sole discretion. NEIF shall not make changes to the underwriting guidelines without the written approval from BUYER.

**Section 5.03. BUYER's *Duties with Respect to All Loans.***

(a) BUYER shall:

- (i) fund the Account such that the Loan Amount can be debited upon NEIF's approval of loan for disbursement to contractor on behalf of borrower.
- (ii) replenish the Account each month unless funds are needed more frequently to ensure availability for disbursement

(b) Each of NEIF and BUYER agree that the loan transactions contemplated by this Agreement are intended to be and shall constitute sales of the Loans from NEIF to BUYER and are not intended to be financings or loans by BUYER to NEIF. The Parties shall treat such transactions as true sales for tax, accounting and all other purposes. The sale of each Loan pursuant to this Agreement transfers to BUYER all of NEIF's right, title, and interest in and to such Loan and the related Loan Documents, and NEIF will not retain any residual rights with respect to any such Loan (except as BUYER's servicing agent) and NEIF shall effectively note the sale of each Loan on the related installment loan note and other Loan Documents. The Parties hereby intend that (i) the Purchased Loans transferred pursuant hereto shall be deemed to no longer be the property, assets, rights, or liabilities of NEIF and (ii) in the event of a bankruptcy, receivership, or other insolvency proceeding with respect to NEIF or NEIF's property, the Purchased Loans transferred pursuant hereto shall not be deemed to be part of NEIF's property, assets, rights, or estate, except with respect to any servicing obligations of NEIF hereunder.

**Section 5.04. *NEIF's Duties with Respect to Servicing All Loans.***

With respect to each Loan, until the earlier of the termination of this Agreement or the sale, assignment or other disposition of ownership by BUYER of the Loan, NEIF shall service the Loan as required herein, and shall do all things necessary to perform such services and duties pursuant to this Agreement consistent with Law and loan servicing industry standards, including without limitation:

- (i) maintain its Servicing and Collection Policy (attached as Exhibit 6) in compliance with Law and ensure its loan servicing activities comply with such policy;
- (ii) manage and perform loan servicing activities including receiving, processing and accounting for payments and credits on all Loans;
- (iii) communicate and correspond with Obligor's regarding billing and payment inquiries and requests for adjustment;

(iv) communicate promptly with BUYER regarding any Loan payment default or request for adjustments;

(v) transfer Loan Payments (minus compensation and reimbursement then due to NEIF under this Agreement) to BUYER's designated accounts by electronic funds transfer pursuant to instructions provided by BUYER in writing from time to time;

(vi) exercise commercially reasonable efforts to collect all payments due under the terms of each Loan, and follow such collection procedures as NEIF would follow with respect to comparable loans held for its own account, subject to requirements of Law, and provided that NEIF shall commence legal action, respond to any legal claim regarding any Loan, take action with respect to collateral seizure or liquidation only with BUYER's prior written consent and pursuant to written direction from BUYER's Executive Director, or his/her designee and only in compliance with Law;

(vii) maintain records of all Loan applications received, all determinations of Loan eligibility or ineligibility communicated to a potential Obligor, all Loan approvals and denials communicated to Loan applicants, all scheduled Loan closings, all completed Loan closings, all Loan disbursements and payments, and all installation measures associated with each Loan, and other reporting as may be necessary for BUYER;

(viii) remit interest earned on the Account to BUYER;

(ix) cause the financial institution at which the Account is maintained to deliver duplicate monthly statements regarding the Account to NEIF and BUYER;

(x) prepare and provide such other records and reports as may be required by applicable Law, or as may be reasonably requested by BUYER from time to time; and

(xi) cause to be implemented and maintained all quality control reviews and audits of Loan origination and servicing practices as may be required by BUYER from time to time or as otherwise required by Law.

**Section 5.05. *BUYER's Duties with Respect to Servicing All Loans.***

BUYER shall do such things as are necessary under applicable Law to permit NEIF to perform its obligations under this Article.

**Section 5.06. *Origination and Servicing Records, Collections and Remittance.***

(a) Without limitation of NEIF's other enumerated duties under this Agreement, NEIF shall establish and maintain for a period of at least three (3) years after expiration or termination of this Agreement, accurate books and records (the "Servicing Record") in which NEIF shall record all Loan applications, closed Loans, funds received and funds disbursed, and Payments received or collected by NEIF in respect of each Loan, and all amounts owing to NEIF in

compensation for services rendered by NEIF hereunder and in reimbursement of costs and expenses incurred by NEIF hereunder (all pursuant to the Fee Schedule) and shall provide a true copy of such Servicing Record to BUYER monthly on the 15<sup>th</sup> day of each month, such Servicing Record to be current through the end of the previous month, and shall remit to BUYER, with each such Servicing Record copy, all Payments net of amounts due to NEIF hereunder as compensation or reimbursement.

(b) Except as otherwise provided herein, Payments shall be credited to the Servicing Record. Any prepaid Monthly Payment received on any Loan shall be recorded as a prepaid Monthly Payment when received. Any partial Monthly Payment may be held by NEIF until the full amount of the payment is received, but the due date will not advance until a full Monthly Payment has been received. All Payments received from or on behalf of an Obligor shall be allocated, first, to the oldest payment overdue at such time and apportioned as to such oldest payment first to scheduled interest (other than default interest, if any) due on such oldest payment date, second to any principal due and payable, and third to default interest, if any, late charges and other amounts payable under the Loan, to the extent permitted by Law.

(c) NEIF shall credit to the Servicing Record relating to each Due Period, individually for each Loan, each of the following Payments collected or received by NEIF in respect of each Loan:

- (i) all payments on account of principal (including all Principal Prepayments);
- (ii) all payments on account of interest;
- (iii) all amounts paid by or on behalf of the related Obligor in respect of legal fees previously advanced by NEIF;
- (iv) any settlements or any payments made by any related guarantor or third-party credit-support provider;
- (v) any and all other amounts received in respect of a Loan and not specified above.

(d) On or before each Monthly Cut-Off Date, NEIF shall record in the Servicing Record, individually for each Loan:

- (i) the amount of fees properly incurred during the preceding Due Period to be paid to any Independent Contractor hired by NEIF to pursue and enforce any judgment, as may be authorized by BUYER in writing; and
- (ii) all amounts due as of the end of the preceding Due Period in reimbursement of legal expenses properly incurred in the pursuit of obtaining repayment of amounts owed by the Obligor (separately identifying the type and amount of each expense then due) as may be authorized by BUYER in writing.

- (e) NEIF shall maintain such records as are necessary under applicable Law.

**Section 5.07. *Certain Tax Matters.*** NEIF shall provide BUYER with such information from the Servicing Record as BUYER shall reasonably request to prepare any tax returns, and any other federal, state or local tax or information returns or reports that are required to be so filed by BUYER.

**Section 5.08. *Modifications, Waivers, Amendments, Legal Consultation, Legal Action and Consents.*** Without the prior written consent of BUYER and only pursuant to the written direction of BUYER's Executive Director or his/her designee, NEIF shall not agree to any modification, waiver, or amendment of any provision of any Loan, nor incur any Third Party Contractor expense, nor take any legal action with respect to any Loan, nor respond to any legal claim regarding any Loan.

**Section 5.09. *Release of Files.***

- (a) If, with respect to any Loan:
- (i) the outstanding balance of principal of such Loan plus all interest accrued thereon and other amounts due thereunder shall have been paid;
  - (ii) NEIF shall have received, in escrow, payment in full of such Loan in a manner customary for such purposes; or
  - (iii) such Loan has been sold or otherwise conveyed to a person other than BUYER;

then NEIF, as the case may be shall, within thirty (30) Days or such shorter period as may be required by applicable Law, (A) in the case of (i) or (ii) above, deliver to Obligor the cancelled promissory note or guaranty executed by such Obligor in connection with such Loan, and (B) in the case of (iii) above, release, or cause to be released, the related File to the appropriate party and deliver for execution by BUYER such instruments of transfer or assignment, in each case without recourse, as shall be necessary to vest ownership of such Loan in such other Person.

(b) After a Purchase, all executed Loan Documents and instruments held in the custody of NEIF shall be held by NEIF for the benefit of, and as agent for, BUYER as the legal owner thereof. NEIF shall promptly report to BUYER in writing any failure by it to hold such Loan Documents and instruments as herein provided and shall promptly take appropriate action to remedy any such failure. In acting as custodian of such documents and instruments, NEIF agrees not to assert any legal or beneficial ownership interest in Loans purchased or such documents or instruments. NEIF agrees to indemnify BUYER for any and all liabilities, obligations, losses, damages, payments, costs or expenses of any kind whatsoever which may be imposed on, incurred by or asserted against BUYER as the result of any act or omission by NEIF relating to the maintenance and custody of such documents or instruments; provided, however, that NEIF will

not be liable (i) for any portion of any such amount resulting from the negligence or misconduct of BUYER and (ii) for any portion of any such amount resulting from NEIF's compliance with any written instructions or directions consistent with this Agreement issued to NEIF by BUYER. BUYER shall have no duty to monitor or otherwise oversee NEIF's performance as custodian hereunder. Provided, however, that nothing in this Section shall modify or limit any rights and privileges granted to BUYER elsewhere in this Agreement regarding inspection, monitoring or oversight of this Agreement.

**Section 5.10. *No Promotion.*** NEIF, its employees, subcontractors, and agents shall not, without the prior written consent of BUYER, (a) use in advertising, publicity or otherwise (i) the name of BUYER, or their respective employees, representatives, or agents (ii) any trade name, trademark, trade device, service mark, symbol or any abbreviation, contraction or simulation thereof owned by BUYER, or (b) represent, directly or indirectly, that any product or any service provided by NEIF is approved or endorsed by BUYER or their respective affiliates.

**Section 5.11. *Reserved.***

**Section 5.12. *Data Security and Disaster Recovery Plan.*** NEIF shall take commercially reasonable steps to safeguard all data and information regarding all Obligors, Loans, Loan Documents, and Loan Materials and shall implement administrative, physical, and technical safeguards to protect all such data and information from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than accepted industry practices. NEIF shall comply with all applicable data security Laws. NEIF shall, at its own expense, maintain a commercially reasonable disaster recovery plan in support of the functions it performs for BUYER under this Agreement that provides for disaster recovery and the resumption of business in the event that a disaster disrupts or impairs its performance pursuant to this Agreement. Upon the reasonable request of BUYER, NEIF shall provide to BUYER a copy of such disaster recovery plan. A copy of NEIF's disaster recovery plan as of the date hereof is attached hereto as Exhibit 4.

**Section 5.13. *Complaints.*** In the event that NEIF receives any complaints with respect to any Loan, NEIF shall notify BUYER of the complaint within three (3) Business Days, inform BUYER of NEIF's plan to resolve such complaint, resolve such complaint, and provide copies of all correspondence relating to such complaint (including the original complaint) to BUYER. In the event a complaint is received from any federal or state banking regulator, any other federal or state agency or regulator or from an attorney representing any Obligor, (collectively referred to as "Escalated Complaints") NEIF shall notify BUYER within three (3) Business Days and provide copies of all correspondence relating to such Escalated Complaint (including any original complaint from the Obligor on which the Escalated Complaint is based). No response to any Escalated Complaint is to be sent without BUYER's prior written approval of the response. NEIF's Complaint Policy is attached hereto as Exhibit 5.

**Section 5.14. *Obligation to Repurchase.***

- (a) NEIF shall repurchase upon written demand from BUYER any particular Loan assigned to BUYER pursuant to this Agreement if any one or more of the following

- circumstances exist with regard to that Loan, regardless of whether Obligor is making payments on said Loan:
- (i) Loan did not meet Loan Criteria;
  - (ii) Loan did not comply with all applicable Laws;
  - (iii) Loan Documents are unenforceable;
  - (iv) NEIF or BUYER determines in a commercially reasonable manner that evidence of fraud exists with respect to the Loan;
  - (v) BUYER's audit procedure reveals any evidence of fraud in the origination of the Loan or in the sale of the Loan to BUYER or that any matter in the Loan file is not materially true and correct;
  - (vi) The Obligor is deceased prior to the applicable Blanket Assignment date; or
  - (vii) Any Loan with an account in bankruptcy, litigation, or process of repossession prior to the applicable Blanket Assignment date.
- (b) For each repurchase of a Loan pursuant to this Agreement, the "Repurchase Price" to be paid by NEIF shall be equal to the Principal Balance of such Loan, plus all accrued but unpaid interest on such Loan, plus any unreimbursed costs and expenses incurred by BUYER due to such Loan. Upon receipt of such Repurchase Price, BUYER shall transfer its interest in such repurchased Loan to NEIF on an "AS-IS," "WHERE-IS" basis, without any representations or warranties other than with respect to BUYER's clear and marketable title to such repurchased Loan. Any repurchase by NEIF shall be made by bank transfer of immediately available funds to the bank account as designated by BUYER.
- (c) Upon any such repurchase of Loan by NEIF, BUYER shall endorse the Loan and any other applicable Loan Documents and shall assign same in recordable form, as commercially reasonable, to NEIF, without representations and warranties, whether express or implied, and without recourse to BUYER.

**Section 5.15. Privacy Requirements.** NEIF and BUYER understand and agree that the Customer Information, as defined herein, is subject to applicable federal and state privacy regulations and other Laws of any government or agency or instrumentality thereof regarding the privacy or security of Customer Information (the "Privacy Requirements"). NEIF and BUYER agree that they shall each comply with the Privacy Requirements and shall cause all of their agents, employees, affiliates and any other person or entity that receives the Customer Information from NEIF or BUYER, respectively, to comply with the Privacy Requirements and the NEIF or BUYER, respectively, will promptly notify BUYER or NEIF, as applicable, of any breach of the Privacy Requirements. Furthermore, NEIF and BUYER shall maintain (and shall cause all of its respective agents, employees, affiliates and any other person or entity that receives the Customer Information from the Servicer to maintain) appropriate administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Customer Information, including, if applicable, maintaining security measures designed to meet the Privacy Requirements. For purposes of this Section 5.15, "Customer Information" means any non-public information

concerning an Obligor regardless of whether such information was provided by BUYER to NEIF or was prepared by NEIF, BUYER or any affiliate or agent of NEIF or BUYER based on or derived from the Customer Information. Any communications by NEIF with any Obligor shall comply with all Laws.

## **ARTICLE VI INVOLUNTARY TERMINATION**

**Section 6.01. *Involuntary Termination.*** BUYER may, by written notice, terminate all of NEIF's rights pursuant to this Agreement with respect to all Loans upon the happening of any one or more of the following events:

(a) Failure of NEIF to properly account for all moneys received by NEIF relating to the Loans, which failure continues unremedied for thirty (30) calendar days; or

(b) Failure of NEIF to pay when due any other amount payable by it under this Agreement; or

(c) Failure of NEIF to notify BUYER of NEIF's failure duly to observe or perform in any material respect any of its other covenants or obligations contained in this Agreement; or

(d) Breach by NEIF of any other representation, warranty, covenant, term, or agreement contained in this Agreement which breach continues for a period of thirty (30) calendar days after the earlier of the date NEIF is or shall have been aware of the breach or the date on which BUYER gives notice of the breach to NEIF; provided, however, if such failure stated in the notice cannot be corrected within the applicable period, BUYER shall consent to a reasonable extension of time if corrective action is instituted by NEIF within the applicable period and NEIF diligently pursues it until fully corrected; or

(e) NEIF avails itself of, or is subjected to by any third party, a proceeding in bankruptcy in which NEIF is the named debtor, an assignment by NEIF for the benefit of its creditors, the appointment of a receiver for NEIF, or any other proceeding involving insolvency or the protection of, or from, creditors, and appointment of a receiver for NEIF, or any other proceeding involving insolvency or the protection of or from creditors, and same has not been discharged or terminated without any prejudice to NEIF's rights or interests under this Agreement within thirty (30) calendar days; or

(f) Consent by NEIF to the appointment of a conservator, receiver or liquidator in any bankruptcy, insolvency, readjustment of debt, marshaling of assets and liabilities or similar proceeding affecting NEIF or substantially all of its properties.

In each and every such case, BUYER may, by notice in writing to NEIF, terminate all of the rights and obligations of NEIF under this Agreement and in and to any Loans or proposed Loans and any Payments or right to Payments. NEIF shall give written notice to BUYER of the occurrence of

any event described in this Section 6.02(e) or 6.02(f) within two calendar days of the happening of such event. Otherwise, NEIF shall give written notice to BUYER of the occurrence of any event described in this Section 6.02(a), 6.02(b), 6.02(c), or 6.02(d) within ten (10) days of the happening of such event.

NEIF agrees to cooperate with the successor originator and/or successor servicer in effecting the termination of the responsibilities and rights of NEIF hereunder and provide to the Obligor any notices required by Law.

BUYER may exercise all rights and remedies available at law or in equity in the event of an involuntary termination of NEIF under this Section 6.02.

**Section 6.02. *Voluntary Termination.*** BUYER may terminate this Agreement at any time in its discretion following twelve (12) months of this Agreement's Effective Date for new originations after desired termination date, by providing NEIF written notice of such termination ninety (90) days prior to BUYER's desired termination date.

**Section 6.03. *NEIF's Duties Upon Termination.***

(a) From and after the receipt by NEIF of such written notice of its termination from BUYER pursuant to Section 6.02, or upon a termination pursuant to Section 6.01 hereof, NEIF shall cooperate with BUYER in effecting the termination of NEIF's responsibilities and rights hereunder, including, without limitation, the transfer to the successor servicer for administration by it of all cash amounts then held by NEIF or thereafter received with respect to Loans and the delivery to the successor originator and/or servicer of all Files and an electronic file in readable form containing the Servicing Record and any other information necessary to enable the successor originator to complete the origination or denial of, and the successor servicer to service, Loans;

(b) NEIF shall cooperate with any such successor servicer in effecting the transfer of NEIF's servicing responsibilities and rights hereunder, including, without limitation, the transfer to such successor servicer of all relevant records and documents (including any Files in the possession of NEIF and the Servicing Record) and all amounts credited to the Servicing Record or thereafter received with respect to Loans and not otherwise permitted to be retained by NEIF pursuant to this Agreement.

**Section 6.04. *Attorney's Fees.*** If it is determined in a judicial proceeding that a party to this Agreement is in breach and has failed to perform under any provision of this Agreement, and if the other party shall employ attorneys or incur other expenses to enforce the performance or observance of the terms of this Agreement by the non-performing party, or to perform such obligations itself, then such party, to the extent permitted by Law, shall be reimbursed by the non-performing party, on demand, for reasonable attorney's fees, paralegal fees and other out-of-pocket expenses, including without limitation such fees and expenses arising in connection with any bankruptcy case or proceeding, to the extent the same are not paid in connection with any such judicial proceeding.



## **ARTICLE VII NOTICE OF CLAIMS**

**Section 7.01. *Notice of Claims.*** NEIF shall promptly, but in no event later than three (3) Business Days after becoming aware, notify BUYER in writing of any and all litigation and claims made or threatened against BUYER or NEIF in connection with Loans or proposed Loans originated, denied, or serviced pursuant to this Agreement.

## **ARTICLE VIII MISCELLANEOUS PROVISIONS**

**Section 8.01. *Amendments, Changes and Modifications.*** This Agreement may be amended, changed, modified or altered only in writing, signed by BUYER and NEIF.

**Section 8.02. *Governing Law.*** THIS AGREEMENT SHALL BE CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE COMMONWEALTH OF PENNSYLVANIA AND APPLICABLE FEDERAL LAW AND THE OBLIGATIONS, RIGHTS AND REMEDIES OF THE PARTIES HEREUNDER SHALL BE DETERMINED IN ACCORDANCE WITH SUCH LAWS WITHOUT GIVING EFFECT TO PRINCIPLES GOVERNING CONFLICTS OF LAW.

**Section 8.03. *Notices.*** All demands, notices, certificates or other communications hereunder shall be in writing (unless otherwise specified) and shall be deemed given one (1) Business Day after mailing by FedEx or two (2) Business Days after mailing by United States Postal Service Second Day Priority Mail, postage prepaid, return receipt requested, addressed to the appropriate Notice Address.

**Section 8.04. *Severability.*** In the event any provision of this Agreement shall be held invalid or unenforceable by any court of competent jurisdiction, such holding shall not invalidate or render unenforceable any other provision hereof and such invalid or unenforceable provision shall be amended, if possible, in accordance with Section 8.01 above in order to accomplish the purposes of this Agreement.

**Section 8.05. *Term of Agreement.*** This Agreement shall become effective upon its approval and execution by the parties hereto (the "Effective Date"), and subject to the provisions of Article VI, shall continue until each Loan closed under this Agreement has been repaid in full and/or BUYER has released the Obligor from liability under such Loan.

**Section 8.06. *Limitation of Liability of Parties.*** Subject to any indemnity obligations of a party under this Agreement, each party to this Agreement shall be liable under this Agreement only to the extent that obligations are imposed upon the party against whom enforcement is sought. Nothing in this Agreement is intended to, nor shall be construed to, waive, limit or diminish immunity from liability of BUYER as a governmental or public agency.

**Section 8.07. *Limitation of Liability of Directors, Officers, Employees and Agents of a Party.*** No director, officer, employee or agent of any party to this Agreement shall be individually liable to any other party for taking of any action or for refraining to take any action in good faith pursuant to this Agreement or for errors in judgment. In addition, in the event any party to this Agreement is entitled to indemnification hereunder, the officers, directors, employees, and agents of such party shall also be entitled to indemnification hereunder to the same extent and under the same circumstances as such party.

**Section 8.08. *Survival of Obligations and Covenants.*** Notwithstanding anything to the contrary herein, neither the expiration nor termination of this Agreement shall affect any obligations of either party which are meant to survive this Agreement. In the event that this Agreement is terminated prior to this Agreement's expiration as provided in Section 8.05, NEIF shall have the duty to continue to provide such services as are required under this Agreement, until such time as BUYER either (a) designates a successor provider of such services or (b) expressly releases NEIF from such duty by written notice to NEIF, and NEIF shall be entitled to fair compensation not inconsistent with this Agreement for its services during such period.

**Section 8.09. *Counterparts.*** This Agreement may be executed in any number of counterparts, each of which shall be an original; provided, however, that all such counterparts shall together constitute one and the same Agreement.

**Section 8.10. *Confidentiality.***

(a) NEIF acknowledges that it may, in the course of performing its responsibilities under this Agreement, be exposed to or acquire Confidential Information of BUYER, its program participants, customers, or third parties to whom BUYER owes a duty of confidentiality. NEIF shall hold the Confidential Information in strict confidence and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give or disclose Confidential Information to third parties or to use Confidential Information for any purposes other than the performance of this Agreement, except as required by Law. NEIF shall (i) advise each of its personnel, employees, agents, affiliates, and subcontractors (and their employees) who may be exposed to the Confidential Information of their obligation to keep such information confidential, and (ii) be liable for breach of this Section by any personnel, employees, agents, affiliates, and subcontractors.

(b) BUYER acknowledges that it may, in the course of performing its responsibilities under this Agreement, be exposed to or acquire Confidential Information of NEIF, its affiliates, their customers, or third parties to whom NEIF owes a duty of confidentiality. BUYER shall hold the Confidential Information in strict confidence and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give or disclose Confidential Information to third parties or to use Confidential Information for any purposes other than the performance of this Agreement, except as required by Law. BUYER shall (i) advise each of its personnel, employees, agents, affiliates, and subcontractors (and their employees) who may be exposed to the Confidential Information of their obligation to keep such information confidential, and (ii) be liable for breach of this Section by any personnel, employees, agents, affiliates, and subcontractors.

(c) If either party is requested to disclose any Confidential Information, that party shall (i) immediately notify the other party of the existence, terms and circumstances surrounding such request; and (ii) consult with the other party on the advisability of taking legally available steps to resist or narrow such request and cooperate with the other party on any such steps it considers advisable; provided, that the ultimate decision on disclosure will be made by the party to which the request was made.

### **Section 8.11 *Proprietary Information.***

“NEIF Proprietary Information” means the following specific, unique and NEIF-created systems and materials: (a) marketing programs; (b) website designs (excluding website media displaying BUYER’s logo) and underlying architecture; (c) computer systems; (d) loan application, processing, disclosure, closing, servicing and reporting systems (excluding (i) any specific loan applications, notices of approval or denial, closing, collection or disclosure documents (in any form or media), (ii) communications and all other records (preserved in any form or media), regarding any of the foregoing, any Payments, and any release or sale of any Loan, and (iii) any Loan Documents not otherwise listed in the foregoing subsections (i) and (ii) (collectively, the “Loan Materials”). BUYER expressly consents and agrees that all NEIF Proprietary Information is owned exclusively by NEIF and that all NEIF Proprietary Information shall be subject to the Confidentiality provisions of Section 8.10. Any and all NEIF Proprietary Information shall be delivered (if in form susceptible to delivery) to NEIF upon request and in any event at the termination of this Agreement, and neither BUYER nor its employees, affiliates, subcontractors or agents shall retain any copies thereof without NEIF’s prior written consent except as may be required by law. For purposes of clarity, all “files, documents, records, data, papers, and other works produced or received by NEIF,” and “works,” both as described in Section 8 of Exhibit 1 to this Agreement do not expand the definition of Loan Materials provided hereinabove, but describe only Loan Materials.

**Section 8.13. *Headings.*** The titles and headings of the articles and sections of this Agreement have been inserted for convenience of reference only and are not to be considered a part hereof and shall not in any way modify or restrict any of the terms or provisions hereof and shall not be considered or given any effect in construing this Agreement or any provision hereof in ascertaining intent, if any questions of intent should arise.

**Section 8.14. *Relationship of the Parties.*** In performing its duties and obligations hereunder, NEIF shall be an Independent Contractor to, and except as expressly provided herein not an agent of, BUYER. Nothing herein contained shall be deemed or construed to create a partnership or joint venture between BUYER and NEIF.

**Section 8.15. *Exhibits.*** The following exhibits are attached hereto and made part of this Agreement, and all references to this Agreement shall include the following exhibits:

Exhibit 1 -- Underwriting Guidelines  
Exhibit 2 -- Fee Schedule  
Exhibit 3 -- Blanket Assignment  
Exhibit 4 -- Complaint Policy  
Exhibit 5 -- Disaster Recovery Plan  
Exhibit 6 -- Servicing and Collection Policy  
Exhibit 7—Required Insurances and Fidelity Bonds  
Exhibit 8 -- Program Setup Services  
Exhibit 9 -- MCE Residential Energy Storage Loan Program Origination and Servicing Operation Details

**Section 8.16. *Electronic Signature; Counterparts.*** Each Party agrees that this Amendment may be executed by electronic signature and that any electronic signatures of the Parties included in this Amendment are intended to authenticate this writing and to have the same force and effect as manual signatures. Electronic signature means any electronic symbol or process attached to or logically associated with a record and executed and adopted by a party with the intent to sign such record, including facsimile or email electronic signatures. The Amendment may be executed in one or more counterparts, with each counterpart constituting an original and all counterparts, when taken together, constituting one and the same agreement. The exchange of executed signature pages of the Amendment by facsimile, email or .PDF transmission will constitute effective execution and delivery of the Amendment.

**Section 8.17. *No Recourse Against Constituent Members.*** BUYER is organized as a Joint Powers Authority in accordance with the Joint Exercise of Powers Act of the State of California (Government Code Section 6500, et seq.). Pursuant to BUYER's Joint Powers Agreement, BUYER is a public entity separate from its constituent members. BUYER shall solely be responsible for all debts, obligations, and liabilities accruing and arising out of this Agreement. NEIF shall have no rights to, nor shall NEIF make any claims, take any actions, or assert any remedies against any of BUYER's constituent members in connection with this Agreement. This Section shall survive termination of this Agreement.

**Section 8.18 *Indemnification.*** NEIF shall indemnify, defend and hold BUYER and its trustees, officers, employees, representatives, members, directors, parent companies, affiliates, subsidiaries, successors and assigns harmless from any and all claims, demands, causes of action, losses, damage, fines, penalties, liabilities, costs and expenses, including reasonable attorney's fees and court costs, sustained or incurred by BUYER by reason of or arising directly from third party claims that were caused by or resulted from (A) any actions or omissions by NEIF or its contractors or agents that are outside the scope of its authority hereunder except to the extent BUYER has approved in writing of the action that was outside the scope of its authority and/or (B) taking any action, or refraining from taking any action, with respect to any Loan or property, by NEIF, NEIF's contractors, or agents, that result from the malfeasance, willful misconduct, gross negligence, breach of this Agreement or a failure by NEIF to act in compliance with the terms of this Agreement. The foregoing indemnification shall survive the termination of this Agreement.

**Section 8.19 *Nondiscriminatory Employment.*** NEIF shall not unlawfully discriminate against any individual based on race, color, religion, nationality, sex, sexual orientation, gender identity, age or condition of disability. NEIF understands and agrees that NEIF is bound by and shall comply with the nondiscrimination mandates of all federal, state, and local statutes, regulations, and ordinances.

**Section 8.20 *Disputes.*** Either Party may give the other Party written notice of any dispute which has not been resolved at a working level. Any dispute that cannot be resolved between NEIF's contract representative and BUYER's contract representative by good faith negotiation efforts shall be referred to legal counsel of BUYER and an officer of NEIF for resolution. Within 20 calendar days after delivery of such notice, such persons shall meet at a mutually acceptable time and place, and thereafter as often as they reasonably deem necessary to exchange information and to attempt to resolve the dispute. If BUYER and NEIF cannot reach an agreement within a reasonable period of time (but in no event more than 30 calendar days), BUYER and NEIF shall have the right to pursue all rights and remedies that may be available at law or in equity. All negotiations and any mediation agreed to by the Parties are confidential and shall be treated as compromise and settlement negotiations, to which Section 1119 of the California Evidence Code shall apply, and Section 1119 is incorporated herein by reference notwithstanding Section 8.02.

## **ARTICLE IX PAYMENT TO NEIF**

**Section 9.1 *Program Compensation.*** In full compensation for NEIF's services, actions, and activities under this Agreement, including payments to Independent Contractors engaged by NEIF in connection with NEIF's obligations under this Agreement, NEIF shall be paid the amounts shown on the Fee Schedule. Payment of servicing fees is subject to the terms of this Agreement.

**IN WITNESS WHEREOF, each of the undersigned parties has caused this Agreement to be duly executed and delivered by its duly authorized officers.**

**BUYER: MARIN CLEAN ENERGY**

DocuSigned by:



8ABF434893004F1...  
By: Chairperson

DocuSigned by:



A50878416EBC4F8...  
By: Dawn Weisz, CEO

**NEIF: NATIONAL ENERGY IMPROVEMENT FUND, LLC**

DocuSigned by:



AEBF3BFD567945B...  
By:

Laura Nelson Chief Operating Officer

(Print Name and Title)

## Exhibit 1

MCE Residential Energy Storage Direct Loan Program	
Credit Guidelines	
05/07/21	
<b>MINIMUM FICO (CREDIT SCORE)</b> <ul style="list-style-type: none"> <li>Each Borrower must have a minimum FICO</li> <li>If there are multiple borrowers, the lower score (regardless of income) must be used for qualification</li> </ul>	All residential loans: 640  *salaried, fixed income or self-employed
<b>Citizenship</b>	Citizen or Permanent Resident (self-certify)
<b>Bankruptcy, Foreclosure, Repossession</b>	None in the last 5 years
<b>DTI</b>	≤ 50%; 42% for loans > \$25,000
<b>Term</b>	5 year – General Market Residential Customers 10 year – Priority Residential Customers 10 year – Low Income Residential Customers
<b>Loan Amount</b>	Maximum Loan: \$50,000 Minimum Loan: \$1,500
<b>Rates</b>	Low-Income: 0.00% Priority: 2.50% General Market: 5.50%
<b>Qualifying Improvements</b>  The following qualifying improvements are eligible for funding: <ul style="list-style-type: none"> <li>Battery Energy Storage System</li> <li>Smart Panel</li> <li>Panel Size Upgrade</li> </ul>	100% of Total Loan Amount
<b>Property</b>	<ul style="list-style-type: none"> <li>1 to 4-unit primary home; no investment properties; no summer homes</li> <li>Owner-occupied or owner cosigned</li> <li>Must be affixed to permanent foundation</li> <li>Unsecured loans – property type is for qualification purpose only—no lien is filed</li> </ul>
Loans may be declined or subject to further review if underwriter determines that FICO score or other factors are inconsistent with actual credit profile.	

Exhibit 1

Income Verification Requirements
<ul style="list-style-type: none"><li>• FICO is 680 or greater:<ul style="list-style-type: none"><li>○ Primary Income: No verification required for primary income; income is subject to verification for loans greater than \$25,000</li></ul></li><li>• FICO is less than 680:<ul style="list-style-type: none"><li>○ Primary Income: Verification is required</li></ul></li><li>• Secondary income is subject to verification for all FICOs</li></ul>



**Exhibit 2- Fee Schedule****Monthly Servicing Fee:**

A fee equal to 2.49% of the unpaid principal balance of all funded loans at the end of each month, divided by 12.

Example- if the portfolio is \$2,123,456.00 after all new loans are funded and all payments are applied for that month, the calc would be as follows:

Calculation of Service Fee	
Balance as of 2/1/2021 -- start of day	\$ 2,123,456.00
Times Loan Servicing rate	0.0249
Divided by 12 months	12
January Fee Calculation	<u>\$ 4,406.17</u>

This monthly servicing fee is for the servicing of loans pursuant to the MCE Residential Energy Storage Loan Program & Servicing Operational Details as provided to NEIF and as updated by BUYER from time to time.

**Origination Fee:**

A fee equal to \$50.00 will be paid to NEIF on each funded loan for loans funded in the prior month.

**Technical Services Setup Fee:**

A one-time fee equal to \$2,500 will be paid to NEIF at execution of the Agreement as a Technical Services setup fee, to include IT setup, training and related setup functions.

**Program Services Setup Fee:**

A one-time fee equal to \$18,450 will be paid to NEIF at execution of the Agreement for Program Services Setup functions outlined in Exhibit 8.

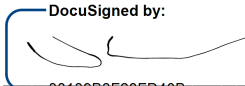
## Blanket Assignment

Lender: National Energy Improvement Fund, LLC

Buyer and Assignee: Marin Clean Energy

Pay each of the Notes immediately upon loan funding to the order of Marin Clean Energy, a California joint powers authority located at 1125 Tamalpais Avenue, San Rafael, CA 94901, without recourse, except as otherwise provided in the Loan Origination and Servicing Agreement dated May 6, 2021 between National Energy Improvement Fund, LLC and Marin Clean Energy

National Energy Improvement Fund, LLC

By:  38139B3F26FD40B...

Matthew H. Brown, Managing Member



Any complaint received by any NEIF staff member will be entered into Compligo for tracking and resolution monitoring. The Department Heads will review complaint reports to determine if there are complaint trends that indicate a need for targeted compliance training or procedural changes. Department Heads will also participate in meetings with Executive Management, during which specific complaints received from or through a federal or state regulatory agency, NEIF, the Better Business Bureau (“BBB”), or state law enforcement agencies will be reviewed. The purpose of these meetings is to determine if any of the complaints indicate a need for procedural changes or represent potential violation of consumer regulations requiring corrective action.

If a complaint is made via telephone:

- Be polite and respectful.
- Listen to the complaint and offer to review the situation immediately.
- Check the facts.
- Review the complaint and the facts with the customer.
- If the customer is right, apologize and fix the problem.
- If the customer is mistaken, qualify that you can see where the misunderstanding occurred and assure them that all is well. Never embarrass them. Offer to send them written proof from their account that corroborates the facts.
- Always notate the account.

- Read the complaint and gather the facts.
- If the customer is right, fix the error. Try calling the customer to explain the error and notate the account. If that is not possible, compose an apology email or letter. Tell them what was done to correct the error. Attach the email or letter to the file for reference if needed in the future. Notate the account.
- If the customer is mistaken, try calling them to verbally review the facts and assure them that all is well. Notate the account. If that is not possible, compose a detailed email or letter listing the facts and offer to review the issue with them via the phone. Attach the email or letter to the account for future reference. Notate the account.
- If an issue takes extended investigation and can not be done immediately, briefly explain this to the customer and let them know that we will return their call asap. As a guideline, NEIF employees try to resolve issues within 24 hours.



If any of the below events occur a complaint must be logged into Compligo and if required the Investor needs to be notified:

- A customer asks to speak to a manager.
- The NEIF Employee is unable to assist the customer to the customers satisfaction.
- A customer is becoming unreasonable on the phone or through email.
- A customer lodges a complaint with any third party.

## Reporting Customer Complaints in Compligo

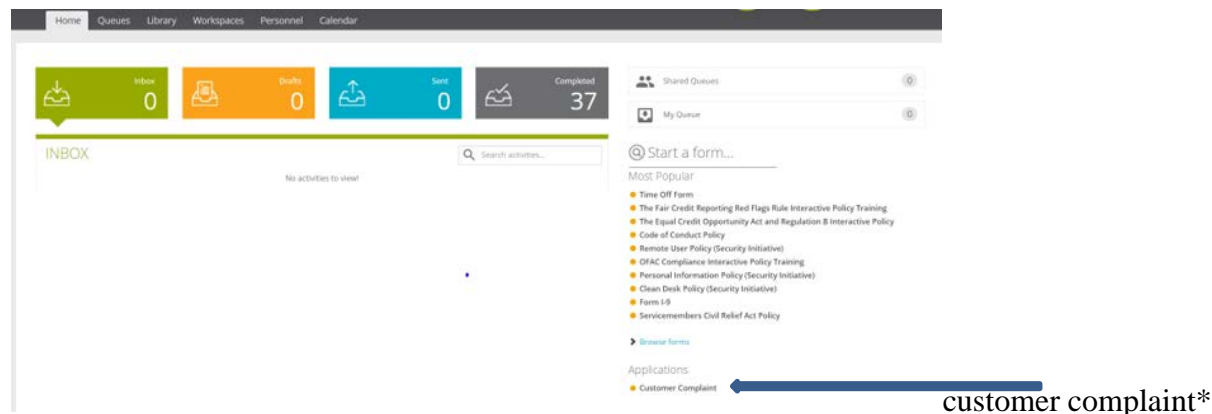
### Policy

Any complaint received by any NEIF staff member will be entered into Compligo for tracking and resolution monitoring. The Department Heads will review complaint reports to determine if there are complaint trends that indicate a need for targeted compliance training or procedural changes. Department Heads will also participate in meetings with Executive Management, during which specific complaints received from or through a federal or state regulatory agency, NEIF, the Better Business Bureau (“BBB”), or state law enforcement agencies will be reviewed. The purpose of these meetings is to determine if any of the complaints indicate a need for procedural changes or represent potential violation of consumer regulations requiring corrective action.

### Procedure

Staff person who received the complaint will take down the details of the complaint and will log into Compligo to track the issue.

On the lower right corner of the first screen, select Customer Complaint.



Then select the Type of complaint that it is and complete the intake form. Provide as much detail as possible from your discussion with the customer.



## Customer Complaint

### Complaint Details

Type *	Please select...
Priority *	Please select...
Source *	Billing
Status *	Confusing Advertising or Marketing
Investor	Contractor
Location	Credit Denial
Date *	Credit Insurance
	Credit Reporting
	Fraud
	Late Fees
	Privacy
	Sales Tactics
	Term Changes - After Closing
	Term Changes - Mid Deal
	Other

The complaints will then be reviewed by the COO and responsible Department Head.

Complaints involving loans servicing issues, such as: payments, payoffs, or collection calls, will be handled by the VP, Accounting & Servicing.

Complaints about the lending process will be handled by VP, Lending & Programs.

Complaints involving work completed by a contractor regardless of loan status, will be handled by the Business Development team. The responsible person will reach out to the contractor to get the details of the situation and will work to resolve any issues as best they can.

If the loan has already funded, the customer is still responsible for payments while the complaint is being investigated.

## Reporting

If required by Investor, monthly reporting is available to the Investor. The reporting shall include only complaints related to loans or actions related to loans owned by the Investor.

## Exhibit 5



### Disaster Recovery Plan (DRP)

#### Plan and related Business Processes

Business Process	Feature	Relevant Technical Components
<i>Residential Lending-Origination</i>	<ul style="list-style-type: none"><li>• eGT, GoldTrak, A/P</li><li>• Contractor Search</li></ul>	<ul style="list-style-type: none"><li>• GoldPoint Systems</li><li>• Energy Circle</li></ul>
<i>Loan Servicing</i>	<ul style="list-style-type: none"><li>• CIM</li></ul>	<ul style="list-style-type: none"><li>• GoldPoint Systems</li></ul>
<i>Commercial Lending</i>	<ul style="list-style-type: none"><li>• Commercial Portal</li></ul>	<ul style="list-style-type: none"><li>• Softlink</li></ul>
<i>Rebate Bridge</i>	<ul style="list-style-type: none"><li>• Intake Form</li><li>• A/P</li></ul>	<ul style="list-style-type: none"><li>• Smartsheet</li><li>• GoldPoint Systems (Funding)</li></ul>
<i>Communication</i>	<ul style="list-style-type: none"><li>• Email</li><li>• Phone System</li></ul>	<ul style="list-style-type: none"><li>• Microsoft Office 365</li><li>• eStreet VOIP</li></ul>

March 17, 2020

Table of Contents

1. Purpose and Objective ..... 3

Scope ..... 3

2. Dependencies..... 3

3. Disaster Recovery Strategies..... 5

4. Disaster Recovery Procedures ..... 5

Response Phase..... 5

Resumption Phase..... 6

Internal or External Dependency Recovery..... 6

Significant Network or Other Issue Recovery (Defined by quality of service guidelines) ..... 7

Restoration Phase ..... 7

Internal or External Dependency Recovery..... 7

Significant Network or Other Issue Recovery (Defined by quality of service guidelines) ..... 8

Appendix A: Disaster Recovery Contacts - Admin Contact List ..... 9

Appendix B: Document Maintenance Responsibilities and Revision History ..... 9

Appendix C: NEIF IT Diagrams ..... 9

Appendix D: Vendor Contacts ..... 14

Appendix E: Server Troubleshooting.....19

Appendix F: GoldPoint Contingency Plan.....20

## 1. Purpose and Objective

---

National Energy Improvement Fund, LLC (NEIF) developed this disaster recovery plan (DRP) to be used in the event of a significant disruption to the features listed in the table above and/or significant disruption to internet access. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

### Scope

---

The scope of this DRP document addresses technical recovery only in the event of a significant disruption. The intent of the DRP is to be used in conjunction with the NEIF business continuity plan (BCP). A DRP is a subset of the overall recovery process contained in the BCP. Plans for the recovery of people, infrastructure, and internal and external dependencies not directly relevant to the technical recovery outlined herein are included in the Business Continuity Plan NEIF has in place.

The BCP has been distributed to Senior Management and key personnel.

This disaster recovery plan provides:

- Guidelines for **determining plan activation**;
- Technical **response flow** and recovery strategy;
- Guidelines for **recovery procedures**;
- References to key **Business Resumption Plans** and technical dependencies;
- **Rollback procedures** that will be implemented to return to [standard operating state](#);
- **Checklists** outlining considerations for escalation, incident management, and plan activation.

The specific objectives of this disaster recovery plan are to:

- Immediately mobilize a core group of leaders to assess the technical ramifications of a situation;
- Set technical priorities for the recovery team during the recovery period;
- Minimize the impact of the disruption to the impacted features and business groups;
- Stage the restoration of operations to full processing capabilities;
- Enable rollback operations once the disruption has been resolved if determined appropriate by the recovery team.

Within the recovery procedures there are significant dependencies between and supporting technical groups within and outside NEIF. This plan is designed to identify the steps that are expected to take to coordinate with other groups / vendors to enable their own recovery. This plan is not intended to outline all the steps or recovery procedures that other departments need to take in the event of a disruption, or in the recovery from a disruption.

## 2. Dependencies

---

This section outlines the dependencies made during the development of this disaster recovery plan. If and when needed the DR TEAM will coordinate with their partner groups as needed to enable recovery.

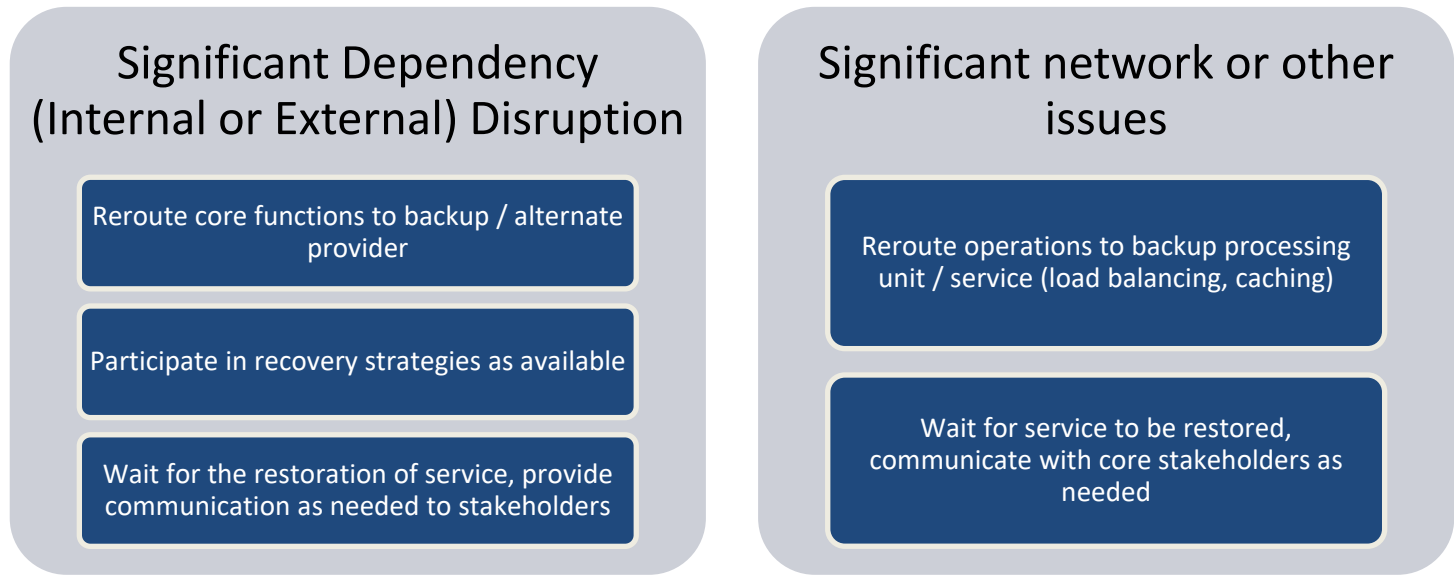


Dependency	Assumptions
<b>User Interface / Rendering</b> Presentation components	<ul style="list-style-type: none"> <li>Users (end users, power users, administrators) are unable to access the system through any part of the instance (e.g. client or server side, web interface or downloaded application).</li> <li>Infrastructure and back-end services are still assumed to be active/running.</li> </ul>
<b>Business Intelligence / Reporting</b> Processing components	<ul style="list-style-type: none"> <li>The collection, logging, filtering, and delivery of reported information to end users is not functioning (with or without the user interface layer also being impacted).</li> <li>Standard backup processes (e.g. tape backups) are not impacted, but the active / passive or mirrored processes are not functioning.</li> <li>Specific types of disruptions could include components that process, match and transforms information from the other layers. This includes business transaction processing, report processing and data parsing.</li> </ul>
<b>Network Layers</b> Infrastructure components	<ul style="list-style-type: none"> <li>Connectivity to network resources is compromised and/or significant latency issues in the network exist that result in lowered performance in other layers.</li> <li>Assumption is that terminal connections, serially attached devices and inputs are still functional.</li> </ul>
<b>Storage Layer</b> Infrastructure components	<ul style="list-style-type: none"> <li>Loss of SAN, local area storage, or other storage component.</li> </ul>
<b>Database Layer</b> Database storage components	<ul style="list-style-type: none"> <li>Data within the data stores is compromised and is either inaccessible, corrupt, or unavailable</li> </ul>
<b>Hardware/Host Layer</b> Hardware components	<ul style="list-style-type: none"> <li>Physical components are unavailable or affected by a given event</li> </ul>
<b>Virtualizations (VM's)</b> Virtual Layer	<ul style="list-style-type: none"> <li>Virtual components are unavailable</li> <li>Hardware and hosting services are accessible</li> </ul>
<b>Administration</b> Infrastructure Layer	<ul style="list-style-type: none"> <li>Support functions are disabled such as management services, backup services, and log transfer functions.</li> <li>Other services are presumed functional</li> </ul>
<b>Internal/External Dependencies</b>	<ul style="list-style-type: none"> <li>Interfaces and intersystem communications corrupt or compromised</li> </ul>

In addition, assumptions within the Business Continuity Plan for this work stream still apply.

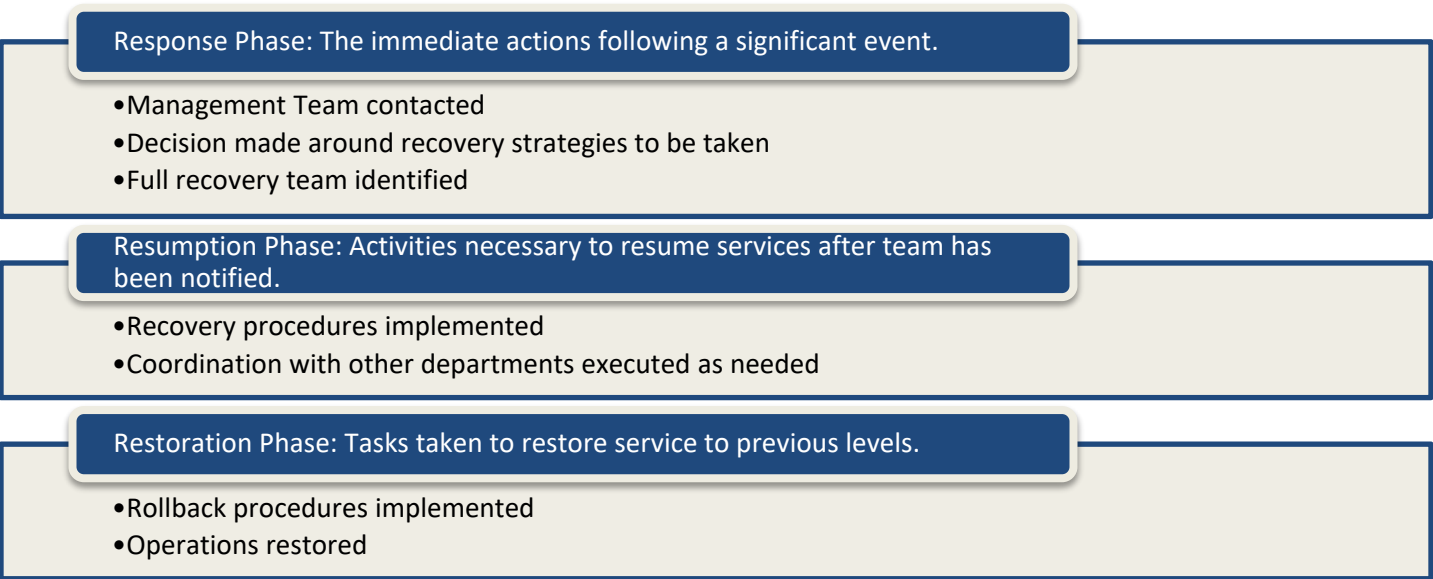
3. Disaster Recovery Strategies

The overall DR strategy of NEIF is summarized in the table below and documented in more detail in the supporting sections. These scenarios and strategies are consistent across the technical layers (user interface, reporting, etc.)



4. Disaster Recovery Procedures

A disaster recovery event can be broken out into three phases, the response, the resumption, and the restoration. These phases are also managed in parallel with any corresponding business continuity recovery procedures summarized in the business continuity plan.



Response Phase

The following are the activities, parties and items necessary for a DR response in this phase. Please note these procedures are the same regardless of the triggering event (e.g. whether caused by a Data Center disruption or other scenario).

**Response Phase Recovery Procedures – All DR Event Scenarios**

Step	Owner	Duration	Components
Identify issue, contact management / Designated Responsible Individual (DR TEAM).	DR TEAM	90 minutes	<ul style="list-style-type: none"> <li>Issue communicated / escalated</li> <li>Priority set</li> </ul>
Identify the team members needed for recovery.	DR TEAM	30 minutes	Selection of core team members required for restoration phase from among the following groups: <ul style="list-style-type: none"> <li>Operations</li> <li>Senior Management</li> </ul>
Establish a conference line for a bridge call to coordinate next steps.	DR TEAM	15 minutes	Primary bridge line: <b>Start Zoom Conference Call</b> Secondary bridge line: <b>641-715-3300; 98155</b> Alternate / backup communication tools: email, Slack
Communicate the specific recovery roles and determine which recovery strategy will be pursued.	DR TEAM	120 minutes	<ul style="list-style-type: none"> <li>Documentation / tracking of timelines and next decisions</li> <li>Creation of disaster recovery event command center / “war room” as needed</li> </ul>

This information is also summarized by feature in [Appendix A: Disaster Recovery Contacts - Admin Contact List](#).

**Resumption Phase**

During the resumption phase, the steps taken to enable recovery will vary based on the type of issue. The procedures for each recovery scenario are summarized below.

**Internal or External Dependency Recovery***Reroute operations to backup provider*

Step	Owner	Duration	Components
Reboot Server	Laura Nelson	As Needed	<ul style="list-style-type: none"> <li>Reboot to determine if connection is reestablished</li> </ul>
Work with Inova to reroute any necessary network connections.	Laura Nelson	As Needed	<ul style="list-style-type: none"> <li>Server is continually backed up to Barracuda cloud, in addition to local backup</li> </ul>
Work with Inova to reroute VPN to backup VPN.	Laura Nelson	As Needed	<ul style="list-style-type: none"> <li>In the event that a backup VPN is needed, Inova will reroute to maintain GoldPoint secure connection</li> </ul>

*Execute available recovery procedures*

Step	Owner	Duration	Components
Inform other teams about technical dependencies.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Staff will be instructed about how to proceed with software or hardware</li> </ul>
Inform stakeholders of situation and provide updated status.	DR TEAM	As Needed	<ul style="list-style-type: none"> <li>VP Lending will inform program partners as required if there will be a delay in operations.</li> </ul>

*Take no action – monitor status*

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the disruption is fully in the control of another department or vendor).

Step	Owner	Duration	Components
Track communication and status with the core recovery team.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Provide feedback about impacted service availability</li> </ul>
Send out frequent updates to core stakeholders with the status.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>VP Lending will inform program partners as required if there will be a delay in operations.</li> </ul>

### Significant Network or Other Issue Recovery (Defined by quality of service guidelines)

#### Reroute operations to backup provider

Step	Owner	Duration	Components
Work with Inova to reroute any necessary network connections.	Laura Nelson	As Needed	<ul style="list-style-type: none"> <li>Server is continually backed up to Barracuda cloud, in addition to local backup</li> </ul>
Work with Inova to reroute VPN to backup VPN.	Laura Nelson	As Needed	<ul style="list-style-type: none"> <li>In the event that a backup VPN is needed, Inova will reroute to maintain GoldPoint secure connection</li> </ul>

#### Execute available recovery procedures

Step	Owner	Duration	Components
Inform other teams about technical dependencies.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Staff will be instructed about how to proceed with software or hardware</li> </ul>
Inform stakeholders of situation and provide updated status.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>VP Lending will inform program partners as required if there will be a delay in operations.</li> </ul>

#### Take no action – monitor status

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the internal or external dependency is fully in the control of another department or vendor).

Step	Owner	Duration	Components
Track communication and status with the core recovery team.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Provide feedback about impacted service availability</li> </ul>
Send out frequent updates to core stakeholders with the status.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>VP Lending will inform program partners as required if there will be a delay in operations.</li> </ul>

### Restoration Phase

During the restoration phase, the steps taken to enable recovery will vary based on the type of issue. The procedures for each recovery scenario are summarized below.

#### Internal or External Dependency Recovery

#### Execute available recovery procedures

Step	Owner	Duration	Components
Work with external partner to restore to primary.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Ensure that all original settings are restored</li> </ul>
Work with Inova to restore to primary.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Ensure that all original settings are restored</li> </ul>
Test Connectivity.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Verify that all functionality is restored</li> </ul>
Notify stakeholders of updated status.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>VP Lending will inform program partners that normal service has resumed.</li> </ul>

### *Take no action – monitor status*

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the disruption is fully in the control of another department or vendor).

Step	Owner	Duration	Components
Track communication and status with the core recovery team.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Provide feedback about impacted service availability</li> </ul>
Test Connectivity.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Verify that all functionality has resumed</li> </ul>
Notify stakeholders of updated status.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>VP Lending will inform program partners that normal service has resumed.</li> </ul>

### *Significant Network or Other Issue Recovery (Defined by quality of service guidelines)*

#### *Execute available recovery procedures*

Step	Owner	Duration	Components
Work with Inova to restore to primary.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Ensure that all original settings are restored</li> </ul>
Test connectivity.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Verify that all functionality has resumed</li> </ul>

### *Take no action – monitor status*

This recovery procedure would only be the chosen alternative in the event no other options were available to (e.g. the cause and recovery of the internal or external dependency is fully in the control of another department or vendor).

Step	Owner	Duration	Components
Track communication and status with the core recovery team.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Provide feedback about impacted service availability</li> </ul>
Test Connectivity.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>Verify that all functionality has resumed</li> </ul>
Send out frequent updates to core stakeholders with the status.	DR TEAM	As needed	<ul style="list-style-type: none"> <li>VP Lending will inform program partners that normal service has resumed.</li> </ul>

## Appendix A: Disaster Recovery Contacts - Admin Contact List

---

For the key internal and external dependencies identified, the following are the primary contacts.

Dependency Name	Contact Information
GoldPoint	Laura Nelson
Commercial Portal	Matthew Brown
Contractor Search	Laura Nelson
eStreet Phone System	Joanne Hartman
Smartsheet	Heather Braithwaite
Server, Internet	Laura Nelson to Inova

In addition the key BCP individuals are:

- Joanne Hartman, Business Manager
- Teri Stoffey, Loan Servicing, Reporting, Accounting
- Tessa Shin, Residential Lending Operations
- Heather Braithwaite, Commercial Lending Operations and Rebate Bridge
- Peter Krajsa, Business Development

## Appendix B: Document Maintenance Responsibilities and Revision History

---

This section identifies the individuals and their roles and responsibilities for maintaining this Disaster Recovery Plan.

**Primary Disaster Recovery Plan document owner is: Laura Nelson**

Primary Designee: Joanne Hartman

Alternate Designee: Teri Stoffey

Name of Person Updating Document	Date	Update Description	Version #	Approved By

## Appendix C: NEIF IT Diagrams

---

## Appendix D: Glossary/Terms

---

**Standard Operating State:** Production state where services are functioning at standard state levels. In contrast to recovery state operating levels, this can support business functions at minimum but deprecated levels.

**Presentation Layer:** Layer which users interact with. This typically encompasses systems that support the UI, manage rendering, and captures user interactions. User responses are parsed and system requests are passed for processing and data retrieval to the appropriate layer.

**Processing Layer:** System layer which processes and synthesizes user input, data output, and transactional operations within an application stack. Typically this layer processes data from the other layers. Typically these services are folded into the presentation and database layer, however for intensive applications; this is usually broken out into its own layer.

**Database Layer:** The database layer is where data typically resides in an application stack. Typically data is stored in a relational database such as SQL Server, Microsoft Access, or Oracle, but it can be stored as XML, raw data, or tables. This layer typically is optimized for data querying, processing and retrieval.

**Network Layer:** The network layer is responsible for directing and managing traffic between physical hosts. It is typically an infrastructure layer and is usually outside the purview of most business units. This layer usually supports load balancing, geo-redundancy, and clustering.

**Storage Layer:** This is typically an infrastructure layer and provides data storage and access. In most environments this is usually regarded as SAN or NAS storage.

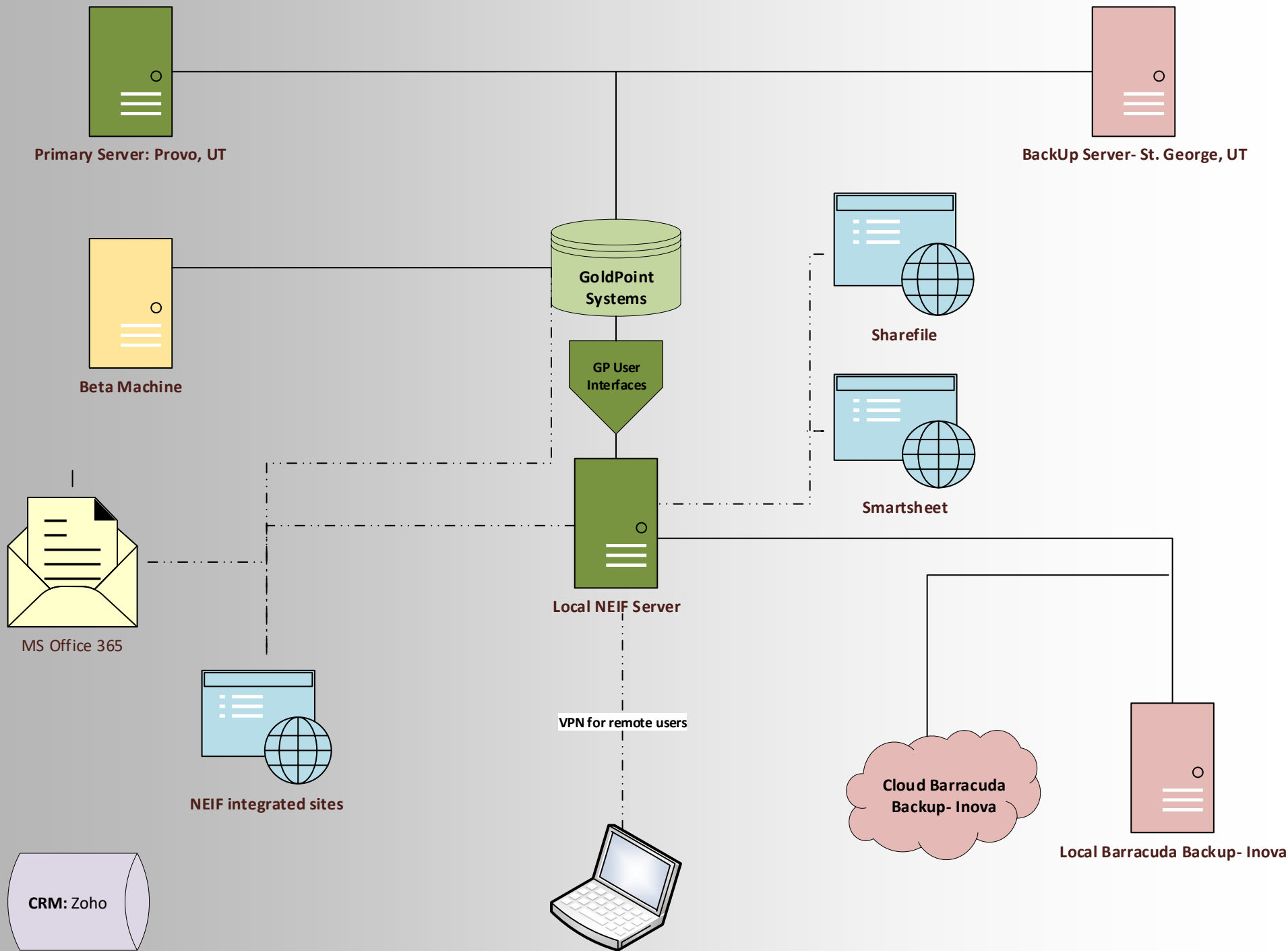
**Hardware/Host Layer:** This layer refers to the physical machines that all other layers are reliant upon. Depending on the organization, management of the physical layer can be performed by the stack owner or the purview of an infrastructure support group.

**Virtualization Layer:** In some environments virtual machines (VM's) are used to partition/encapsulate a machine's resources to behave as separate distinct hosts. The virtualization layer refers to these virtual machines.

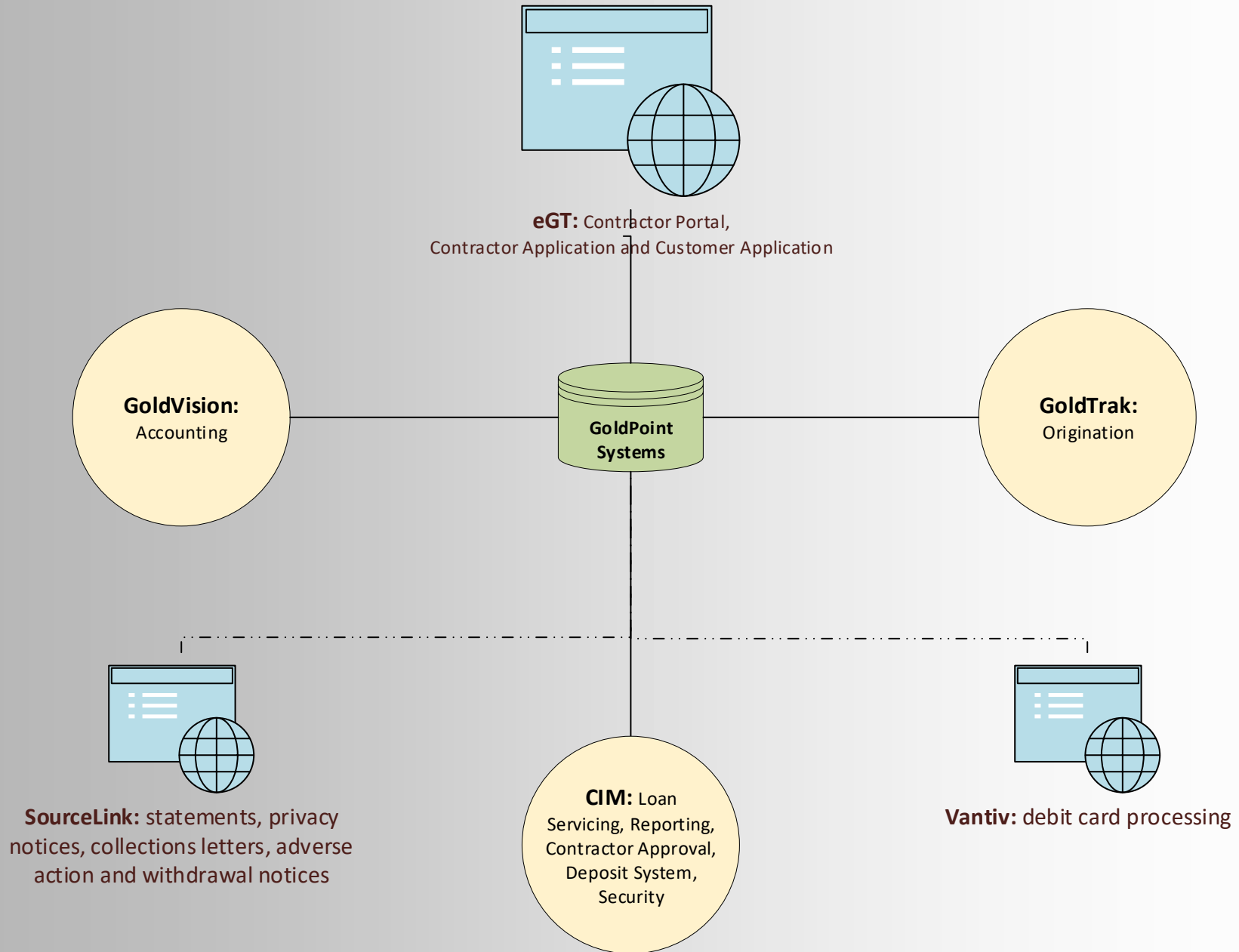
**Administrative Layer:** The administrative layer encompasses the supporting technology components which provide access, administration, backups, and monitoring of the other layers.

# NEIF Systems

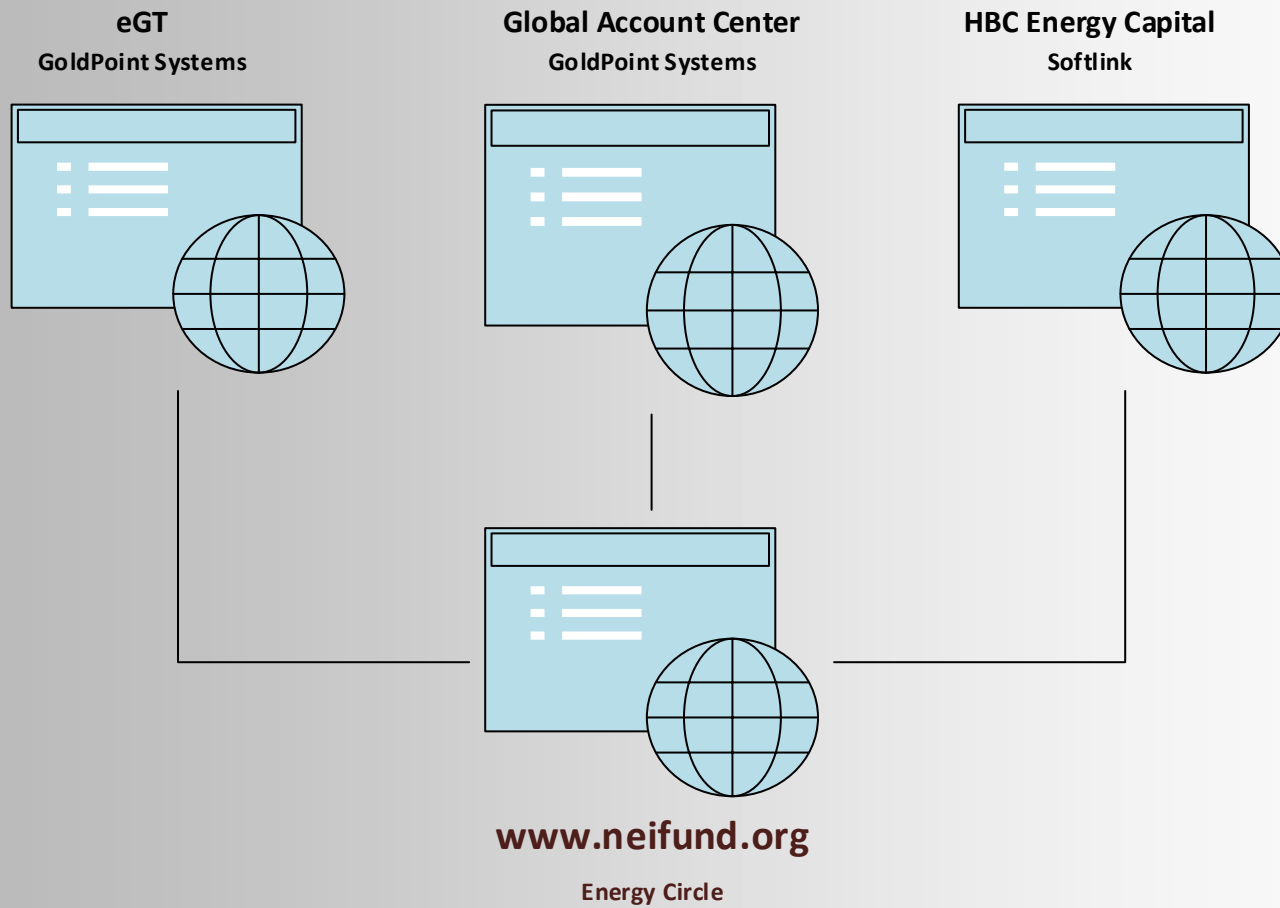
Att. A: Loan Origination & Servicing Agrmnt. by & Between NEIF & MCE







## NEIF Integrated Websites



## NEIF Third Party Tools/Resources

- CreditSafe- contractor and commercial credit
- DocMagic- secured lending
- TransUnion- residential credit
- NMLS- licensing
- ADP- payroll/HR
- SourceLink- statement/letter generation
- Vantiv- debit card processing
- Firsttrust- banking
- CT Corp- licensing
- Compligo- compliance

### GoldPoint Contact Information

Account Manager: Jordan Biesinger  
[jbiesinger@goldpointsystems.com](mailto:jbiesinger@goldpointsystems.com)  
801-344-6712

Customer Service/After Hours: 888-477-0099

Transmissions: Corey Jones  
801-376-1917

GoldTrak/eGT: GPS Account Manager 3  
[gpsam3@goldpointsystems.com](mailto:gpsam3@goldpointsystems.com)

Customer Service Team Manager: Shelcy Barrett  
[shelcyb@goldpointsystems.com](mailto:shelcyb@goldpointsystems.com)

24 hour on call numbers:

Loan Servicing – 801-369-6141

Origination – 801-361-5303

On Call escalation – 801-319-5456

## Appendix D: Vendor Contacts

### **eStreet Contact Information**

As Office Manager, Joanne has been communicating all phone related items to eStreet.

All support issues should be EMAILED to eStreet: [support@estreet.com](mailto:support@estreet.com)

Our representative is Bill Brownrigg:

**Email:** [bbrownrigg@estreet.com](mailto:bbrownrigg@estreet.com)

**Phone:** 303-584-0640 ext:1017 or 877-ESTREET

**Inova Contact Information**

Dave Shafinsky: 610-248-3818 Cell

**Main Number**/Bob Trump: 610-440-0708

Robb Piotrowski: 610-248-3436 Cell

1320 Hausman Road  
Suite 201  
Allentown, PA 18014

[www.inovatechs.com](http://www.inovatechs.com)

## Key Resources

- Sign Up for Live Trainings: <https://www.sharefile.com/resources/events/>
- Knowledge Base: <https://www.sharefile.com/support>
- ShareFile Technical Support: 24/7 Call 800-441-3453

**SOFTLINK LLC Emergency /Support\*\*\* Contact List for HBC\*.softlink.solutions**

<b>Name</b>	<b>Company</b>	<b>Preferred Contact Method</b>	<b>Preferred Phone/Text</b>	<b>Email</b>	<b>Address</b>	<b>Primary Contact For</b>
Diane Novak	Softlink	Text / Phone / Email	(714) 308-2202	dnovak@softlinkdev.com	163 Balboa Drive, Palm Springs, CA 92264	First contact for ALL issues
Tom Seeds	Softlink	Text / Email	(541) 891-1286	t_seeds@hotmail.com		Secondary contact for ALL issues
Jorge Fuentes	Softlink Developer	Text / Email	(714) 450-0283	jfsicairos@gmail.com		Site Performance / Availability Issues; contact if 1st 2 contacts are on scheduled absence or do not respond within reasonable time
Juan Carlos Garibaldi	Softlink Developer	Text / Email	(714) 726-2743	jcggaribaldi@gmail.com		
Alfonso Moran	Database Backup	Text / Email	(714) 240-2757	alfonsomoran@me.com alfonso@dividendfinance.com		General Emergency Contact
Chris Kirkwood	SoCalData Center	Text / Email / Phone	(714) 580-9199	chris@socaldata.com	<a href="http://www.socaldata.com/">http://www.socaldata.com/</a>	Contact as Last Resort if all other contact attempts fails; Site Availability / Data Recovery Issues
John Gamma	SoCalData Center	Email	800-244-9420	john@socaldata.com		

\*\*\*

Alert Levels:  
(Include in critical, emergency communications)

**1** = Production Site is inaccessible or significant loss of data; requires immediate response

**2** = Critical Issue requires attention within 4 hours

**3** = Critical Issue requires attention within 24 hours

**4** = Non-critical issue request call back within 24-48 hours

**5** = Non-critical issue request callback at earliest convenience



## Appendix E:

### Server Troubleshooting

If you experience issues with internet, network, phones or GoldPoint connectivity, you will need to start by checking the server to see if it is on. The internet connects to our server- so without server power, the internet, network and phones will not work.

1. If server is on, but needs to be rebooted:
  - a. Notify staff to save their work and let them know that you will be rebooting the server
  - b. Log into server with the NEIF/Administrator user id (this is the user id that comes up with the machine- DO NOT USE YOUR OWN LOGIN)
    - i. Password is: !Novatech5
  - c. Select Shut Down when you click Power
  - d. Allow Server to shut down- this may take a few minutes
  - e. Once it appears to be shut down, wait 30 seconds
  - f. Open the cover on the server machine by moving the key (on top) to the unlock position and gently lower the cover
  - g. Press the Power Button (it may be orange) on upper right
  - h. Power Button will turn green and start the power up process (this will take a few minutes)
  - i. You can verify that everything is up and running by logging back into the server, but you don't necessarily need to do this.
    - i. There may be messages about Windows Updates on the screen. Ignore these- DO NOT DO THE UPDATES... Inova handles these updates for us once a month.
2. If the server is off:
  - a. Open the cover on the server machine by moving the key (on top) to the unlock position and gently lower the cover
  - b. Press the Power Button (it may be orange) on upper right
  - c. Power Button will turn green and start the power up process (this will take a few minutes)
  - d. You can verify that everything is up and running by logging back into the server, but you don't necessarily need to do this.
    - i. There may be messages about Windows Updates on the screen. Ignore these- DO NOT DO THE UPDATES... Inova handles these updates for us once a month.

If rebooting the server does not resolve an internet or network connectivity issue, call Inova to help troubleshoot- see Inova contact sheet for phone numbers.

If the server is rebooted and we have internet and network connectivity, but you have a GoldPoint connectivity issue, call GoldPoint for assistance. See the GoldPoint contact sheet for phone numbers.

If the server is working and you can access the internet, but the phones are not working, you need to reach out to eStreet Support to resolve. See eStreet contact sheet.

# **Contingency Plan**

**DHI Computing Service, Inc.  
June 2018**

**Emergency Notification and Voice Mail Number: 801-602-1671**

**This page intentionally left blank.**

## Contingency Plan

Version 18.0

June 2018

Effective: June 2018

Expires: July 2019

DHI Computing Service, Inc.  
1525 West 820 North  
Provo, Utah 84601

---

## Release Information

This manual contains the current DHI contingency plan for events that could interrupt the normal flow of business. This plan is often referred to as a disaster recovery plan and is referenced hereafter as "the plan." The plan is updated annually and you should verify that you have the most current release before making decisions based upon this plan. When the plan is updated it is automatically distributed to the list contained in Appendix J. Changes to or comments about this document should be forwarded to the DHI Internal Services department.

## Security Notice

This document contains the policy, plans, and functions implemented at DHI as a contingency against events that would adversely affect DHI, its employees, or its clients. The material contained in this document and the procedures contained in this plan constitute unpublished trade secrets which belong to DHI Computing Service, Inc. **Any distribution or use of this information or the concepts and procedures discussed in this document, except as authorized in writing by DHI, is prohibited.** In order to track copies of the plan, each copy is individually numbered and distribution is limited to authorized personnel. NO ADDITIONAL COPIES of any numbered copy of the plan may be made for any reason. Requests for additional copies of the plan should be made to the executive vice president of the department responsible for the business function where the additional copy of the plan is required. Copies of the plan are made and controlled by the Emergency Services Coordinator. The plan will be updated at least once every 12 months. ANY COPY of the plan that is more than 14 months old will contain outdated information, and should be destroyed or returned to DHI to avoid the problems that occur when obsolete material is used to make decisions.

## TABLE OF CONTENTS

---

<b>CHAPTER 1</b>	<b>INTRODUCTION, OBJECTIVES, and OVERVIEW</b>	
	1.1 Objectives .....	1-1
	1.2 Audit Notes .....	1-2
	1.3 Policy Statement.....	1-2
	1.4 Overview of the Plan .....	1-2
	1.5 The Disaster Recovery Scenario.....	1-4
<b>CHAPTER 2</b>	<b>THE CONTINGENCY TEAM</b>	
	2.1 Purpose .....	2-1
	2.2 Organization and Planning .....	2-1
	2.3 Emergency Coordinator.....	2-3
	2.4 Alternate Emergency Coordinator .....	2-3
	2.5 Offsite Emergency Coordinator and Alternate.....	2-4
	2.6 The Use of Emergency Action Teams.....	2-4
	2.7 Emergency Control Center.....	2-5
<b>CHAPTER 3</b>	<b>MAJOR FUNCTIONS AND KEY CONSIDERATIONS</b>	
	Each section contains: description, policy, schedule, responsible departments, hardware requirements, network considerations, additional considerations, and expected recovery time.	
	3.1 Online Client Processing .....	3-1
	3.2 Afterhours Processing .....	3-2
	3.3 Dairy Batch Processing .....	3-3
	3.4 Programming Support and Development .....	3-4
<b>CHAPTER 4</b>	<b>GENERAL PROCEDURES FOR POTENTIAL INTERRUPTIONS</b>	
	4.1 Fires.....	4-1
	4.2 Electrical Power Outages .....	4-5
	4.3 Telecommunications Failures.....	4-6
	4.4 Flooding .....	4-6
	4.5 Building Alarm System Procedures.....	4-8
	4.6 Equipment Failures.....	4-9
	4.7 Major Disasters.....	4-9
	4.8 Pandemic.....	4-10
<b>CHAPTER 5</b>	<b>POLICIES FOR REDUCING RISKS</b>	
	5.1 Protection of Personal, Data and Software Files, and Hardware.....	5-1
	5.2 Protection of Server Computer Data .....	5-1
	5.3 Protection of Personal System Data .....	5-1
	5.4 Protection of Business Operations .....	5-2
	5.4.1 Importance of Security.....	5-2
	5.4.2 Physical Security .....	5-2
	5.4.3 Computer Access Security .....	5-2
	5.4.4 Security of Personnel .....	5-5
	5.5 Protection of Vital Records.....	5-5
	5.6 Supplies, & Documentation .....	5-5

---

5.7 Insurance .....	5-6
<b>CHAPTER 6    CONTINGENCY SITE DESCRIPTION</b>	
6.1 Location and Contacts .....	6-1
6.2 Equipment Configuration and Facilities .....	6-1
6.3 Scheduling Considerations .....	6-1
<b>CHAPTER 7    RECOVERY PROCEDURES FOR A MAJOR DISASTER</b>	
7.1 Emergency Action Teams and Responsibilities .....	7-1
7.1.1 Business Operations Team .....	7-1
7.1.2 Data Processing Applications Team .....	7-3
7.1.3 Equipment Team .....	7-4
7.1.4 Facilities Team .....	7-5
7.1.5 Administrative Team .....	7-5
7.1.6 Communications and Logistics Team .....	7-6
7.1.7 Web Server Recovery Team .....	7-6
7.2 Disaster Recovery Critical Timeline .....	7-7
7.2.1 Notification of Contingency Team .....	7-7
7.2.2 Initial Contingency Team Procedures .....	7-8
7.2.3 Activation of the Emergency Control Center .....	7-9
7.2.4 Notification of Action Teams and Top Management .....	7-10
7.2.5 Notification of Offsite Storage and Contingency Sites .....	7-11
7.2.6 Summary of Procedures for Contingency Operations .....	7-11
7.3 Specific Procedures for Contingency Operations .....	7-12
7.3.1 Initial Procedures .....	7-12
7.3.2 Coordination of DP/User Interfaces by Applications Team .....	7-14
7.3.3 Normalizing Procedures .....	7-16
7.3.4 Equipment Salvage or Replacement by Equipment Team .....	7-16
7.3.5 Facilities Salvage or Replacement by Facilities Team .....	7-16
7.3.6 Administrative Coordination by Administrative Team .....	7-16
7.4 Specific Procedures for Functional Operations .....	7-16
7.4.1 NCC Alternate Site Procedures .....	7-17
7.4.2 Support Console Installation .....	7-18
7.4.3 Specific Procedures for Setup of Recovery Systems .....	7-18
7.4.4 Procedures to Acquire Supplies at Remote Site .....	7-19
7.5 Procedures for Replacement of Business Facility .....	7-20
7.6 Procedures for Return to Normal Operations .....	7-21
<b>CHAPTER 8    TESTING AND MAINTENANCE OF THE PLAN</b>	
8.1 Policies and Procedures for Testing .....	8-1
8.2 Policies and Procedures for Review and Update .....	8-2
<b>CHAPTER 9    CLIENT DEMONSTRATION AND CERTIFICATION OF READINESS</b>	
9.1 Level 0 - Not Certified .....	9-2
9.2 Level 1 - Remote Network Recovery .....	9-2
9.3 Level 2 - Basic Network Recovery .....	9-3
9.4 Level 3 - Full Network Recovery .....	9-3
9.5 Level 4 - Business Recovery Partner .....	9-3
<b>APPENDIX A    EMERGENCY NOTIFICATION</b>	
Service Numbers .....	A-1
Contingency Team .....	A-1

---

Emergency Action Team Lists ..... A-2

Top Management Notification List..... A-3

Management Succession List..... A-4

Contingency Site ..... A-4

DHI Computing Service Cellular Phones (DHI Only).....A-5

Employees With Remote Access (DHI Only).....A-6

**APPENDIX B DHI COMPUTING SERVICE ORGANIZATION CHART**

**APPENDIX C DHI EMPLOYEE ADDRESS BOOK (DHI ONLY)**

**APPENDIX D CUSTOMER CONTACT LISTS (DHI ONLY)**

**APPENDIX E VENDOR CONTACTS**

**APPENDIX F EQUIPMENT CONFIGURATION – ALTERNATE SITE**

**APPENDIX G EQUIPMENT CONFIGURATION – PROVO SITE**

**APPENDIX H SOFTWARE CONFIGURATION**

**APPENDIX I FLOOR AND EQUIPMENT LAYOUTS**

**APPENDIX J DISTRIBUTION LIST FOR THE CONTINGENCY PLAN**

**APPENDIX K CERTIFICATION OF ANNUAL REVIEW**

**APPENDIX L VOICEMAIL INSTRUCTIONS (DHI ONLY)**

**APPENDIX M ALTERNATIVE SITE DIRECTIONS (DHI ONLY)**

**APPENDIX N DISASTER RECOVERY DEPLOYMENT CHECKLIST (DHI ONLY)**



**This page intentionally left blank.**

## CHAPTER 1 INTRODUCTION, OBJECTIVES, AND OVERVIEW

This manual contains the CONTINGENCY OPERATIONS PLAN for:

**DHI Computing Service, Inc.**  
**1525 West 820 North**  
**Provo, Utah 84601**

Mission:	The mission of DHI Computing Service is to provide quality data processing services and software to our clients and to maintain a secure, satisfying and rewarding working environment for our employees.
Mission of Plan:	The mission of the contingency plan is to define procedures and implement strategies that will allow our clients to continue their business operations when operations at DHI have been interrupted.
Department:	The Internal Services group, which is responsible for the corporate computer operations at DHI, leads the contingency planning and implementation process. Each individual department (FPS GOLD Financial Processing, GOLDPoint Systems Financial Processing, Amelcor Dairy Processing, and PCIS GOLD Medical Records Processing) is responsible for the departmental specific planning to support specialized operations that may be required in addition to this plan. In addition, the planning for contingency in each client location is the responsibility of that client.
Primary Operations:	DHI Computing Service serves several different industry segments. The standard for recovery in all environments is complete restoration of all customer-related server operations. DHI has placed strong emphasis on online real-time operations throughout all application areas. The contingency plan supports this online philosophy by emphasizing the timely restoration of teleprocessing operations in all disaster situations.

### 1.1 Objectives

The primary objective of the plan is to help ensure the continued operation of our business by providing the ability to successfully recover business functions in the event of a disaster or temporary emergency.

Specific goals of the plan relative to an emergency include:

- 1) To detail the correct course of action to follow
- 2) To minimize confusion, errors, and expense to the company
- 3) To coordinate recovery with our clients in advance
- 4) To affect a quick and complete recovery of business operations.

Secondary objectives of this plan are:

- 1) To reduce the risk of loss of business functions
- 2) To provide ongoing protection of company assets
- 3) To allow our clients to plan
- 4) To ensure the continued viability of this plan.

---

## 1.2 Audit Notes

Auditors should examine each department's compliance with the requirements of this plan. Departmental records should reflect information related to ongoing training, familiarity with the plan, and involvement with the tests of the plan. It is DHI's policy that the plan and its implementation be reviewed periodically by the internal audit staff. The internal audit staff then reports on the readiness of the participating departments, as well as the corporation as a unit, to the Board of Directors.

Auditors of client institutions should review client procedures and plans that define and implement contingency plans for each client site. Contingency planning is a cooperative effort on the part of both the service bureau and the client. Complete recovery from the complex and varied events that may occur can only be accomplished by the implementation of complete plans by both the service bureau and the client. DHI will provide a list of clients that have certified their recovery capabilities according to the requirements in Chapter 9.

## 1.3 Policy Statement

Management personnel of the company are responsible for protecting all assets of our organization. These assets include employees, physical property, information, and records relating to the conduct of the business. As a service bureau, DHI also holds in trust, information assets that belong to our clients. These assets in trust are treated just as the assets of our own organization.

The Board of Directors is responsible to approve this Contingency Plan prior to distribution of the Plan every year.

Management personnel are specifically responsible for:

- Identifying and protecting all assets within their assigned areas of control.
- Ensuring that all employees understand their obligation to protect the organization's assets.
- Implementing and observing security practices and procedures that are consistent with generally accepted practice and within the specific guidelines stated in this Contingency Plan.
- Noting any variance from established security practices and initiating corrective action.
- Assigning responsibilities for establishing, maintaining, coordinating, and testing the Contingency Plan.
- Training their employees about the Contingency Plan and its procedures. Departmental managers are responsible for all training and implementation of the Contingency Plan within their departments. Internal Services personnel are available to assist but are not responsible for the training of individual departments.

## 1.4 Overview of the Plan

This contingency plan is a comprehensive document. The plan contains the necessary instructions, policies, organization, and information required for our company to be prepared for an emergency that would have an impact on our business operations. The plan consists of nine chapters:

Chapter 1 - Introduction, Objectives, and Overview  
Chapter 2 - The Contingency Team  
Chapter 3 - Major Functions and Key Considerations

---

Chapter 4 - General Procedures for Potential Interruptions  
Chapter 5 - Policies for Reducing Risks  
Chapter 6 - Contingency Site Description  
Chapter 7 - Recovery Procedures for a Major Disaster  
Chapter 8 - Testing and Maintenance of the Plan  
Chapter 9 - Client Demonstration and Certification of Readiness

The following is a brief description of each of the following eight chapters of the plan:

#### CHAPTER 2 - THE CONTINGENCY TEAM

Described in this section is the establishment of an organization of personnel known as the Contingency team. This team is responsible for constructing and maintaining the contingency plan, regular testing of the plan, managing the disaster recovery activities, and maintaining the continued viability of the plan.

#### CHAPTER 3 - MAJOR FUNCTIONS AND KEY CONSIDERATIONS

This section includes descriptions of the critical business functions, products, and key considerations such as equipment configurations, work schedules, and processing priorities.

#### CHAPTER 4 - GENERAL PROCEDURES FOR POTENTIAL INTERRUPTIONS

Potential, non-major interruptions of service are described, and general instructions for handling each type of interruption are provided. Typical interruptions include fire, power outage, and telecommunications failure.

#### CHAPTER 5 - POLICIES FOR REDUCING RISKS

Included in this section are policies designed to reduce risks (1) of disasters occurring, (2) of excessive damage when they do occur, and (3) of failing to recover from a disaster.

#### CHAPTER 6 - CONTINGENCY SITE DESCRIPTION

Alternate site for business operations is identified. This section includes a description of the facilities provided and all requirements associated with the use of the site. This section will also include a description of an Emergency Control Center gathering site for employees to access the contingency site from.

#### CHAPTER 7 - RECOVERY PROCEDURES FOR A MAJOR DISASTER

Instructions and procedures to be followed in the event of a major disaster are described in this section. Included are activation of emergency procedures, establishment of business operations at the contingency site, and subsequent restoration of normal operations. Included is a general timeline of the recovery process.

#### CHAPTER 8 - TESTING AND MAINTENANCE OF THE PLAN

This section contains the policies and procedures needed to ensure that the plan remains viable as the business environment evolves.

#### CHAPTER 9 - CLIENT DEMONSTRATION AND CERTIFICATION OF READINESS

This section contains the policies and procedures used by DHI and our clients to demonstrate and certify readiness under the plan.

## 1.5 The Disaster Recovery Scenario

The scenario for recovery following a disaster involves three "phases": (1) the initial response of the management team, (2) implementation of contingency plans, and (3) restoration of normal operations. Although the three phases occur in every recovery situation, the tasks and the people involved vary according to the nature of the emergency and its severity.

Following are three example disaster recovery sequences that are helpful for understanding the steps involved in recovering from a disaster. The three examples also illustrate some of the differences in recovery steps and elapsed times for emergencies of minor, moderate, and major severity.

### EXAMPLE #1 - PARTIAL INTERRUPTION OF BUSINESS OPERATIONS

DISASTER RECOVERY SEQUENCE	Elapsed Time After Failure
INTERRUPTION OF SERVICE (Example - telecommunications equipment failure affecting several clients)	0 hour
RECOVERY PHASE 1	
Initial response of operations management:	
• Problem/repair alternatives evaluated	.2 hours
• Interruption of service assessed	.2 hours
• Decision to implement contingency actions	.3 hours
RECOVERY PHASE 2	
Contingency plans implemented:	
• Customer service for affected users notified	.3 hours
• Customers allowed to use alternate backup connections if they desire	.3 hours
• The work/processing schedule adjusted for the delay (overtime authorized)	.5 hours
RECOVERY PHASE 3	
Normal telecommunications service restored:	
• Equipment repaired	2 hours
• Affected users notified	2 hours
• Normal telecommunications restored (clients return to normal connection usage)	2 hours

**EXAMPLE #2 - MAJOR FAILURE BUT FACILITY INTACT**

DISASTER RECOVERY SEQUENCE	Elapsed Time After Failure
MAJOR FAILURE OF SERVICE (Example - telephone company's Provo central office destroyed by fire)	0 hour
RECOVERY PHASE 1	
Initial response of Contingency team:	
• Contingency team notified and assembled	1 hour
• Interruption of service assessed	1.5 hours
• Decision to implement contingency plans	2 hours
RECOVERY PHASE 2	
Contingency plans implemented:	
• Emergency Control Center activated	2 hours
• Select Emergency Action Teams notified and assembled	2 hours
• Supplies, documentation, and other needed materials assembled	2-4 hours
• Prepare contingency equipment for operation	4+recovery time hours
• Recover any lost work in progress	4+recovery time hours
• Resume business operations on a contingency basis.	4+recovery time hours
RECOVERY PHASE 3	
Business Operations Restored:	
• Problem resolved at facility	5 days
• Functional operation tested	5 days
• Operations transferred back to facility	5-6 days
• Operations normalized	5-6 days

**EXAMPLE #3 - BUSINESS FACILITY DESTROYED**

DISASTER RECOVERY SEQUENCE	Elapsed Time After Disaster
----------------------------	--------------------------------

MAJOR DISASTER AFFECTING FACILITY (Example - major fire destroys facility)	0 hour
---	--------

**RECOVERY PHASE 1**

## Initial Response of Contingency team:

- |   |           |
|---|-----------|
| • Contingency team notified and assembled | 1 hour    |
| • Damage assessed                         | 1.5 hours |
| • Decision to implement contingency plans | 2 hours   |

**RECOVERY PHASE 2**

## Contingency plans implemented:

- |   |                       |
|---|-----------------------|
| • Emergency Control Center activated                            | 2 hours               |
| • Select Emergency Action Teams notified and assembled          | 2 hours               |
| • Supplies, documentation, and other needed materials assembled | 2-4 hours             |
| • Prepare contingency equipment for operation                   | 4+recovery time hours |
| • Recover any lost work in progress                             | 4+recovery time hours |
| • Resume business operations on a contingency basis.            | 4+recovery time hours |

**RECOVERY PHASE 3**

## Replacement Business Facility Made Operational:

- |   |            |
|---|------------|
| • New facilities established - replacing Home Site        | 3-8 months |
| • New equipment obtained and installed - At Home Site     | 3-8 months |
| • New facility tested and made operational - At Home Site | 4-9 months |
| • Operations transferred to Home Site                     | 4-9 months |
| • Business operations normalized                          | 4-9 months |

## CHAPTER 2 THE CONTINGENCY TEAM

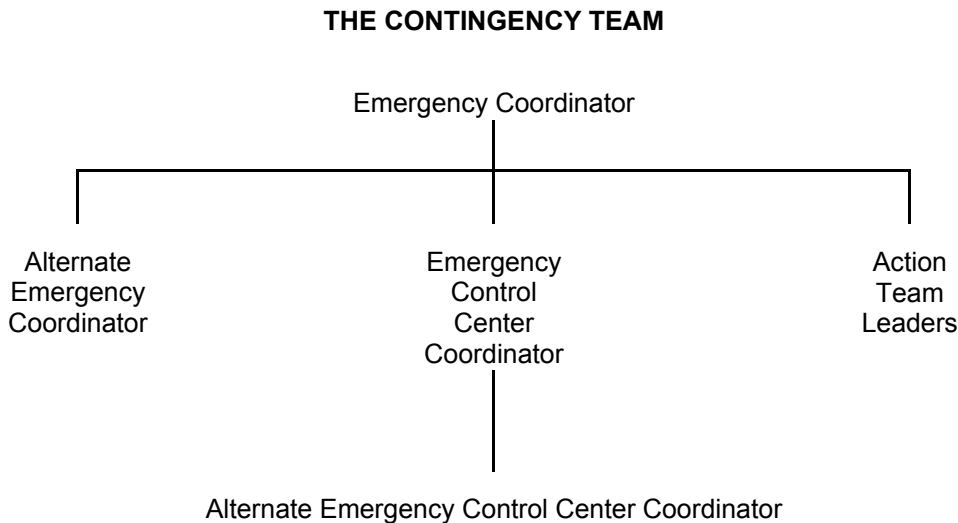
### 2.1 Purpose

The purpose of the Contingency team is to establish and direct plans of action to be followed during an interruption or cessation of business operations caused by a disaster or lesser emergency. As the name implies, the Contingency team maintains readiness for emergencies by means of the contingency plan. The Contingency team is also responsible for managing the recovery activities following a disaster, and can be thought of as the "disaster management team." Through the contingency plans, the Contingency team will provide for:

- 1) The safety of personnel
- 2) The protection of property
- 3) The continuation of business operations

### 2.2 Organization and Planning

The Contingency team consists of an Emergency Coordinator, an Alternate Emergency Coordinator, an Emergency Control Center Coordinator and alternate, the Action Team Leaders, and any other designated individuals. The list of designated members of the Contingency team, showing names and functions, is provided in Appendix A - Emergency Notification (Contingency team). The Contingency team reports to the Executive Vice President of Internal Services.

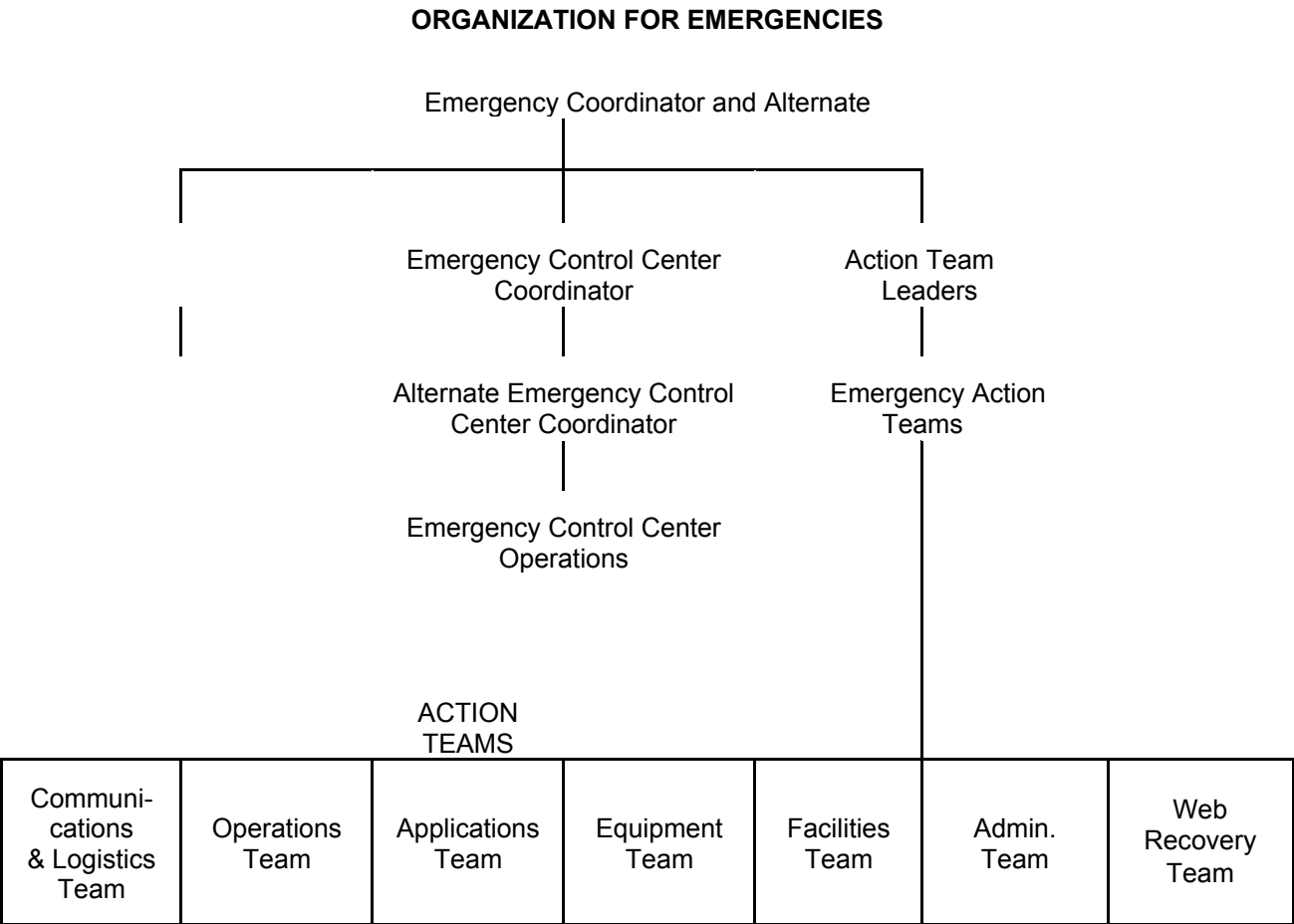




The responsibilities of individuals assigned to the Contingency team are in addition to their regular assignments and are made on the basis of familiarity with business and application systems and competence in their respective areas or specialties.

The plan is administered by the Emergency Coordinator and the Alternate Emergency Coordinator. Emergency Action Teams are used to facilitate the response to various types of emergency situations. An Emergency Control Center Coordinator and alternate are designated for disasters requiring offsite operations at an agreed upon site.

The responsibilities of the Coordinators, the functions of Emergency Action Teams and team leaders, and the purpose of the Emergency Control Center are discussed in the following sub-sections. The overall organization for the management of emergencies is illustrated by the following diagram.



---

## 2.3 Emergency Coordinator

The Emergency Coordinator is responsible for developing and coordinating the Contingency team. During an emergency, the Emergency Coordinator will activate and then direct all activities until the emergency is under control. In the absence of the Coordinator, the Alternate Emergency Coordinator will assume his duties. Additionally, the Coordinator is responsible for the following:

- 1) Reviewing, evaluating, and updating the contingency plan at least annually to assure that all emergency situations have been adequately considered and that appropriate contingency plans have been prepared. The coordinator will also ensure that the plan is updated to reflect new installations of hardware, changes in configuration or additional applications that must be recovered.
- 2) Ensuring that the emergency teams and other employees receive proper training in emergency plans and procedures. This will routinely be done as a part of annual (or more frequent) tests of the plan. The coordinator will also ensure that new employees are properly trained by their managers and that certain emergency procedures are reviewed as frequently as necessary.
- 3) Conducting meetings with the Alternate Coordinator, the Control Center Coordinator, and the Emergency Action Teams as necessary.
- 4) Keeping all members of the Contingency team fully briefed on all aspects of the disaster plan.
- 5) Evaluating the readiness and proficiency of each Emergency Action Team and the appropriateness of their assignments.
- 6) Keeping management informed of the status of the Contingency team and the Disaster Recovery plan.
- 7) Communicating the status of emergency situations to management promptly and efficiently.
- 8) Monitoring all tests of the Disaster Recovery plan, and recording the progress, problems, and successes.
- 9) Direct the proper distribution of the Contingency Plan document.

The designated Emergency Coordinator is identified in Appendix A - Emergency Notification (Contingency team).

## 2.4 Alternate Emergency Coordinator

In the absence of the Emergency Coordinator, his duties will be assumed by the Alternate Emergency Coordinator. The following additional duties are assigned to the Alternate Coordinator:

- 1) Directing the activation of the Emergency Control Center and administering the Emergency Control Center itself during an emergency.
- 2) Assisting the Emergency Coordinator in maintaining an up-to-date contingency plan and other emergency procedures, and in directing proper distribution of the plans.

- 
- 3) Providing emergency evacuation programs and posting them on bulletin boards or otherwise distributing them to all personnel.
  - 4) Maintaining up-to-date listings of Emergency Control Center Coordinators, Emergency Action Team members, and emergency telephone numbers.
  - 5) Maintaining liaison with local fire and police agencies, other company locations, and other involved parties as appropriate.

The designated Alternate Emergency Coordinator is identified in Appendix A - Emergency Notification (Contingency team).

## **2.5 Emergency Control Center Coordinator and Alternate**

The Emergency Control Center Coordinator and Alternate are responsible to help establish and maintain written plans to be followed during emergency situations requiring operation at our contingency site. During such an emergency, the Emergency Control Center Coordinator will be responsible to direct operations at the Emergency Control Center location. In the absence of the Emergency Control Center Coordinator, his alternate will assume these duties.

In addition, the Emergency Control Center Coordinator and Alternate are responsible for the following:

- 1) Periodically reviewing and evaluating the Disaster Recovery plan to assure all contingency site procedures have been adequately considered and prepared.
- 2) Ensuring that testing procedures included in the plan are appropriate and maintaining complete testing procedures for all major business operations.
- 3) Conducting periodic tests of the contingency site and maintaining technical readiness for operation of business functions from the contingency site.
- 4) Reporting the progress, problems and successes of each test of the contingency site to the Emergency Coordinator.
- 5) Recommending to the Emergency Coordinator any necessary changes or improvements in the plan.
- 6) Keeping management informed of the status of the contingency site and any changes relative to requirements or planning.

The designated Emergency Control Center Coordinator and Alternate are identified in Appendix A - Emergency Notification (Contingency team).

## **2.6 The Use of Emergency Action Teams**

Emergency Action Teams are used for specific functions during an emergency and subsequent recovery. The teams and their responsibilities are defined in Chapter 7. Designated leaders and members of Emergency Action Teams are identified in Appendix A - Emergency Notification (Emergency Action Team).

In general, the Team Leader of each team is responsible for the following duties:

- 1) Periodically reviewing and evaluating the emergency planning with emphasis on completeness and accuracy of specific recovery procedures, team responsibilities, assignments of and changes in personnel, and availability of equipment, facilities, and services.
- 2) Recommending to the Emergency Coordinator any necessary changes or improvements in the plan.
- 3) Recruiting and training personnel for emergencies and maintaining proficiency at a high level. All team members must be capable of performing their duties quickly under stress.
- 4) Informing the Emergency Coordinator of any additions or changes of individuals assigned to the Action Team.
- 5) Participating in the scheduled testing of the plan.

## 2.7 Emergency Control Center

In the event of a major disaster, an Emergency Control Center will be established from which all communications and activities are directed. The Emergency Control Center will be used to coordinate the management of recovery procedures, and will serve as the center of all communications between the Emergency Coordinators, the Action Teams, and all other personnel. The Emergency Control Center might not be a single physical location, but a network of locations in different geographic areas where employees can work together to meet local customer needs while communicating through a centralized phone mail system or other available communications network to coordinate recovery efforts. In addition to the designated physical locations where employees can work together to coordinate recovery, key DHI employees will be provided with cellular telephones that have proven quite reliable in the event of major disaster in other areas. The numbers of these cellular phones are included in Appendix A.

The administration of the Emergency Control Center is the responsibility of the Emergency Control Center Coordinator.

- 1) The designated Emergency Control Center and alternate locations are identified in Chapter 7.2.3.
- 2) The Emergency Control Center will be activated when a major disaster has occurred, especially when the personal safety of employees or property is jeopardized. Activation of the Emergency Control Center is the responsibility of the Emergency Control Center Coordinator. Direction of activities and communications from the Emergency Control Center is the responsibility of the Emergency Control Center Coordinator. As soon as the Emergency Control Center is activated, the Emergency Control Center Coordinator will set up proper messages on the emergency message mailbox for both employees and clients.
- 3) This center will provide centralized and coordinated control of communications during emergencies. When the Emergency Control Center is in operation, Emergency Coordinators and Action Team Leaders will coordinate with the center and keep it informed of status and progress.
- 4) If conditions warrant closing our facilities, the Emergency Control Center will communicate the closing notice through the management chain to all employees.

**This page intentionally left blank.**

## CHAPTER 3 MAJOR FUNCTIONS AND KEY CONSIDERATIONS

This section describes our organization's critical business functions that must be kept in service in the event of a disaster. Each function is described here in light of the key considerations in a disaster recovery scenario. The functions are listed in order of most critical (that is, the greatest risk to the business) first.

### 3.1 Online Client Processing

#### Description

Online Processing includes the FPS GOLD Financial Service Bureau Product, the GOLDPoint Systems Financial Service Bureau Product, and the Amelcor Online Dairy Processing.

#### Policy

Online real-time processing is the basis of all major DHI systems. DHI is committed to providing the best and most reliable online real-time systems in the industry. All online processing must be done in such a manner as to minimize the steps required in the event of an unexpected system failure. All online systems, and their related after-hours processing, must report conditions that indicate file inconsistencies that may have occurred due to system failures.

#### Schedule

Online processing is scheduled Monday through Saturday except on scheduled national holidays. The Online system is available from approximately 5:00 a.m. to 11:00 p.m. Mountain Time (these times vary according to individual customer contracts). In addition to these hours, Amelcor Dairy online processing, FPS GOLD and GOLDPoint Systems file and print down load, FPS GOLD and GOLDPoint Systems ATM, FPS GOLD and GOLDPoint Systems GOLDPhone, and Internet Banking processing is available on a limited basis 24 hours per day.

#### Responsible Departments

Programming and support of online processing is accomplished by each of the individual industry departments. Operations support for online processing is provided by the Internal Services Department. Due to the design of our systems, in the event of catastrophic disaster, any industry department could provide basic customer support for other departments.

#### Hardware Requirements

Online processing requires the full processing system currently installed at DHI's main office in Provo, UT. All equipment necessary for online processing is functionally duplicated at the remote site.

#### Network Considerations

Online processing requires the availability of a communications network to connect the remote client to the processing center. Several contingency plans are in place to recover and switch telecommunications network assets to the remote center. In addition, each client site should have backup hardware that allows connection to the remote or the main processing site in the event of a network failure.

## Major Functions and Key Considerations

---

### Additional Considerations

With replication of our customer's data to our contingency site in place, the need to reenter data is almost nonexistent. When the system becomes available at the recovery site, it is the responsibility of each institution to verify that the transactions for the day have been properly recorded, and if not then reenter them.

### Expected Recovery Time

If the disaster event requires moving the processing to the off-site location, a minimum of 5 hours and a maximum of 8 hours will be required before processing can be resumed. The actual number of hours required is based on the nature of the disaster and the availability of people and/or the ability to remotely access our recovery equipment.

## 3.2 Afterhours Processing

### Description

Afterhours processing includes the functions required to verify monetary balances, maintain client files, post information not entered through teller terminals and the generation of reports used by the clients. Afterhours processing is done for FPS GOLD Customers, GOLDPoint Systems Customers and Amelikor Dairy Customers.

### Policy

Afterhours processing must back up all files and define a checkpoint that can be used as a base restart point in the event of any processing failure. Afterhours processing will always be controlled by a special computer program that will determine the sequence of steps required to accomplish processing. The controlling program will also control all restarts including the cases where steps must be re-run due to restarting. Operations staff members must never be required to make decisions related to the sequence of steps to be run in any standard run or restart condition.

### Schedule

FPS GOLD and GOLDPoint Systems after hours processing is scheduled Monday through Saturday except on specified national holidays. The afterhours processing starts at 6:00 p.m. Mountain Time and usually runs until 4:00 a.m. the next morning.

### Responsible Departments

Programming and support of afterhours processing is accomplished by each of the individual industry departments. Operations support for afterhours processing is provided by the Internal Services Department.

### Hardware Requirements

Afterhours processing requires the same hardware required for the online. All equipment necessary for online processing is functionally duplicated at the remote site.

### Network Considerations

---

## Major Functions and Key Considerations

---

Afterhours processing does not require the online system. However, communications lines are required to receive transmissions from inclearing processing providers used by the FPS GOLD and GOLDPoint clients. The backup site is fully equipped with lines and hardware to accomplish this function.

### Additional Considerations

Afterhours processing begins with making a copy of the database files prior to any processing. This allows the afterhours to be restarted at the beginning of the run if any catastrophic event occurred during the run. At the end of the afterhours, the files are again copied for a restart point in the case of any need to access the data from the end of afterhours processing. This "two set" approach to backing up files provides a high level of recovery options no matter what kind of failure occurs. The secure files from the beginning and end of each processing day are maintained in a backup disk both onsite and offsite.

## 3.3 Dairy Batch Processing

### Description

Dairy batch processing is performed for each dairy customer once per month. Typically the data to run the dairy batch runs is transmitted from both on-farm as well as milk laboratory locations. This data is then processed using the previous month's history creating several reports which are returned to the dairy client as well as a new copy of the dairy history for the client which is saved on disk for use during the next month's run.

### Policy

DHI policy for dairy batch processing includes the commitment to process the data normally within one day of receipt. Dairy history files are kept in online storage for 45-60 days. Incremental tape backup is taken of dairy history each day. This backup scheme eliminates the need to ever recover more than one day's processing in the event of any failure. Sites transmitting data to DHI Provo are responsible to back up the transmitted data and keep the backups for at least two additional working days after they are notified that their data has been successfully run.

### Schedule

Dairy batch processing is scheduled Monday through Saturday except on scheduled national holidays. Dairy batch processing normally occurs on an as-needed basis both during the day and during the night.

### Responsible Departments

The Amelcor Dairy staff accomplishes programming and support of online processing. Operations support for processing is provided by the Internal Services Department. Distribution and mailing of Amelcor reports is the responsibility of the dairy department.

### Hardware Requirements

Dairy batch processing requires the same hardware required for the online processing. All equipment necessary for batch processing is functionally duplicated at the remote site.

### Network Considerations



## Major Functions and Key Considerations

---

Dairy batch processing requires the availability of a communications network to connect to some of the dairy records processing functions that are performed on other Dairy division servers at the processing center. Transmissions of data used in the dairy batch processing are received using other communications servers and the online dairy processing system. Dairy uses the before-mentioned hardware configuration for its processing needs. The Dairy processing is isolated from the other industry departments' processing by running in a separate server under Sierra.

### Additional Considerations

Dairy batch processing creates a high volume of printed output. Print will be sent electronically to where it can be printed.

## 3.4 Programming Support and Development

### Description

Programming support and development groups assist in the support of customers, find and fix errors in existing program codes and develop new programs for use in their application areas. In addition, clients in all divisions run products on remote systems. Support and development groups assist in the maintenance and operation of these systems when second level support is required.

### Policy

DHI has made and continues to make major commitments of resources to the programming and support function. It is critical that the programming and development system be available to support the other functions that have been listed in the sections above.

### Schedule

Programming support and development systems are normally available for use 24 hours per day. Typically they are most heavily used during the prime shift.

### Responsible Departments

Programming Support and Development functions are located in each of the individual industry departments. In addition, Operations support for programming and development is provided by the Internal Services Department. Due to the design of our systems, in the event of catastrophic disaster, programmers from industry departments could provide basic programming support for other departments.

### Hardware Requirements

Programming development requires a very small percentage of the processing resources currently installed at DHI's main office in Provo, UT. All equipment necessary for programming support is functionally duplicated at the remote site.

### Network Considerations

Programming and development uses the same communications network as the online processing function.

## Major Functions and Key Considerations

---

### Additional Considerations

Due to the size of our programming staff, in the event of a major disaster, programmers would be dispersed to our remote office sites as well as some centrally located customer sites to assist and support processing through the recovery period. All file and library resources required for the programming and development function are replicated to our remote site. Key programmers are also equipped with remote access for programming support. It is not our intention to continue the development of new software during a major disaster. The programming staff would be focused on supporting existing applications and customers during such an event.

## **Major Functions and Key Considerations**

---

**This page intentionally left blank.**

## CHAPTER 4      GENERAL PROCEDURES FOR POTENTIAL INTERRUPTIONS

A series of procedures follow as a reference for prompt and appropriate actions to be taken in potential emergencies or events which cause interruption of business operations.

Orientation sessions are to be held periodically by department managers to familiarize employees with these procedures and to outline responsibilities in the event of such emergencies. The sessions will be held as needed and determined by the responsible department manager. Internal audits will ensure that employees are properly trained and familiar with these procedures.

Copies of this plan are to be kept in key locations for ready reference. Members of the Contingency team are to be given copies of this plan to be stored at home and at work. The Distribution List is contained in Appendix J.

Remember that the assets of this organization are extremely important to its very existence. **The most important asset is our personnel. Risks should not be taken to save other assets if personnel may be in jeopardy.**

### 4.1    Fires

#### Contingency Plan for Fires

##### Prevention

1. Review all areas of responsibility for combustible materials, including below raised floors.
2. Operational areas are to be sight checked by each shift before they leave, particularly if area is to be left unoccupied.
3. All new employees will be educated about the fire plan. All employees will have periodic reviews of the fire plan on a schedule to be determined by their department managers.
4. Regular site inspections, which include general area review and checks of electrical connections, fire extinguishers, and smoke detectors are to be made every three months by the Building Manager.
5. Smoking by employees, visiting clients or other visitors is prohibited in all areas of the building at all times.
6. The building manager will conduct fire drills annually to allow employees to practice the evacuation procedures in this section.

##### Detection

Detection of fire is the responsibility of the employees located in each area. Once a fire has been detected, employees should ONLY activate the building alarm system if the building's heat/smoke detectors have not been activated. For all buildings, the alarm system is activated by pulling one of the fire alarm switches located near the building exits.

##### Extinguishing Fires

1. The staff will be trained in the use of fire extinguishers during the periodic fire plan reviews. Additionally, Building Management personnel are to arrange to have all extinguishers inspected annually. Extinguishers are located in the following areas:

- 
- 1 in N. building north entrance lobby (dry chemical)
  - 1 in N. building mail room near the service window (dry chemical)
  - 2 in N. building front hallways - one on each side (dry chemical)
  - 2 in N. building back hallways - one on each side (dry chemical)
  - 2 in N. building print room near the entrance doors (dry chemical)
  - 3 in N. building warehouse (1 C02, 2 dry chemical)
  - 1 in N. building employee entrance door (dry chemical)
  - 1 in Main Entrance Vestibule (dry chemical)
  - 1 in S. building first floor elevator mechanical room (dry chemical)
  - 3 in S. building first floor (dry chemical)
  - 3 in S. building second floor (dry chemical)
  - 3 in S. building third floor (dry chemical)
  - 1 in S. building third floor kitchen (dry chemical)
  - 1 in W. building first floor hall by bathrooms (dry chemical)
  - 3 in W. building outside the stairway of each floor (dry chemical)
  - 3 in W. building outside of the elevator on each floor (dry chemical)
  - 1 in W. building first floor elevator mechanical room (dry chemical)

Fire extinguishers that are Dry Chemical (ABC) may be used for all types of fires. The C02 fire extinguisher is for gas/fuel fires (our generators).

2. An employee should only attempt to extinguish a fire if it is very small or confined to a particular piece of equipment. Otherwise, the fire department should be called and the building should be evacuated immediately.
3. DO NOT PLAY HERO. If the fire is of any consequence, activate the building alarm system and then follow the DHI Fire Plan to evacuate the building.

### **Evacuation**

Do not stop to take papers or tapes from the building. Computer room personnel should make sure the door to the tape vault is closed prior to evacuation.

## **Emergency Procedures for Fires**

### **Goals**

- Protect the lives and health of employees
- Protect essential documents, records, and data
- Minimize damage to equipment and other property

### **Procedures in the Event of a Fire**

1. If the alarm is not sounding, activate it on the way out
2. In the event of a fire located in areas of the building protected by a fire suppression system such as the NCC area or Operations area, personnel should exit as quickly as possible in order to avoid being present during a discharge. Any employee caught in a discharge should remain in the room until the agent has cleared to prevent re-igniting a fire. The only place that a fire will cause both the strobes and the bells to go off together is in the raised floor data center. The fire suppression system is designed to go off 30 seconds after the bells

---

and strobes begin going together. If it is obvious that there is no fire in the raised floor data area, the countdown can be stopped by pressing one of the 3 yellow buttons (labeled “suppression system abort”) located in the NCC area, on the north wall near the east doors in the data center, and in the hallway outside the operations room. Once the button is pressed it must be held down until someone else is able to reset the alarm or the suppression gas will immediately be released.

3. If the fire is small, use a fire extinguisher, **AFTER YOU HAVE CALLED THE FIRE DEPARTMENT**. Pull the pin on the fire extinguisher, then discharge the extinguisher by aiming at the base of the fire using a side-to-side sweeping motion.
4. If the fire is such that employees should evacuate the building and the building alarm system has not been activated, for all buildings the fire alarm can be activated by pulling one of the fire alarm switches located near the exits.

## DHI Fire Plan

When the building fire alarm is activated, horns will sound in a **steady tone** and wall-mounted **strobes lights will flash**. If this happens, ***remain calm, get out NOW, and stay out.***

### Exit Routes

You should prepare yourself for a potential fire to avoid unnecessary confusion and panic. Prepare yourself by:

1. Learning your environment.
2. Planning two routes to use in the dark. (The building may be dark due to smoke, a power outage, or the time of day.) **NOTE: DO NOT USE THE ELEVATOR**

## Exit Procedures

### Normal Business Hours (NCC in the building)

Between 7:00am – 6:00 pm on weekdays (approximately)

- **Always** exit the building when the fire alarms and strobes go off.
- Everyone should be out of the buildings within **2 minutes**
- If you are on a telephone call, politely end the conversation and exit the building.
- Gather in the far west parking area closest to Independence High.
  - Gather in departmental groups so that the managers can get an accurate count.
  - Notify your manager if someone is unaccounted for
- Do not use the elevator during evacuation
- Once in the gathering area, report to your immediate supervisor to be marked “accounted for”.
- **Do not** return to the building without an OK from the building manager or someone from the NCC department.

### After Hours (NCC Not in the Building)

Between 6:00pm – 7:00am on weekdays (approximately) and 24 hrs on weekends and holidays

- **Always** exit the building when the fire alarms and strobes go off.

- 
- Everyone should be out of the buildings within **2 minutes**
  - If you are on a telephone call, politely end the conversation and exit the building.
  - Gather in the far west parking area closest to Independence High.
  - Do not use the elevator during evacuation
  - Once in the gathering area, report to the Operations shift supervisor.
  - The Operations shift supervisor will work with the fire department when they arrive.
  - Do not return to the building until you receive the OK from the fire department.

### Manager/supervisors

- Supervisors must appoint 1 or 2 individuals in their department as backups for when they are not available during a fire/fire drill (prior to fire drill). Make sure the appointed individuals are familiar with the duties.
- Make sure that all your employees know who to report to during a fire drill/alarm – they should all know who the acting supervisor (s) is/are.
- Fire reporting forms and pencils will be distributed at the gathering area by members of NCC.
- Complete the fire reporting form focusing on those unaccounted for
  - If the main supervisor is not available, the appointed backup should handle the form.
- Each supervisor must turn completed forms into the building manager or another member of NCC within **10 minutes**
- NCC will give the “Unaccounted for” list to the Fire Department (**15 minutes**).
- **Do not** return to the building without an OK from the building manager or someone from the NCC department.

### Inside Fire

If you are in the same room as the fire, stay low, quickly crawl to an exit, and try to keep beneath the smoky buildup.

### Door Checks

It is important to correctly perform a door check to help prevent a fire from spreading. To perform a door check:

1. Gently touch door handle to determine whether or not it is warm. If the handle is warm, a fire is probably on the other side.
2. Feel the door to determine whether or not it is warm. If the door is warm, a fire is probably on the other side.
3. Do NOT open a door until you have performed one of the following tests:
  - A. For a door that you must **push to open** into a room or stairwell, slightly open the door. Be ready to slam the door shut if a fire or compressed, hot air rushes in from the stairwell. Note: A fire spreads extremely quickly when this procedure is not followed correctly.
  - B. For a door, such as a closet door, that you must **pull to open**, use the Three-Point Method below:
    - High (place a flat, open-palmed hand **near**, but not at or above, the top of door),
    - Middle (place your hip against door),
    - Low (secure your foot against bottom of door)

---

Shift your weight and lean against the door so that you can quickly slam it shut. Slam the door shut if you feel hot or high-pressured air or if flames appear. The pressure can be explosive.

C. Inside Door Checks

- Gently touch door handle to see if it's warm – DON'T burn your hand needlessly.
- Place your **flat, open-palmed hand** on the door. If the door feels warm, a fire is probably on the other side.
- If a door is warm, try to find an alternative route to take out of the building.
- If a door is warm, place something such as a jacket or towel under the door to keep smoke from entering the room.

## 4.2 Electrical Power Outages

With the implementation of an extensive power backup system, a power outage resulting in the interruption of computer room operations, voice and/or data telecommunications is very unlikely. However, while the backup power generator is operating, the Operations Manager is responsible to contact the Power Company to determine how long the public utility power outage is expected to last.

The backup generators run on a #2 diesel fuel and have a tank capacity to run 24 hours without refueling. In the unlikely event that power cannot be restored for an extended period, then the Operations Manager will notify the contingency team to consider whether contingency site operations are required.

If a power problem exists even though public power is not out of service, such as after restoration of power, the following people need to be notified:

**BUILDING MAINTENANCE:**

Name:	Phone No.:
Jeff Abbott	Office 801-344-6431 Cell 801-400-5935
Lynn Crandall	Office 801-429-2102 Home 801-489-7161
Melissa Carpenter	Office 801-344-6620 Cell 801-404-2965

**ELECTRICAL SERVICE COMPANY:**

Name: Provo City Power Phone No.: **801-852-6868**

**UPS & GENERATOR SERVICE COMPANY:**

Name: Techconnect Phone No.: **801-298-9087**



---

## 4.3 Telecommunications Failures

Failures of the telecommunications system fall into two basic categories:

1. **Hardware Failure** – Should a piece of telecommunications equipment fail, it must either be repaired or replaced, like any other equipment failure (see Section 4.6 below and/or refer to Appendix E for vendor contacts.)

Contingency plans for telecommunications equipment, by type of equipment or specific location, are as follows:

Telephone System contingencies:

Cellular phones are issued to several employees to allow communication during a phone outage. Clients are urged to call the emergency notification voice mail number 801-602-1671 if the main office number is unresponsive.

2. **Line Failure** - The line is a utility service provided by a communications carrier company. If a line fails, just as in a power outage, the organization is dependent on the utility to fix the problem and restore service.

An extreme phone system outage would affect the entire business operation, in which case the contingency site is our option for temporarily operating the business or some key portions of the business until repairs are made. See Chapter 7 for procedures relative to contingency site operations.

Contingency plans for line failures are as follows:

- Access via VPN and the Internet.

## 4.4 Flooding

### Contingency Plan for Flooding

#### Prevention

The facility design is to be reviewed at least annually by Operations Management for knowledge of risks relative to flooding.

1. It is their responsibility to know where water pipes and drains are in respect to our equipment. If possible, route pipes and add drains for reducing the risk of flooding, taking into consideration the potential for flooding from above (upper floors or roof).
2. Know how the facility lies physically in respect to external floods and what steps can be taken for prevention, such as sandbagging. If floods are a substantial risk, the facility will be equipped with bags and shovels and availability of sand will be determined. If the opportunity arises to choose a new business facility, take into account the flood plain and building construction.
3. During heavy weather conditions, particularly rain and snow, operations personnel will inspect windows, roofs, and basements for flooding or water buildup.

- 
4. Building personnel or contract maintenance staff will inspect all pipes and valves within the facility for leaks at least twice annually.

### **Detection**

1. The detection of water within the business facility, particularly under the raised floors, is vitally important to prevent electrical shocks, short-circuits, or equipment damage. The building alarm system has water sensors beneath the raised floors. Once the alarm system detects water, the system will send a water alarm message to the Central Station, which will then notify DHI personnel of the problem.
2. Personnel who see water leakage of any kind should notify the Operations Manager or Building Manager as soon as possible.

### **Evacuation**

1. If flooding is such that employees must evacuate the building, call the building management immediately and give them the details (what is happening, where in the building, etc.).
2. When leaving the building, exit through available exits.
3. Do not attempt to take tapes or papers with you when evacuating the building.
4. If possible before evacuation, all power is to be shut off to equipment and overhead lights.

## **Emergency Procedures for Flooding**

### **Goals**

- Protect the lives and health of employees
- Protect essential documents, records, and data
- Minimize damage to equipment and other property

The following procedures should be filed in the Operations Procedures Manual and be easily accessible.

### **Procedures in the Event of Flooding**

1. Call building management immediately.

Name:	Phone Number:
Jeff Abbott	Office 801-344-6431 Cell 801-400-5935
Lynn Crandall	Office 801-429-2102 Home 801-489-7161
Melissa Carpenter	Office 801-344-6620 Cell 801-404-2965

## 4.5 Building Alarm System Procedures

### Main Purposes and Objectives of Building Alarm System

1. **Continual Sensing:** The building alarm system is designed to continually sense for various problems within the buildings. Once it detects a problem, it notifies personnel of a problem. The following are problems for which the alarm system searches and the way it notifies personnel:
  - Heat/smoke                                      When smoke or excessive heat is detected a siren sounds **and** Strobe lights flash
  - Perimeter Monitoring                              makes a “yelping” tone **without** strobe lights when windows or doors are broken or an entrance is open
  - Water    Calls central monitoring if a floor alarm
2. **Monitoring:** The building alarm system monitors the following items within the building:
  - Lock boxes
  - Perimeter doors and windows
  - Doors to secure areas of the building
3. **Notification:** Once the building alarm discovers a problem within the building, it will notify:
  - Computer Room operators
  - Central Station (24:7 Monitoring Office)
  - Designated DHI Personnel
4. **Alarms**
  - Fire    siren & flashing strobe lights
  - Burglar    short “yelping,” no strobe lights
  - Water    Operations keypad, Central Station will call DHI contacts, etc

### How to Respond to Alarms

#### Fire

1. **Stay calm**
2. **Evacuate immediately**—Do NOT stop, get out NOW, stay out, and call 911
  - A. Stay low and crawl, if necessary
  - B. Hold your breath if you are surrounded by heavy smoke
  - C. CONCENTRATE - FOCUS
  - D. Be prepared
    - Know your surroundings because you may need to feel your way out, or count doorways, hallways, windows, etc. to exit
    - Determine **two** exits you can take before a fire occurs
  - E. Do NOT use the elevator
  - F. Check for HOT DOORS using the three-point method:

- High (place a flat, open-palmed hand **near**, but not at or above, the top of door),
  - Middle (place your hip against door),
  - Low (secure your foot against bottom of door)
- G. Open a door very slowly and be prepared to quickly slam it shut.

3. Reassemble by department in west parking lot

### **Burglar**

1. Do NOT confront a burglar
2. STAY in your office
3. Call 911 & stay on the line
4. DESCRIBE yourself & your location
5. FOLLOW Police instructions

### **Water**

If any wires are in the water, GET OUT of the water and STAY OUT! Shut it off!

## **4.6 Equipment Failures**

Our equipment is maintained by:

<b>EQUIPMENT TYPE</b>	<b>VENDOR</b>	<b>CONTACTS</b>	<b>PHONE NOS.</b>
IBM 6500 Printer	IBM Rico	IBM Customer ID 368090	800-IBM-SERV 877-834-7878 or 866-483-7877
Xerox Printers	Xerox	Xerox Mark Dixon	800-821-2797 801-641-8758
Cisco Security System	Cache Valley Electric Stanley Security	Eric Luther Stanley Security	801-231-9646 888-742-4210
Disks	Hitachi Data Systems	Shawn Kearns	801-815-8388

In most circumstances, the equipment can be repaired quickly to restore operation within several hours. Even if the downtime were as long as a day, the preferred approach is to allow the engineers to make their repairs in the normal manner. If the anticipated repair time exceeds one hour you must notify the Operations Manager. Operations Management will then inform additional management team members as necessary to implement any procedures necessary to accomplish the fastest possible recovery.

## **4.7 Major Disasters**

Since we own our recovery equipment, no call to a vendor is necessary. Initiate recovery procedures as outlined.

A major disaster is one that requires activation of the contingency site due to our inability to function at this site for a period long enough to seriously affect business operations. Reasons may vary from actual destruction of the facility to less severe emergencies. Refer to Chapter 7 for all major disasters.

---

The Emergency Coordinator in his judgment and in consultation with available members of the management team will be responsible for determining the magnitude of an emergency and taking appropriate actions accordingly.

## 4.8 Pandemic

Business contingency plans are based upon geographically specific business disruptions. A pandemic can affect business continuity differently from other business disruptions in that it affects customers, employees, and vendors simultaneously, possibly worldwide.

Of prime concern in a pandemic, is to limit the transmission of the disease between people. Depending on the severity of the disease and how widespread it is, specific plans will need to be modified at the time of the outbreak to minimize the risk to the continuity of business operations. Some of the options to reduce the spreading of a particular illness are:

1. Store facemasks and medical gloves that could be worn by employees, during a pandemic, to reduce contamination while they are in the building. These masks and gloves are currently located in the warehouse in the north building.
2. Identify specific functions, such as programming, communications, customer support, that could effectively be done from home. There are currently many company-owned laptop computers and cellular phones to enable employees to work remotely. Also, a good number of employees have PC-s and Internet access in their homes. A list of cellular phone users and numbers is found in Appendix A. Addresses and home phone numbers of employees are found in Appendix C. Client addresses and phone numbers are found in Appendix D.
3. Use remote collaboration tools to enable employees to continue routine meetings without actually being in the same room.
4. Store a supply of bottled water to use in the case of a water-born contaminant. This water is currently stored in the warehouse in the north building.
5. Ask the custodial staff to increase procedures of disinfecting surfaces that may transmit disease such as; doorknobs, drinking fountains, bathroom fixtures, etc.
6. Implementing and communicating policies that encourage the sick to stay at home.
7. Monitor the CDC (Center for Disease Control) and WHO (World Health Organization) for updates on the spread and effect of the pandemic. Also follow the recommendations that they give to prevent the spread of the pandemic and regain our health if we are infected.
8. In the case our workforce is significantly diminished, we would rely on the existing organizational knowledge and our documentation to recover our business functions and provide technical and customer support to our customers.
9. We realize that some things will be out of our control *ie* public authorities restricting travel and other business related activities. In that event we will work with any and all resources to reestablish and maintain our business functions.

## CHAPTER 5 POLICIES FOR REDUCING RISKS

### 5.1 Protection of Personnel, Data and Software Files, and Hardware

This protection falls under the auspices of various portions of DHI security. Please consult the *DHI Computing Service, Inc. Security Policies and Procedures* manual. Some abbreviated excerpts from that manual are included in this chapter only for convenience purposes. Any discrepancies are to be resolved through the Security Manual.

### 5.2 Protection of Server Computer Data

#### Policy

Server computer data is protected using a combination of data replication and backup procedures with offsite storage in the Tonaquint Data Center in St George, Utah.

DHI has a disk farm from Hitachi Data Systems. This disk farm contains all of our customer's data. A similar farm is stored at the Tonaquint Data Center facility in St. George, Utah. The two farms are connected with a high-speed phone line. When data is changed in our Provo facility, that data is automatically replicated to the St George site. Therefore, all of our customer's data is in both Provo and St George. This data will be used in case of an outage in Provo.

At the end of each working day the FPS GOLD and GOLDPoint files are copied to our tape server (which has only disk associated with it, no physical tapes) and stored both in the tape server system and on a separate disk at Tonaquint. These "end of day" backups can be used if for any reason the files must be reset to the beginning of the night condition to re-run the after hours or to answer programming or data questions. These files are retained for seven to forty-five days.

### 5.3 Protection of Personal System Data

Our Personal Computer data protection is the responsibility of the person that has possession of the personal computer. If an employee wants their personal computer data backed up they may copy the data to a server that is automatically backed up in accordance to the procedure explained in section 5.2.

#### Policy

Due to the portability and lack of security associated with distributed personal systems, all possible data (including client data and system application programs) is to be stored permanently on the server disk sub-systems which are backed up according to the schedule explained in section 5.1. All other critical data used on any personal system will be based on a network server. System servers are backed up weekly with incremental backups made on a daily basis.

Since personal systems are readily available nationwide from computer dealers, in the event of a major disaster it is DHI's intention to replace any necessary personal systems with new hardware.

## Policies for Reducing Risks

---

The tracking of personal system and Local Area Network backups are the responsibility of the Operations Manager working with the Network Control Center. They are to build checklists, verify that the correct backups are taken.

### 5.4 Protection of Business Operations

#### 5.4.1 Importance of Security

We consider security in all forms to be the highest priority. Security will be considered in all aspects of the Contingency Plan.

#### 5.4.2 Physical Security

Access to the business facility is controlled by ID cards. ID cards and the physical security system are controlled by NCC. The ID cards control access into various parts of the building. An employee's job description determines what access they have. Upon termination, the employee's card access is revoked. Operators can activate electrical locks on the outside entrance doors to allow entrance to the building once the operator has verified the identity of the person seeking entrance into the building. Security cameras are stationed in all access areas to the building, as well as all parking lots. These security cameras are used in the identification process.

Operations center access is controlled by the operations staff. Operators can activate electrical locks on the door to allow entrance to the operations center when required.

Visitors to DHI are to sign in at the front office. They are to be accompanied into the secure part of the building by an employee at all times. Visitors are not to be allowed in the computer room without clearance from the operations shift supervisor. Visitors are not to be allowed in the back employee's entrance of the building at any time. Outside doors are not to be propped open for any reason without the constant presence of an employee during the time the door is open. If a door is open for more than 30 seconds an alarm will sound, and an operations employee will have to reset the alarm. Employees should be instructed by their managers to watch for physical security problems and report them immediately to management.

#### 5.4.3 Computer Access Security

All DHI corporate security systems will be administered as outlined in the DHI security policies and procedures documents which can be found on the internal web site.

The security policies and procedures are reviewed and updated at least annually under the direction of the CISO. The CISO will maintain a log of these changes for reference and examination by internal and external auditors.

#### Procedures

1. Physical and media security provide the necessary protection to keep computer systems and media from theft and vandalism. Such protection mechanisms include locks, special computer rooms, shredders, etc. We have a locked, secure computer environment and entrance to certain parts of the data center is authorized only by job requirements and designated ID card access security. These people include the Computer Operations manager and shift supervisors, systems software personnel, the Network Control

## Policies for Reducing Risks

---

manager, and the CEO. Backup data is stored on site in a multi-hour rated fireproof vault. In addition, data is stored offsite on a daily basis. The offsite storage location is fully identified in Appendix A.

2. Assessment is an important component of computer security. This consists of evaluating a system or network to determine the state of its security and integrity. Regular assessment makes it possible to maintain a high level of security. Security assessment is conducted regularly in some of the forums mentioned in Section 2 above by the CISO as well as senior management personnel. When conducting operational audits, the Internal Auditor audits compliance with these procedures.
3. Online access control systems have been designed and written by DHI to protect DHI corporate as well as our client's data. The CISO grants the authority to each of the Client Security Administrators. The Client Security Administrator in turn grants authority to each employee in the client institution. Authority is granted at both the program level and at the function level. Program-level authority allows or denies access to the user. Function authority is controlled at three levels: no access, inquiry access, or file maintenance access. "No access" denies the user any access to the program or function. "Inquiry access" allows the user to look at data with the function but not to change data. "File maintenance access" allows the user to both look at and change data using the specified function.

Client Security Administrators may also grant authority for client security administration to other members of the client's staff. This should be done carefully. Auditors should examine the authority granted by Client Security Administrators to members of the client staff. Ideally only one other member of the staff should have the authority to maintain the client's security files.

4. Programming system access control is accomplished through additional checking beyond the standard security access system. The CISO is required to set up the programmer identification, department information and security profile. System programmers set up the file allocation required to allow the programmer access to the programming system. This "two key" method of allocation prevents a single individual from establishing a new programming user. Programmers may access the work of other programmers in their department but not those of programmers in another department. Because department work files are physically separated, programmers from one department may not access the files of programmers in another department.

If programmers are doing work for a client who requires file updates, the client must set up the programmer to allow access to their files. This protects production files against alteration by DHI application department employees without the proper security given by the client.

5. Our customer may choose an option in the security system called Customer Service Security. If this option is selected, the customer must set up a profile to allow specific access to a program or function. The customer must then select the FPS GOLD or GOLDPoInt employee from a computer-generated list of FPS GOLD or GOLDPoInt employees to whom they want to give specific access. This gives the customer complete control over which FPS GOLD or GOLDPoInt employees have access to their data.
6. Programmer file authorization is controlled by department. Programmers in one department may not update the programs from another department. Programmers in each department may access the application programs for that department through a checkout system. When they have finished updating the program it is checked into a source code repository. Subsequent requests for the program by the same or another programmer will return the latest copy of the program. A path exists to allow the emergency update of a program by the change and release manager in a department. The departmental program change and release manager will move the program upon release of the program. Passwords



## Policies for Reducing Risks

---

are used to protect release and main libraries from unauthorized access. Reports are available to show the current checkout status of all programs in the library.

7. New employees will be set up in the security system by the NCC. Their employee number will be inserted into the security record for reporting and tracking purposes. The CISO will ensure that the new employee receives the appropriate security awareness training.
8. The payroll department is to report terminated employees to the CISO immediately. NCC will immediately inactivate the employee's security, preventing further access by the employee.
9. Client security administration is provided by the establishment of a Client Security Administrator. Client institutions are responsible to set their own internal policy regarding security administration. They should have policies regarding the profiles to be established for their employees, the setup of new employees, the cancellation of security privileges for employees who have been terminated, the suspension of security privileges for employees on vacation and the time out and security change intervals. Daily reports of security change activity are sent to client security or audit departments directly from the DHI internal audit department. These reports also include notification of security violations that have occurred on institution terminals. Auditors should examine the client's security plan, policies, and procedures. Examinations should look for completeness as well as compliance with the established procedures and tracking of security changes and violations using the supplied reports.
10. Password checking and control is provided automatically by the system. When the user is initially established, the password of the user is set to the user name. Immediately upon the first access to the system, the system forces the change of password. Password changes are done using three non-display fields on the display screen. The user must enter the current password in the first field to authorize their password change. The new password is entered twice into two separate fields. These fields are compared to make sure the password was typed correctly.

Passwords must be from five to eight alpha-numeric characters in length; no more than two characters in the password can be the same and patterned passwords will not be accepted. The password may not be the same as the user name. The password may not be the same as any of the last five passwords for the user. The system enforces the password restrictions automatically. Passwords must be changed at intervals that are specified by the System and Client Security Administrators. Because the password change activity is secured by the non-display feature of the clients display terminals, terminals which do not process this feature correctly should be removed from the system by the client and replaced with terminals which are more secure. Auditors should examine all types of terminals for secure non-display fields on each type of terminal.

Passwords are stored on the system in an encrypted format. No one has access to passwords. If a user forgets their password, the System or Client Security Administrator can reset the password of the user to the user name. When the user next accesses the system, they are again required to select a new password to enter the system. The password change must occur within the day it was reset. If the password change is not completed on the day it was set up or reset, the password must be reset again. With Amelikor application software excepted, there are no screens or reports that display passwords.

11. Online terminals that have been logged on and then left inactive, are protected through the use of a time-out interval. When the time-out interval has expired, the password must be re-entered and the user must log on to the system again. The length of this interval is established by the System or Client Security Administrator.

## Policies for Reducing Risks

---

12. Attempts to access applications with the incorrect user/password combination will create a security violation. Security violations are logged by the system and reported in security reports mailed directly to the Client Security Administrator or internal audit department. Security violations are also logged on the system console logs. Security violations cause the terminal to be unusable. The terminal must be reset by the Client Security Administrator or the DHI operations group before a successful logon can be accomplished.

### 5.4.4 Security of Personnel

The following procedures are for the safety and security of operations personnel:

- 1) Operators coming on duty are required to overlap with those going off duty. At night, operators going off duty may request operations staff members to escort them to their vehicles.
- 2) Operators are to be equipped with, or know the locations of battery-powered portable lights in easily accessible places in case circumstances result in extreme darkness. In addition, automatic lights are installed in the building, which are activated in the event of a power failure. A number of lights in strategic locations throughout the building are tied to the Uninterruptable Power Supply. These lights are always on.
- 3) Operators are to have a posted list of emergency telephone numbers, a first aid kit, and emergency procedures available at all times in prominent locations.
- 4) Lights are placed throughout the building and grounds for security purposes.

### 5.5 Protection of Vital Records

Many documents and records are vital to the operation of the business. Procedures and plans have been implemented to protect these vital records. Vital records that are required to continue business operations are stored in the data vault in locked files. Other records that are important but not vital to the existence of the company are kept in locked files with short-term fire protection.

### 5.6 Supplies & Documentation

All information and materials that have been identified as critical for the disaster recovery process are stored in offsite storage. The offsite storage location is fully identified in Appendix A.

Backups that are stored offsite include:

- 1) Critical operating supplies
- 2) All critical documentation

#### Supplies

## Policies for Reducing Risks

---

A limited amount of critical supplies, including special forms and items for the Emergency Control Center (such as letterhead), are stored in offsite storage. The Emergency Coordinator is responsible for the inventory of backup supplies offsite.

Should contingency site operations be required, enough supplies will be available to continue operations until more supplies can be obtained from the organization's vendors. We will arrange for the storage of client checks and forms in the offsite storage site upon their request. Clients will be billed the costs of storage for any items stored in the site. Clients may contact their customer service representative for more information about our offsite storage agreements.

Critical supplies and the quantities stored offsite are:

- A limited supply of letterhead and envelopes from each division in the company.
- A limited supply of DHI purchase orders.

Because the vast majority of our forms are created through use of Advanced Function Print Software, they are stored offsite on the system backups taken each week. Other non-critical forms can be replaced in such a timeframe as to not seriously impact our business.

### Documentation

Critical documentation is stored offsite to assist recovery in the event of a disaster. Critical documentation is also stored in SharePoint, part of Office 365. Copies of the following documentation are maintained in offsite storage:

DOCUMENT NAME	COPIES	RESPONSIBLE PARTY
Disaster Recovery Plan	2	Alt. Emergency Coordinator
Applications Documentation	2	Manager, Programming
Operations Documentation	2	Manager, DP Operations
External Product Documentation	1	System Programming Staff
Miscellaneous Documentation	2	Emergency Coordinator



Documentation is also stored on a server in the Tonaquint Data Center and can be accessed at [dr.dhiprovo.com](http://dr.dhiprovo.com).

## 5.7 Insurance

The following summarizes our insurance coverage as it relates to our business operation.

- Property and Casualty Insurance:

## Policies for Reducing Risks

		<b>CERTIFICATE OF LIABILITY INSURANCE</b>		DATE (MM/DD/YYYY) 05/18/2018			
THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.							
IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).							
PRODUCER MCGRIFF, SEIBELS & WILLIAMS OF GEORGIA, INC. 5605 Glenridge Drive - Suite 300 Atlanta, GA 30342		CONTACT NAME: Allison da Silva PHONE (A/C, No, Ext): 404 497-7500 FAX (A/C, No): E-MAIL ADDRESS: adasilva@mccgriff.com					
INSURED DHI Computing Service, Inc. 1525 West 820 North Provo, UT 84601		INSURER(S) AFFORDING COVERAGE		NAIC #			
		INSURER A: The Travelers Indemnity Company of Connecticut		25682			
		INSURER B: Travelers Property Casualty Company of America		25674			
		INSURER C: Lloyds of London					
		INSURER D:					
		INSURER E:					
		INSURER F:					
COVERAGES CERTIFICATE NUMBER: 6DCGHMDQ REVISION NUMBER:							
THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.							
INSR LTR	TYPE OF INSURANCE	ADOL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR  GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:			6309K118231	05/01/2018	05/01/2019	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMPIOP AGG \$ 2,000,000
A	<input checked="" type="checkbox"/> AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY			BAK131081	05/01/2018	05/01/2019	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$
B	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input checked="" type="checkbox"/> RETENTION \$ 10,000			CUP9K14654	05/01/2018	05/01/2019	EACH OCCURRENCE \$ 1,000,000 AGGREGATE \$ 1,000,000
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N	N/A				PER STATUTE <input type="checkbox"/> OTH-ER <input type="checkbox"/> E.L. EACH ACCIDENT \$ E.L. DISEASE - EA EMPLOYEE \$ E.L. DISEASE - POLICY LIMIT \$
C	E&O/ Cyber Liability			ASG18G005535	05/01/2018	05/01/2019	Limit - Each Claim \$ 10,000,000 Limit of Liability - Aggregate \$ 10,000,000
DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)							
CERTIFICATE HOLDER				CANCELLATION			
FOR INFORMATIONAL PURPOSES ONLY FOR INFORMATIONAL PURPOSES ONLY FOR INFORMATIONAL PURPOSES ONLY, GA XXXXX				SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.  AUTHORIZED REPRESENTATIVE 			

## **Policies for Reducing Risks**

---

**This page intentionally left blank.**

## **CHAPTER 6 CONTINGENCY SITE DESCRIPTION**

### **6.1 Location and Contacts**

Name of Business Contingency Site:

Location: Tonaquint Data Center  
1108 W 1600 S  
St George, UT 84770

Telephone Numbers: 1-435-628-6164 main number  
1-435-628-7926 support

Name of Contact: Phil Daily, Chris Howard

#### **The Nature of the Arrangement**

Type of contingency site:

Full Functional Replacement for DHI Site

General nature of the arrangement:

The TDC Site is available 24\7. It is covered by contract with TDC.

### **6.2 Equipment Configuration and Facilities**

The equipment there is owned by DHI. The equipment is configured for our needs. It is updated whenever the main DHI site configuration changes or when additional communications facilities are required for client communications.

### **6.3 Scheduling Considerations**

The site is available 24 hours per day 7 days per week.

**This page intentionally left blank.**

## CHAPTER 7      RECOVERY PROCEDURES FOR A MAJOR DISASTER

The following contingency plans are for use in a major disaster, that is, a disaster of serious enough magnitude to require our business operation to be moved to our Emergency Control Center site.

### 7.1      Emergency Action Teams and Responsibilities

The following Emergency Action teams have been defined for use in disasters or major emergencies. The purpose, responsibilities, and members of these teams are described on the following pages. The teams will be activated selectively by the Emergency Coordinator and/or the Contingency team according to the nature of the emergency. The teams report to the Emergency Coordinator, or the Emergency Control Center Coordinator if offsite.

Emergency Action Teams

Business Operations Team	7.1.1
Data Processing Applications Team	7.1.2
Equipment Team	7.1.3
Facilities Team	7.1.4
Administrative Team	7.1.5
Communications & Logistics Team	7.1.6
Web Server Recovery Team	7.1.7

The use of Emergency Action teams and the general responsibilities of Team Leaders are discussed in Chapter 2.6. Designated leaders and members of the action teams are identified in Appendix A.

#### 7.1.1 Business Operations Team

**Purpose**

The purpose of the Business Operations team is to ensure the resumption of business functions following a



## **Recovery Procedures for a Major Disaster**

---

disaster by recovering and continuing the scheduled processing at the Emergency Control Center site until such time that operations can resume at the original or replacement facility.

### **Responsibilities**

- 1) Periodically review and evaluate the appropriateness and completeness of procedures for backups, offsite storage, and recovery. "Backups" must include data, PC software, forms, supplies, and operations documentation.
- 2) In a disaster, obtain all appropriate backups from offsite storage including supplies, and documentation.
- 3) Participate in initiating operations at the Emergency Control Center site. Then continue contingency operations until the Emergency Control Center site is no longer required. This will require communication with the other teams to understand levels of service and functional differences in the contingency mode, with the user departments to prepare a revised processing schedule, and with the Emergency Control Center or Emergency Coordinators concerning status of work.
- 4) Coordinate with users about submission of requests to the Emergency Control Center site and about distribution of information from the site.
- 5) If contingency operations continue for an extended period of time, ensure that adequate levels of operating supplies are maintained at the Emergency Control Center site.
- 6) Provide manpower to support the offsite operations. Coordinate with the Administrative team for transportation and housing of the operations staff. Revise operations schedules as appropriate to meet the needs of the emergency situation.

### **Team Members**

The Business Operations Team is comprised of two separate teams: The Technical Support Team and the Operations Team. See Appendix A for the current and complete list of the leaders and members of these teams. Overall coordination duties for the Business Operations Team are the responsibility of the Offsite Emergency Coordinator.

## **Recovery Procedures for a Major Disaster**

---

### **7.1.2 Data Processing Applications Team**

#### **Purpose**

The purpose of the Applications team is to ensure proper functioning of Data Processing applications at the Emergency Control Center site and to coordinate with users and our Data Processing department during the contingency period.

#### **Responsibilities**

- 1) The Applications team must participate in preparing and conducting tests at the Emergency Control Center site. If problems with application operations are identified at the Emergency Control Center site, the Applications team must prepare and document solutions for the problems. Applications documentation and contingency plans should be stored offsite with an electronic copy at [dr.dhiprovo.com](http://dr.dhiprovo.com) and on SharePoint.
- 2) In a disaster, obtain offsite applications documentation and contingency plans in order to assist in restoring Emergency Control Center site operations.
- 3) Coordinate with Operations and users to determine work that was in progress at the time of the disaster. When operations are restored at the Emergency Control Center site, the Applications team must first help recover any lost work that was in progress.
- 4) Once user work has been recovered, coordinate with the users concerning changes in the way they will interface their various applications.

#### **Team Members**

See Appendix A for the current and complete list of the designated team members and team leader.

## **Recovery Procedures for a Major Disaster**

---

### **7.1.3 Equipment Team**

#### **Purpose**

The Equipment team is responsible for repair or replacement of critical equipment, its installation and testing, and all equipment contingency planning -- whether at the original site, the replacement site, or the Emergency Control Center site. Unless a separate team is established, the Equipment team is also responsible for telecommunications.

#### **Responsibilities**

- 1) Participate in all equipment-related contingency planning.
- 2) In the event of a disaster, assess the extent of damage or the effect of failures on equipment and telecommunications.
- 3) Coordinate with vendors in obtaining necessary repairs or replacement of equipment. Agreements for rush delivery of equipment or telecommunications hardware in the event of a disaster should be negotiated in advance wherever possible.
- 4) Coordinate with purchasing, finance, insurance, and other departments in equipment salvage, insurance claims, and financing for replacement equipment.
- 5) Install and test all replacement equipment or data lines, and supervise all problem-solving when failures are encountered.

#### **Team Members**

See Appendix A for the current and complete list of the designated team members and team leader.

## **Recovery Procedures for a Major Disaster**

---

### **7.1.4 Facilities Team**

#### **Purpose**

The purpose of the Facilities team is to restore or replace the business operations site.

#### **Responsibilities**

- 1) Maintain current configurations of the site facilities, either as an appendix to the plan or as part of the supporting documentation also backed up in offsite storage. The configurations should include space layouts lists and of all requirements such as air conditioning, power distribution, power conditioning, etc., as well as specifications of model numbers, capacities, electrical requirements, and so on.
- 2) In the event of a disaster, assess the damage and recoverability of our facility. If the facility is usable, proceed to organize immediate repairs.
- 3) If our business facilities are destroyed and not usable, proceed to locate replacement facilities that can be acquired quickly and are usable for a reasonably long period if not permanently. Again, facilities include not only requisite square footage in a building, but raised flooring, cabling, air conditioning, power, etc.
- 4) Coordinate with facilities vendors to provide necessary facilities (buildout, equipment, installation, and permits) on an emergency basis. As much as possible, negotiate contingency plans in advance.
- 5) Coordinate with purchasing, finance, insurance, legal and other departments in contracting for space and buildout, insurance claims, and financing the new facilities.

#### **Team Members**

See Appendix A for the current and complete list of the designated team members and team leader.

### **7.1.5 Administrative Team**

#### **Purpose**

The Administrative team is responsible for all activities in the disaster recovery process which are not handled by the other Emergency Action teams. These activities would include arranging expense advances, performing clerical and other administrative functions, etc.

## **Recovery Procedures for a Major Disaster**

---

### **Responsibilities**

- 1) Develop and review administrative procedures of the plan.
- 2) Participate in tests of the plan to actually perform the administrative functions and evaluate procedures and requirements.
- 3) Perform clerical errands and administrative functions as needed during the disaster recovery.

### **Team Members**

See Appendix A for the current and complete list of the designated team members and team leader.

## **7.1.6 Communications and Logistics Team**

### **Purpose**

The purpose of the Communications and Logistics team is to provide transportation, housing, shipping, and other miscellaneous items as needed.

### **Responsibilities**

- 1) Provide any needed travel arrangements such as airline flight reservations, arrangements for transportation of employees and their baggage to the airport, etc.
- 2) Provide housing arrangements and food, rest and recuperation facilities as needed for those traveling, or any others involved in the disaster recovery efforts having any special needs.
- 3) Prepare press releases or other communications deemed necessary.
- 4) Provide for any shipping needs to include correspondences, packages, crates, etc.
- 5) Coordinate with clients to distribute the proper dial up and communication procedures.
- 6) Notify the insurance agency of any disaster recovery efforts or actions when reasonably convenient to do so. If any deaths are involved, insurance agent notification is to be done immediately. See Appendix E.

### **Team Members**

See Appendix A for the current and complete list of the designated team members and team leader.

## **7.1.7 Web Server Recovery Team**

The purpose of the Web Server Recovery Team is to recover the World Wide Web server sites used by end-users at the Emergency Control Center site and insure that users are able to use the applications provided by these Web servers.

- 1) The Web Server Recovery Team must participate in preparing and conducting tests at the Emergency Control Center site. If problems with Web server operations are identified at the Emergency Control Center site, the Web Server Recovery Team must prepare and document solutions for the problems. All documentation and contingency plans for Web servers should be stored offsite and on SharePoint.
- 2) In the case of a disaster, the Web Server Recovery Team must obtain the offsite applications documentation and contingency plans in order to restore Web server operations at the Emergency Control Center site.

## Recovery Procedures for a Major Disaster

---

- 3) The team will coordinate with Operations and users to determine work that was in progress at the time of the disaster. When the Web servers are made operational at the Emergency Control Center site, the team must recover all lost work. If this proves impossible, the team must inform the affected institutions of the time period during which work may have been lost so that institutions can inform their end-users.

### Team Members

See Appendix A for the current and complete list of the designated team members and team leader.

## 7.2 Disaster Recovery Critical Timeline

Task	Estimated Time	Estimated End Time
Incident Evaluation	2 hours	D + 2 hours (D = Disaster)
Declare and create Emergency Control Center	1 hours	D + 3 hours
<u>NCC timeline recovery site:</u>		
Prepare disks for write access	½ hour	D + 3 ½ hours
Build VM Hosts	½ hour	D + 4 hours
Load VMWARE Virtual Center	1 hour	D + 5 hours
Attach storage to VM Hosts	½ hour	D + 5 ½ hours
Verify router configuration	½ hour	D + 6 hours
Verify Firewall configuration*	½ hour	D + 6 ½ hours
<u>Application timeline at recovery site:</u>		
Verify WEB Services are up	½ hour	D + 7 hours
Verify data integrity (see checklist)	1 hour	D + 8 hours
Set/verify run dates – all sets	½ hour	D + 8 1/2 hours
Recover FRB ACH files	1 hour	D + 9 hours
Recover inclearings files	1 hour	D + 10 hours
Recover lockbox files	2 hour	D + 12 hours

\*When the configuration is complete, the application recovery can begin.

Note that the ATM systems will be available according to the procedures of the individual ATM processors.

### 7.2.1 Notification of the Contingency Team

A critical aspect of disaster recovery is the quick reaction of the Contingency team. This requires immediate notification of appropriate personnel so the Disaster Recovery plan can be initiated as quickly as possible.

The Emergency Coordinator has established and will maintain an Emergency Notification List (see Appendix A) and will ensure that all key personnel have it available. Additionally, it has been provided to the following emergency organizations:

## **Recovery Procedures for a Major Disaster**

---

- 1) Building Management
- 2) Fire Department
- 3) Police Department

In the event of a disaster, the following notification procedures will be followed:

### **Procedures**

- 1) If the disaster occurs while operations staff are on duty, they should initiate the notification process as soon as possible.
- 2) The Emergency Coordinator is at the top of the Notification List. If the Emergency Coordinator cannot be reached, the Alternate Emergency Coordinator or other named persons will be called until a member of the Contingency team has been notified.
- 3) The first member of the Contingency team notified is responsible to notify other critical members of the Contingency team and to initiate action. The initial action will be to assemble the team at our facility or the Emergency Control Center.

### **7.2.2 Initial Contingency Team Procedures**

Once the Contingency team has been notified, they must proceed to make an immediate assessment of the situation and initiate appropriate actions.

### **Procedures**

- 1) The first member of the Contingency team notified is responsible to notify other critical members of the Contingency team and to initiate action. The initial action should be to assemble the team at our facility or the Emergency Control Center.
- 2) If the Emergency Coordinator has not yet been reached, the Alternate or persons listed next on the Emergency Notification List will assume full responsibilities of the Emergency Coordinator, until he or she has arrived and been fully briefed. The Emergency Coordinator or acting Coordinator will proceed to

## Recovery Procedures for a Major Disaster

---

implement the contingency plans.

- 3) Make an assessment of the situation directly at the scene if possible, or if not, indirectly based on reported information from the notification sources.
- 4) Based on the team's assessment of the situation, determine the severity of the problem and decide on the appropriate action.
- 5) If the Contingency team judges the emergency to be a major disaster, proceed to do the following:
  - a) Activate the Emergency Control Center
  - b) Notify the appropriate Emergency Action teams
  - c) Notify top management
  - d) Set up proper message on the information mailbox (801) 602-1671

These steps constitute activation of the contingency plans for a major disaster. Additional procedures are provided on the following pages for these tasks.

- 6) If the emergency is not regarded as a major disaster, then the appropriate correction or contingency plans will be implemented. In such case, selected action teams may still be required and will be notified to take action.

REMEMBER, IN A DISASTER RECOVERY SITUATION,  
TIME IS OF THE ESSENCE!

### 7.2.3 Activation of the Emergency Control Center

In the event of a major disaster, a centralized control center will be established from which all communications and activities can be directed by the Emergency Coordinator.

#### Control Center Location

- 1) The primary Emergency Control Center location will be:

The home of B. Lynn Crandall, located in Springville, UT. However, emergency control center operations will actually be conducted through use of standard telephones and the cellular telephone network. Not all members of the emergency team will be in the control center.
- 2) If designated sites are not accessible, the Alternate Emergency Coordinator is responsible to select another location.

#### Procedures

- 1) The Alternate Emergency Coordinator is responsible to maintain an Emergency Control Center in a state of readiness. The Control Center is equipped with table(s), chairs, telephones, marker boards, flip charts, etc. These emergency supplies are stored offsite.



## **Recovery Procedures for a Major Disaster**

---

- 2) When the Emergency Coordinator has declared a major emergency, the Alternate Coordinator will proceed to take all steps necessary to activate the Control Center.
- 3) The first step will be the selection of either the primary, designated alternates, or some other location for the Control Center. For all designated sites, the Coordinators have requisite items, including names, addresses, and phone numbers, necessary to gain access to the site(s). The Alternate Coordinator will notify the owners, managers, and other responsible personnel.
- 4) If necessary, telephones and telephone lines will be ordered from the telephone company for emergency installation, and supplies obtained from backup or other sources to properly equip the Center.
- 5) All emergency personnel and organizations will be notified of the location and telephone numbers of the Control Center (if other than the designated primary control center).

### **7.2.4 Notification of Action Teams and Top Management**

In the event of a major disaster, Emergency Action teams and top management of the organization will also be notified and informed of the situation. Top management needs to know the extent of the emergency and the current status of personnel, property, etc. Action teams are intended to carry out very specialized functions in a disaster recovery situation, and will be called in to act accordingly.

Emergency Action teams are defined in Chapter 7.1. Designated Team Leaders, and the members of each team, are identified in Appendix A, along with addresses and phone numbers.

### **Procedures**

- 1) Determine which Emergency Action teams should be activated and if the presence of any top management is required to support the emergency activities or contingency procedures.
- 2) The Emergency Coordinator should notify top management. The Coordinator or anyone else on the Contingency team can notify the Emergency Action teams.
- 3) In notifying top management, names, positions, phone numbers, and addresses are contained in

---

## **Recovery Procedures for a Major Disaster**

---

Appendix A. If the managers are absent or unavailable, the management succession is defined in Appendix A. Inform them briefly of what has happened, the current status, the plan of action, and the location and phone numbers of the Emergency Control Center. The Emergency Coordinator should inform the executives whether their presence is required and when.

In activating the Emergency Action teams, the Team Leaders of each required team will be called from the Notification List in Appendix A. Inform them briefly of what has happened, the current status, the plan of action, and the location and phone numbers of the Emergency Control Center. Each Team Leader has the Disaster Recovery plan at home and is expected to be prepared to initiate action appropriate to his Team. He or she is responsible for notifying the team to assemble and act according to their contingency plans.

### **7.2.5 Notification of Offsite Storage and Contingency Sites**

Activation of contingency plans will require retrieval of equipment, documentation, and supplies from offsite storage, and establishing business operations at the Emergency Control Center site. These tasks will be carried out by specific Action teams according to procedures in Chapter 7.1. However, to expedite the initial recovery process, the Contingency team will notify the contingency business site that a disaster has occurred and that the contingency plans have been activated. Names, addresses, and phone numbers for the site is contained in Appendix A.

### **7.2.6 Summary of Procedures for Emergency Operations**

This section provides an overview of contingency operations. Specific tasks and procedures are provided in the following sections.

#### **Summary of Procedures**

- 1) All activated teams will assemble at the Emergency Control Center for briefing, discussion of any identified problems, and coordination of the contingency plans. If necessary, the Communications team will make travel and accommodation arrangements for the teams going to the Emergency Control Center site.
- 2) The Applications and Web Server Recovery teams will proceed to identify the work in progress related to

## **Recovery Procedures for a Major Disaster**

---

data processing that needs to be recovered and how that can best be accomplished. The Applications and Web Server Recovery teams will connect to the alternate site via VPN to help bring up the data processing applications and recover work in progress. They will be responsible for assisting user departments in coordinating their application interface procedures. This team will provide all coordination with Client Service Departments and the rest of the recovery team.

- 3) The Operations team will proceed to the Emergency Control Center. Once established, operations will be maintained at the Emergency Control Center site as long as required. Our Emergency Control Center Coordinator will be in charge if there are extended offsite operations involving a significant number of staff. If equipment has been destroyed, damaged, or negatively affected, the Equipment team will proceed to take the appropriate contingency measures to repair or replace the affected equipment.
- 4) If facilities have been destroyed, damaged, or negatively affected, the Facilities team will proceed to take the appropriate contingency measures to repair or replace the affected facilities.
- 5) The Administrative team will support the operation of the Emergency Control Center and the action teams as required.
- 6) The Emergency Control Center Coordinator will continue to maintain the Emergency Control Center as long as appropriate, and will coordinate the contingency operations until they can be returned to a normal, non-emergency state.
- 7) The Web Server Recovery team, with any necessary assistance from NCC personnel, will rebuild or replace and then restore service of an out of service server, going to the contingency site if necessary.

### **7.3 Specific Procedures for Contingency Operations**

This section contains specific procedures for implementing contingency business operations.

#### **7.3.1 Initial Procedures**

##### **At Contingency Site:**

---

## **Recovery Procedures for a Major Disaster**

---

The equipment at the Tonaquint Data Center (TDC) should be configured with what we need. If there have been updates in Provo that haven't been made at TDC then these updates need to be made before we can bring up our systems there. No notification is required in order to use the equipment at the TDC.

### **Assembly and Coordination of All Emergency Teams**

The Emergency Coordinator will notify all team leaders. All team leaders are responsible to activate their teams.

### **Activation of Contingency Site by Operations Team**

No activation procedures are required at the TDC.

### **Recovery of DP Work in Progress by Applications Team**

The replicated disk farm is the starting point for recovery. If the replication is broken at an inopportune time, then it will be necessary to use the previous night's backups to get to a state where our customers can begin inputting data to the system.

Each division is responsible for determining if restores of their customer's data is necessary. The procedure to do these restores is located in the binder for that division. These binders are stored in disaster recovery box 1 and an electronic copy is store at [dr.dhiprovo.com](http://dr.dhiprovo.com) and on SharePoint.

### **Restoration of Web Services by Web Server Recovery Team**

The documentation for restoration of web services can be found at [dr.dhiprovo.com](http://dr.dhiprovo.com) and on SharePoint.

See the DHI Disaster Recovery Documentation folder for specific, detailed web server recovery items needed and for all the necessary instructions.

### **Disaster Recovery Procedures for Restoration of Virtual Servers**

All critical servers in the DHI Network are virtual and are provisioned on replicated tier-one storage. The replication process copies changes as they occur on the primary storage to the backup storage array located in

## **Recovery Procedures for a Major Disaster**

---

the Tonaquint data center. Since the backup storage array is typically only seconds behind the primary, very little data is lost should a major failure occur on the primary system.

In order to restore virtual servers, the replication link must be “broken”, a process of disconnecting the replication, and configuring the backup disk system for attachment to the physical servers.

The physical servers require configuration along with the Virtual Center software used to manage the virtual infrastructure. Detailed instructions, along with configuration scripts are used to configure both the storage and server systems for recovery. Once the configuration is complete the virtual servers will be available for power on. Servers providing critical internal functions such as domain controllers and DNS services will be powered up based on the order listed in the recovery scripts. Application servers that may require configuration changes will not be powered on. Departmental team members will be notified when application servers are ready for power up.

The recovery instructions and associated scripts can be found on the server dhidrnet1 under the scripts folder.

The recovery sequence should be as follows:

- 1) Break replication and enable backup disk array for production.
- 2) Configure VM host and Virtual Center using supplied scripts
- 3) Discover storage and configure virtual network using supplied scripts
- 4) Power on critical servers using supplied scripts
- 5) Remove firefighter security access
- 6) Notify departments as application servers become available

### **7.3.2 Coordination of DP/User Interfaces by Applications Team**

The applications team is responsible to guarantee that user application software is functioning correctly. The applications team communicates with the FPS GOLD and GOLDPoint Systems clients through the banking consultants assigned to help with the disaster recovery operation.

In addition, the applications team is responsible to keep FPS GOLD and GOLDPoint Systems management informed as to how the operation is proceeding. The application team leader will see that the two most senior ranking members of management available are called every two hours to give a brief update of how things are proceeding.

## **Recovery Procedures for a Major Disaster**

---

FPS GOLD and GOLDDPoint Systems banking consultants will be at an off-site command post and will be responsible to be the communications link between the applications team and the FPS GOLD and GOLDDPoint Systems clients that are participating in the disaster recovery operation. When a problem is detected by the client, the problem should be reported to the customer service command post.

The order of procedures to resolve a problem are as follows:

<u>Action</u>	<u>Responsible person</u>
Problem discovery	User
Notify FPS GOLD Customer Service	User
Resolve the problem if possible	Banking Consultants
Notify applications team leader	Banking Consultants
Log problem	Applications Team Leader
Assign problem to team member	Applications Team Leader
Problem resolution	Team Member
Communicate resolution	Team Member to Team Leader
Notify Banking Consultants	Team Leader
Notify Customer	Banking Consultants

By following this procedure, the applications team leader becomes responsible to see that all reported problems are tracked, resolved, and the resolution reported back to the FPS GOLD and GOLDDPoint Systems customer through banking consultants. Banking consultants become the communications link between customers and the applications team. The applications team leader should make regular phone calls to each of the off-site customer service command posts to verify that things are functioning correctly. The problem log should list who has the problem, a brief description of what the problem is, who to notify (phone number) upon problem resolution, and who is responsible to complete the problem. This log should be reviewed at the end of the test or after normal operation resumes in the event of an actual disaster for any new procedures that may need to be implemented in the future to avoid similar problems from occurring.

Only problems that require applications team intervention should be recorded in this log. Banking consultants should also keep an additional log of all calls they receive and answer.

## **Recovery Procedures for a Major Disaster**

---

### **7.3.3 Normalizing Procedures**

Documentation for normalizing procedures for each division can be found online at [dr.dhiprovo.com](http://dr.dhiprovo.com) and on SharePoint.

### **7.3.4 Equipment Salvage or Replacement by Equipment Team**

The Equipment team will assemble at the DHI building, determine what if any of the equipment is salvageable. The Equipment team work together to get equipment salvaged and into operation. Equipment which is not salvageable will be replaced either by new equipment or used from dealers listed in the suppliers' section of Appendix E.

### **7.3.5 Facilities Salvage or Replacement by Facilities Team**

The facilities team will work with our suppliers to determine the extent of damage and the necessary repairs, etc. The facilities repair/replacement decisions will be made by the Executive Committee upon recommendation of the Facilities team.

### **7.3.6 Administrative Coordination by Administrative Team**

The administrative team's mission is to provide all administrative support for the business recovery process. DHI Payroll is the top priority. In the recovery process, many employees will be away from their families. Payroll continuity is of utmost importance. The administrative team is to work to reduce any stress which might be encountered by staff members as a result of the recovery process.

## **7.4 Specific Procedures for Functional Operations**

This section contains specific procedures for ongoing operation of business functions at the Emergency Control Center site.

## **Recovery Procedures for a Major Disaster**

---

### **7.4.1 NCC Alternate Site Procedures**

Network Control Center personnel will be responsible for set up and operation of the networking and virtualized computing infrastructure at the alternate DR site. NCC will perform the following listed functions under the supervision of the Emergency Control Center Coordinator as well as any other assignments made by the Emergency Control Center Coordinator.

- 1) Attend and participate in the initial planning meeting. Assist in setting up the job status board and take assignments.
- 2) Break any storage replication to the primary storage at the Provo data center and enable storage for attachment to the virtual hosts.
- 3) Change host servers from standby to recovery configuration, attach to replicated storage and configure virtual networking.
- 4) Change DR site routers and switches from standby configurations to recovery configuration.
- 5) Assist recovery teams in configuring and powering up restored systems.
- 6) Monitor the network for proper operation and assist users with any equipment or procedure problems.

#### **Network Recovery Concepts**

Recovery of the data communication network from the Tonaquint datacenter is done via VPN. NCC configures a VPN appliance at the alternate DR site to accept connections from end client VPN routers. Client routers should each have a backup configuration that will establish a connection to the DR site when activated. Clients should use their same procedures developed during the certification process to connect to the contingency site. Those who are unfamiliar with their procedures should consult their written instructions for disaster recovery. A copy of the client's recovery plans is kept in DHI Disaster Recovery Box #1 and can be consulted if the client is having difficulty.

Most systems should immediately come active and begin to communicate as soon as a VPN connection is established. NCC personnel should check each client as they come up and verify that they have connected properly.

Most systems should immediately come active and begin to communicate as soon as a VPN connection is established. NCC personnel should check each client as they come up and verify that they have connected properly.



## **Recovery Procedures for a Major Disaster**

---

### **7.4.2 Support Console Installation**

Operations support consoles are accomplished through Sierra Studio. See operations documentation for the use of Sierra Studio as a support console.

### **7.4.3 Specific Procedures for Setup of Recovery Systems**

For testing only; all replication suspending and resuming operations should be done from the Hitachi disk farm in Provo. In an emergency that renders the Hitachi disk farm in Provo inoperative, all prep work will be done to the disk farm in the TDC.

#### **Suspending Replication**

Using a web browser, log on the G400 disk array in Provo through Hitachi Storage Navigator. The URL is:

<https://10.0.57.46/dev/storage/834000440420/emergency.do>

Click on replication->Remote Replication->UR Pairs...

This will display the Paired LUNs (note: the term LUN and LDEV are interchangeable). Place a check mark in the box of all paired LUNs and click on "Split Pairs". A dialog box will come up showing all the pairs to be split. At the bottom of this box click on the radio button to "Enable Secondary Volume Write" and click finish. In the next box verify that all LUNs in the "Secondary Volume Write" column show "Enabled" and split mode column show "Flush" then click Apply.

Upon completion of the task all LUNs should show a status of PSUS. The Secondary LUNs are now ready to be used.

#### **Resuming Replication**

Using a web browser, log on the G400 disk array in Provo through Hitachi Storage Navigator. The URL is:

<https://10.0.57.46/dev/storage/834000440420/emergency.do>

Click on replication->Remote Replication->UR Pairs...

This will display the suspended LUNs. Place a check mark in the box of all suspended LUNs and click on "Resync Pairs". A dialog box will come up showing all the pairs to be re-synced. Click "Finish" then "Apply".

Upon completion of the task all LUNs should show a status of "Copy".

Once the replication is caught up, all LUNs should show a status of "Pair". This may take hours to days

## Recovery Procedures for a Major Disaster

---

depending on disk activity and split time.

Pair – The LUNs are fully replicated.

PSUS – Replication has been suspended.

Copy – The LUNS are in a state of Syncing, progress is shown as a percentage.

In the event a forensics firm is needed to assist in the recovery process then you may use Richard Hickman. He may be reached at 385-282-5461.

### 7.4.4 Procedures to Acquire Supplies at Remote Site

#### Procedure to Procure Paper

We use 20 pound weight paper. You will need to get equal amounts of three hole punch paper and non-punched paper per day, depending on if you are going to have statements to print. (We average approximately 10 cases per week.)

Call the following vendors:

**First**        Xerox  
                 675 East 500 South  
                 Salt Lake City, UT 84102  
                 Metered Supplies (800) 822-2200  
                 HLC Colored Toner (800) 822-2200  
                 Acct. #691069462

**Second**     Printworks  
                 Mike Olsen - Sales Representative  
                 (801) 367-6172  
  
                 Domtar – Stock Paper  
                 (800) 458-4640 option 4

## **Recovery Procedures for a Major Disaster**

---

Customer number: 200955

**Third**      Dixon Paper  
Mark Green - Sales Representative  
(800) 662-4228

**Fourth**     Zellerbach Paper Company  
Boyd Edmond - Sales Representative  
(800) 662-6800

Any one of these vendors supply the type of paper we use and have the connections to get it to the address we provide them with.

### **Additional Vendor**

DTC Computer Supplies  
9033 9th Street  
Rancho Cucamonga, CA 91730  
Contact – Nick Kingsley  
(909) 466-7680

This vendor supplies CDT checks, MICR toner, 3592 tapes, HP toner, DVDs – CDs. Most local vendors carry other brands, i.e., 3M, Scotch, Carlisle. Provide the vendor with proper shipping address and they will get it there.

## **7.5 Procedures for Replacement of Business Facility**

If the facility is destroyed, steps will be taken immediately to establish a replacement facility. A location must be found with adequate space; the space must be constructed or modified; and PCs, equipment, air conditioners, power distribution equipment, cabling, etc., must all be obtained and installed to prepare a working business site.

### **Procedures**

- 1) The Facilities and Equipment teams have contingency plans that identify potential replacement sites and

## **Recovery Procedures for a Major Disaster**

---

probable means of obtaining equipment and facilities on an emergency basis. These plans include written agreements from the various vendors.

- 2) If equipment or facilities are salvageable, the Equipment and Facilities teams will assess what is usable or repairable and what needs to be replaced. They will initiate all salvage, relocation, and repair activities as necessary.
- 3) The Equipment and Facilities teams will initiate ordering of all new replacement equipment and facilities on an emergency (rush) basis. Financial, legal, and insurance issues will be dealt with in this process.
- 4) As the new facility is constructed and equipment arrives, the Equipment and Facilities teams will coordinate obtaining permits, installation, wiring, etc., to ensure that the facility is properly prepared.
- 5) Equipment and Facilities teams will test the readiness of the new facility. When it is ready, they will coordinate with the Operations team to transfer operations from the Emergency Control Center site to the new facility.
- 6) The procedures will be complete when all problems with the new facility have been resolved and operations have been normalized.

### **7.6 Procedures for Return to Normal Operations**

The following procedures are for returning to normal operations after contingency operations.

#### **Procedures**

- 1) When the business operation is transferred back either to the original facility or to a new replacement facility, employees are to be kept informed. This is the job of the Emergency Coordinator. Operations staff, users, and management all have an interest and a need to know what is happening. There must be understanding and coordination of changes.
- 2) As the business operation is transferred back, the contingency operation will very quickly be phased down. The Operations team is responsible to leave the Emergency Control Center site with all property

## **Recovery Procedures for a Major Disaster**

---

and materials belonging to the organization, and to use due care and caution to protect all assets.

- 3) The Emergency Coordinator and Contingency team are responsible to maintain a full state of readiness during and particularly after returning to normal operations.
- 4) An official statement will be made to all employees stating that the emergency is over and that operations are now or soon will be returned to normal. The Emergency Control Center will be deactivated.
- 5) The final activity of the disaster recovery process, will be the meeting and debriefing of the Contingency team, all Coordinators, and Action teams concerning the activities of the disaster recovery. The Emergency Coordinator is responsible to make sure that events, problems and solutions, etc., are documented. Once documentation has been completed, the action teams and Contingency team can be deactivated. During the next review of the plan, the Emergency Coordinator will be responsible to ensure that any lessons learned are incorporated into the plan.

## CHAPTER 8 TESTING AND MAINTENANCE OF THE PLAN

The Contingency Recovery plan is not considered complete and final until it has undergone Acceptance Testing. The testing verifies that all facets of the plan have been implemented and have been found to be accurate and sufficient. After initial acceptance of the plan, ongoing testing on a periodic basis is necessary to ensure the continued viability of its contents. The plan must also be reviewed regularly and updated as necessary. This section deals with these issues by providing policies and procedures for testing the plan and for periodic review and update of the plan.

### 8.1 Policies and Procedures for Testing

The organization will enforce the following policies and procedures governing testing of the plan.

#### Policies

It is important for the emergency teams to remain familiar with the Contingency Plan; the Emergency Coordinator is responsible for conducting one or more tests each year following the release of the plan.

#### Procedures

- 1) By October 1 of each year, in conjunction with the process of review and update of the plan, the Emergency Coordinator will design, schedule and notify team members of the test dates for the next year. The tests may vary from year to year, in order to evaluate different elements of the plan, but at the least it must address all major procedures involving all teams and must test the ability to function at the contingency site.
- 2) The tests may be organized as several different tests during the year, each testing a different portion of the plan. However, at least once annually the plan must be tested. Departments should emphasize recovery procedures in the planning and implementation of new systems. Techniques learned during these types of operations can be very useful during disaster recovery.
- 3) The tests are to be regarded as review and training exercises as much as tests of the workability of the plan. However, there will always be some features of the plan which are truly tested. This means that the tests must be observed, measured, and all successes and failures recorded. A test monitor will be appointed by the Chief Technology Officer for each scheduled test. During the progress of the test, if problems are encountered, solutions will be sought at that time.
- 4) Each year ALL critical functions will be tested at the contingency site to verify that no technical problems prevent those services from working.
- 5) The tests will extend over a fairly limited time period - normally one or two days - so as not to have an undue impact on other business activities.
- 6) Following the tests, the Emergency Coordinator will document the results of the tests, including any recommended changes in the plan. The test results will then be reviewed and approved by the Chief Technology Officer. The test results will be reported to the Board of Directors in written form. For each problem encountered, the current status and responsible party will be reported.
- 7) After the test report is prepared, the results of the test will be reported to participating clients by the department responsible for the client's applications.
- 8) The individuals involved in each test will meet periodically as needed to determine the current status of all problems encountered during the test. All problems will be tracked until they have been closed and

---

## Testing and Maintenance of the Plan

---

procedures or programs have been changed to correct the problem. Changes to the Contingency Plan which result from the testing process will be incorporated along with the changes from the semi-annual review process (see Section 8.2).

### 8.2 Policies and Procedures for Review and Update

The effectiveness of the contingency plan is impacted by changes in the environment that the plan was created to protect. Some major factors which will impact the plan are: new equipment, changing business environment, staff and organizational changes, and new or changing functions.

The following policies and procedures have been developed to ensure that the plan is reviewed and updated on a regular and reliable basis.

#### Policies

Once per year the Contingency Plan will be reviewed by the Emergency Coordinator and approved by the Chief Technology Officer. For scheduling considerations, the plan will be reviewed and revised by July 31 of each year.

#### Procedures

- 1) The Emergency Coordinator will appoint a review team of one or more people each year to review and update the Contingency Plan.
- 2) When the review team has completed their review and update process, the Emergency Coordinator will also review and approve the revised plan.
- 3) Once approved by the Emergency Coordinator, the revised plan will be submitted to the Chief Technology Officer, by the date required by the Review Policy, for final approval.
- 4) The revised plan (after review and update) will be used as the basis of the annual test. Updates must be distributed prior to the test. However, the tests themselves may also identify changes to the plan; therefore, final distribution of updates will occur following the tests.
- 5) The Emergency Coordinator will then direct the Alternate Coordinator to distribute the revisions to the plan. To avoid confusion, the plan will be entirely reprinted after each update. It will be distributed to those individuals and client institutions that have been registered for a copy of the plan.
- 6) More frequent reviews/updates of the plan may be initiated by the Emergency Coordinator, but shall require the approval of the Chief Technology Officer because of probable impact on other projects.

## **CHAPTER 9      CLIENT DEMONSTRATION AND CERTIFICATION OF READINESS**

### **Policy**

Due to the limited resources available when a disaster situation occurs, it is important to use the available resources in the most efficient way to support our clients. To maximize our use of available resources, we have established the following policy:

1. Clients who have the highest level of certification will be connected first. They should require the least time to connect per terminal to be recovered.
2. Clients who have tested the most recently will be connected next. They have current written recovery procedures and are recently experienced with the process of recovering their work.
3. Clients who have tested at some time will be connected next. They should have written recovery procedures and should have experience at some time in the past recovering their work.
4. Clients who have never tested will then be recovered if resources are available and they have the necessary facilities (Modems, lines, etc.). It should be noted that the probability of the recovery of this group is very low because they have never tested.

### **Planning**

Each of our clients need to analyze their risks and needs for disaster recovery. Contingency planning must include more than the data center and its operations. Fire, earthquake, floods, power failures, and even civil unrest can affect one or more of our clients' offices with no advance notice. While the data center could be perfectly safe, the client could be unable to operate their business normally due to one of these or some other event. While the probability of a major disaster is fairly low, the effects of even small events that interrupt normal business operation can be devastating to an institution.

Clients must have a plan in place that assesses the relative risks for each type of disaster and outlines the actions to be taken. Command structures, phone numbers, and contact lists must be maintained to allow the institution to recover from extraordinary events and continue serving their customers. An adequate plan must cover the full range of problems, from those that affect only one office to those which affect the entire client institution. The effectiveness of the plan is determined by testing parts of the plan on a regular basis. The data processing parts of the plan can be tested almost any time with VPN connections to the DHI data center in Provo. Full recovery tests, which allow the client to link with the backup recovery site, can be done during the annually scheduled test dates. Additional test dates can be made available with the responsibility of who pays for the test to be determined by DHI management.

Good plans will include defined responses from employees to customers for each type of problem that may occur. The attitude and responses given by the client's employees to customer questions will largely determine the public perception of the client institution's integrity and responsibility. When problems occur, the customer is very seldom concerned with who is at fault. The customer wants to know who will fix the problem, when it will be fixed, and when they can do business with the institution on a normal basis. Good plans focus on strategies for avoiding or minimizing risks.

It is the responsibility of the client institution to do risk-based planning to determine the comparative risks of potential contingencies and costs to minimize those risks. Operations management should assess the risk to the continued health and existence of the client institution and its customer base for each type of disaster. Planning should then reflect the client institution's strategy to use its resources to minimize these risks. Effective contingency plans are a way of doing business, not something that is written and put up on a shelf to fulfill an outside requirement.



## Client Demonstration and Certification of Readiness

---

### Certification

As a Service Bureau, we must require our clients to be actively participating in the preparation and testing of the Contingency Plan. In order to allow clients to demonstrate their readiness to participate as a partner with DHI in the recovery process, standards have been established. The standards have been placed into groups of increasing levels of preparation and readiness. The higher readiness levels demonstrate a greater participation in the planning and testing process. As the level of readiness increases, the chance of success for recovery of the client's business functions also increases. Each client can determine their readiness to recover business activity in the event of a disaster based on their certification at the various levels of recovery capability. Application departments may issue certificates showing the clients level of readiness.

Network attachment certification may be done any business day based on the workload at DHI. Scheduling a test with the Tonaquint Data Center is at our discretion. No one at the remote site is involved in the test. We can schedule the test based on DHI's and our customer's convenience.

Clients will receive a certification score after participating with DHI in a scheduled test. The level of certification is based on the following criteria:

- Whether institution's backup equipment is tested with Provo annually.
- Whether institution participates with DHI in an annual test and executes required number of transactions.
- Whether institution has documented disaster recovery plans, updates them annually and original plans are reviewed by DHI.
- Certificate of Annual Review is received by DHI that disaster plan has been reviewed and updated.

DHI replicates all client's data files. DHI also contracts with Tonaquint Data Center and we have equipment always available in the event a disaster occurs at the DHI-Provo location. These services are rendered to all clients regardless of their certification level.

Clients who have previously qualified for a level of certification may be placed in a lower level if they fail to maintain certification requirements for the higher level.

### 9.1 Level 0

This level includes all clients that have failed to certify at any level of readiness. Clients who fall into this category have not tested with DHI or demonstrated any disaster recovery planning.

Summary:

There are no requirements for this level of certification.

### 9.2 Level 1

Clients certified at Level 1 have backup communications equipment and have tested their backup equipment annually with NCC in Provo. Clients at this level have not prepared their own formal disaster plans.

Summary:

1. Client has acquired and tested backup communications equipment.
2. Client lacks a formal disaster recovery plan.

---

## Client Demonstration and Certification of Readiness

---

### 9.3 Level 2

Clients certified at this level have certified each of their offices at Level 1, and they have participated in the annual disaster recovery test.

Summary:

1. Client has acquired and tested backup communications equipment.
2. Client participated in the test and executed the required number of transactions.
3. Client lacks a formal disaster recovery plan.

### 9.4 Level 3

Clients at this level have certified all their office locations at level 2. They have prepared their own disaster recovery plan, and they have had DHI review the plan completeness. They have not provided DHI with the Certificate of Annual Review (see Appendix K) because they may not have updated their disaster plans or tested their plan as required.

Summary:

1. Each location has certified at level 2.
2. Client has documented disaster recovery plan.
3. Client failed to update own disaster plan.

### 9.5 Level 4

This category includes all clients who have certified at Level 3. Clients at this level have prepared their own disaster recovery plans, complied with the requirements associated with the Certificate of Annual Review (see Appendix K), and sent a copy of the Certificate of Annual Review to DHI prior to November 30th.

Summary:

1. Client has tested backup communications equipment.
2. Client has participated in the annual test.
3. Client has prepared formal disaster recovery plans.
4. Client has sent a Certificate of Annual Review to DHI.

## **Client Demonstration and Certification of Readiness**

---

**This page intentionally left blank.**

## APPENDIX A      EMERGENCY NOTIFICATION & CALLING TREE

### Service Numbers

<u>Emergency Service</u>	<u>Organization</u>	<u>Telephone Numbers</u>
POLICE	Provo City	<b>911 Emergency Number</b> 801-852-6210
FIRE DEPARTMENT	Provo City	<b>911 Emergency Number</b> 801-852-6300
AMBULANCE SERVICE	Provo City	<b>911 Emergency Number</b>
BUILDING MANAGEMENT		801-429-2100 - Dial 0 for operator
Physical Facilities	Jeffrey Abbott	801-344-6431 (DHI Office)
		801-400-5935 (Cell)
Computer Room	Melissa Carpenter	801-429-2150 (Computer Room)
		801-404-2965 (Cell)
		801-429-2151 (Alternate)
ADDRESS OF OUR BUILDING:		1525 West 820 North Provo, UT 84601 801-429-2100

### Contingency Team (Emergency Notification List)

Executive Member - Leader	Dirk Baum, CTO
Executive Member	B. Lynn Crandall, President & CEO
Emergency Coordinator	Gilbert Porter, Assistant Vice President, Internal Services
Alternate Emergency Coordinator	Scott Howell, Operations Manager, FPS GOLD
Member	Yancy Barnett, Systems Programming, Internal Services
Emergency Control Center Coordinator	Ken Jorgensen, SVP/CRO, GPS
Alternate Control Center Coordinator	Doug Carpenter, Assistant Vice President, Internal Services
Member	Stuart Nelson, Senior Network Engineer

Note:      There are only names in this list. Addresses and phone numbers are listed in the Master Employee List found in Appendix C.

## **Appendix A - EMERGENCY NOTIFICATION & CALLING TREE**

---

### **Emergency Action Team Lists**

#### Emergency Action Teams

Technical Support Team

Operations Team

Applications Team - FPS GOLD

Applications Team – GOLDPPoint

Applications Team - Amelikor

Equipment Team

Facilities Team

Administrative Team

Communications & Logistics Team

Web Recovery Team

#### Designated Team Leaders

Yancy Barnett, Systems Programming, Internal Services  
Gil Porter

Melissa Carpenter, Manager, Computer Operations  
B. Lynn Crandall

Steve Carter, Senior Vice President, FPS GOLD Programming  
Mark Benson

Walt Whitaker, Vice President Operations/Releases GPS  
Ron Cloud

Neil Thompson, Programming Supervisor, Amelikor  
Karl Child

Melissa Carpenter, Manager  
Dirk Baum

Jeffrey Abbott, Manager, Facilities

B. Lynn Crandall, President/CEO, DHI Computing Service  
Dirk Baum

Val Thurston Manager of Training and Logistics  
Randy Palmer

Jeff Foster, Internet Specialist, Amelikor  
James Frazee

#### **TECHNICAL SUPPORT TEAM**

Gil Porter - Leader  
Yancy Barnett  
Doug Carpenter

Assistant Vice President, Internal Services  
Systems Programming, Internal Services  
Assistant Vice President, Internal Services

#### **OPERATIONS TEAM**

Melissa Carpenter - Leader  
Lynn Chesnut  
Carry Squire  
James Draughn

Manager, Computer Operations  
Lead Operator, Computer Operations  
Computer Operations  
Computer Operations

#### **APPLICATIONS TEAM - FPS GOLD**

Steven Carter - Leader  
Mark Benson

Gloria Kimbal

Senior Vice President, FPS GOLD Programming  
Vice President, FPS GOLD Programming  
Programming Procedures Manager, FPS GOLD Programming  
Vice President, FPS GOLD Programming

#### **APPLICATIONS TEAM – GOLDPPoint**

Ron Cloud - Leader  
Walt Whitaker  
David Fietkau  
Rob Jacobson

Senior Vice President, Servicing  
Vice President Operations/Releases GOLDPPoint Systems  
CIO/SVP over Product Development  
Programmer/Analyst, GOLDPPoint Systems Programming

## **Appendix A - EMERGENCY NOTIFICATION & CALLING TREE**

---

### **APPLICATIONS TEAM - Amelicor**

Neil Thompson – Leader  
Karl Child

Programming Supervisor, Amelicor Programming

### **EQUIPMENT TEAM**

Melissa Carpenter  
Dirk Baum

Manager, DHI Computing Service

### **FACILITIES TEAM**

Jeffrey Abbott  
Dan Hopkinson

Building Manager, DHI Computing Service  
Building Maintenance

### **ADMINISTRATIVE TEAM**

B. Lynn Crandall  
Matt De Visser  
Gary Allen  
Dirk Baum

CEO/Executive VP, DHI Computing Service  
President, FPS GOLD  
Senior Vice President, FPS GOLD  
Senior Vice President, Internal Services

### **COMMUNICATIONS AND LOGISTICS TEAM**

Val Thurston - Leader  
Kent Chauncey  
Randy Palmer

Manager, Training and Logistics  
Manager, Technical Communications  
Manager, Training and Logistics

### **WEB RECOVERY TEAM**

Jeff Foster – Leader  
James Frazee  
Glen Twede  
Lee Day  
DJ Heap

Internet Specialist, Amelicor  
  
Administrative Auditor, DHI Computing Service  
President, Amelicor  
Programmer/Analyst, DHI Computing Service

## **Top Management Notification List**

### Position

President/CEO DHI Computing Service, Inc.  
Senior Vice President, Internal Services  
President, FPS GOLD  
Senior Vice President, FPS GOLD  
President, GOLDPoint Systems  
President, Amelicor

### Name

B. Lynn Crandall  
Dirk S. Baum  
Matt De Visser  
Steve Carter  
Jeff Collinsworth  
Lee Day

## **Appendix A - EMERGENCY NOTIFICATION & CALLING TREE**

---

### **Management Succession List**

The following is the plan for management succession in the order listed, in the event of disability or absence of top management:

The board of directors has listed the following management succession policy.

If Lynn Crandall is not available, contact one or all of the four management committee members:

Kyle Crandall  
Dirk S. Baum technical questions  
Jeff Collinsworth customer service and marketing questions  
Matt De Visser customer service and marketing questions  
Gary Allen financial questions

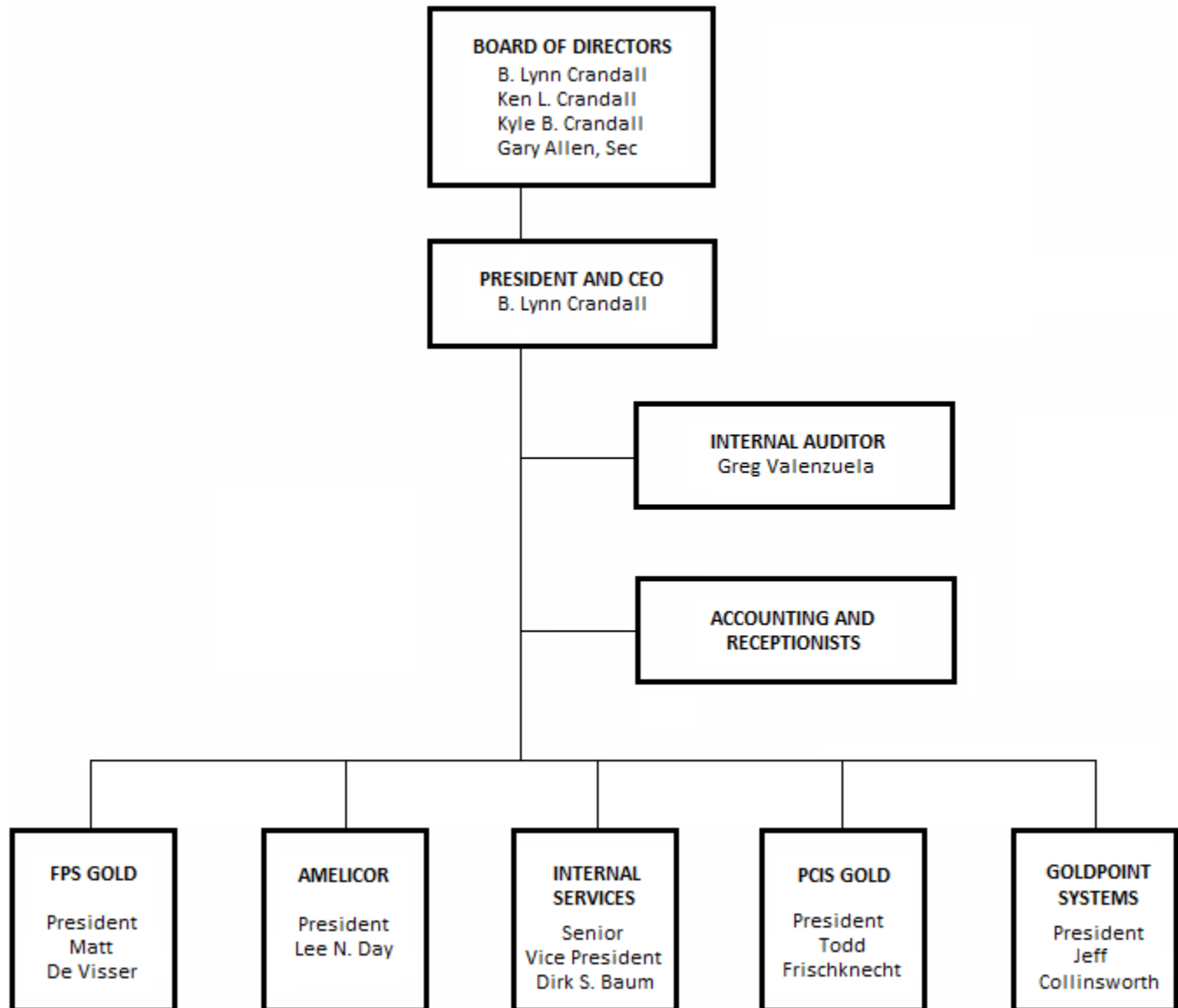
If they are not available, contact: Lee Day

### **Contingency Site**

NAME -	Tonaquint Data Center
ADDRESS -	1108 W 1600 S St George, UT 84770
CONTACTS -	Phil Daily, Chris Howard
TELEPHONE -	1-435-628-6164 main number 1-435-628-7926 support

## APPENDIX B DHI COMPUTING SERVICE ORGANIZATION CHART

### DHI COMPUTING SERVICE, INC. June 2018





## **Appendix B – DHI Computing Service Organization Chart**

---

**This page intentionally left blank.**

## **APPENDIX C     DHI EMPLOYEE ADDRESS BOOK (DHI ONLY)**

**This page intentionally left blank.**

## **Appendix C – DHI Employee Address Book**

---

**This page intentionally left blank.**

## **APPENDIX D    CUSTOMER CONTACT LISTS (DHI ONLY)**

**This page intentionally left blank.**

## **Appendix D – Customer Contact Lists (DHI ONLY)**

---

**This page intentionally left blank.**

## APPENDIX E      VENDOR CONTACTS

<b><i>Company</i></b>	<b><i>Contact</i></b>	<b><i>Number</i></b>
AES Alarm Systems	Sergio Gonzalez	(801) 491-3804 (Office)
		(801) 836-0121 (Cellular)
	Scott Woodard	(801) 358-4150 (Office)
		(801) 836-8656 (Cellular)
	Dave Erickson	(801) 377-5677 (Office)
		(801) 787-4380 (Cellular)
AT&T (Leased Lines)		(800) 325-1230
AT&T (Switched 56K)		(800) 367-7956
AT&T Main SLC	Shane Berg (Account Rep)	(801) 237-1056 (Office)
Addmaster Corp.	Roberta Ryhal (Rcpt/Valid Printer)	(626) 358-2395
Attorney	Ken Birrell	(801) 328-3600
Baltimore Technologies	Stacey McBride	(425) 460-6000
Cache Valley Electric	Eric Luther (Cisco sales)	(801) 231-9646
CDW (PC hardware and software)	Ryan Mapili	ryanmap@cdw.com
CenturyLink(Utah)	Data Circuit Repair	(801) 237-6710
		(801) 575-1012
		(801) 575-1079
CenturyLink	David Cook (Sales)	(801) 703-3762 (Mobile)
		(801) 575-1043 (Office)
Christensen Oil	Todd Christensen (UPS Fuel) 1828 N. 2000 W. Provo	(801) 373-7970 (Office)
		(801) 374-8607 (Home)
Cisco Tech Support		(800) 553-2447
Coda Technologies	Danny Hafen	(801) 200-1505
CompuCare Canada	Calvin Perkins (PC hard/soft)	(415) 861-8837 (Fax)
Computer System Products	Paul Granovski (Cables)	(800) 422-2537 ext. 352
Data Comm Warehouse	(Mail order PC products)	(800) 328-2261
Dialogic Computer Center	Jean Caulfield (Voice/GOLDPhone adapters)	(800) 755-4444
Digi, Inc.	(T1 Comm. Cards)	(800) 344-4273
Diversified Insurance Brokers	Matt Henriod (Ins. Agent)	(801) 325-5000
		(801) 325-5020 (Office)
		(801) 201-4077 (Cellular)

---

	Sharri Baker Don Sparks (Benefits/Health Plan) Utah	(801) 583-8125 (Home) (801) 325-5021 (Office) (800) 325-5070 (Office) (888) 244-1212 (Toll-Free Number)
Domtar Paper	Customer Number 200955	(800) 458-4640 option 4
DTC Computer Systems	Nick Kingsley Toner and other supplies	(909) 466-7680
Elan-US Bank	Processor DPC470	(877) 935-2637 option 1 then 0# then 5
FDR, Inc.	(Give "Link #1" or "Link #2")	(800) 288-8774, Opt. 1
Firetrol	Rep: Bannon Alarms: Mike	(801) 414-2772 (385) 415-4210
First Data-Star	Processor LMC 22W	(888) 377-8726 opt. 1 then 1 then 1
Fiserv EPOC	Processor FPSP-EPOC	(800) 336-6955 opt. 1
FRB	Fedline Fedline ACH Check 21 Services	(888) 333-7010 (866) 234-5681 (877) 372-2457
Gunthers Comfort Air	Ken	(801) 756-9683 (801) 592-6227 (Cell)
High Point Plumbing	Greg	(801) 787-6369
Hitachi Data Systems	Shawn Kearns	(801) 815-8388
Hitek Security	Fred Fullmer	(801) 224-4775
IBM	All service calls	(800) IBM-SERV
IBM Credit	Susan Birrell	(602) 217-2522
IBM National Parts Ctr. IBM NDD	Deon Harris (Serv/Warranty parts) Scott Stewart (PC Marketing)	(303) 924-4125 or (800) 388-7080 (800) 426-7272
IBM Partner Choice	JoAnne Ballard	(800) 755-9652 ext. 6309
IGS	Nick Paul	(435) 849-4514 (Cell) (801) 450-0403 (Cell)
Ingram Micro	Devan Dunbar (PC hard/soft)	(800) 456-8000 x 25478
Intermountain Door	Warehouse roll-up door	(801) 224-2649
Lexmark International	(PC printers marketing support)	(800) 453-9872
Linford Plumbing	Van	(801) 360-7970

---

---

Microsoft Support		<a href="http://support.microsoft.com">http://support.microsoft.com</a>
Moore Business Forms	Debbie Bachman Kirt Cutler	(801) 333-7219 (801) 333-7216
Neopost – Rocky Mountain	Erik Andersson	(801) 367-1540 (801) 487-8508 (Office)
New Riders Publishing	Richard Hopkins	
Optimum Data	Joe Turco (AT&T/Paradyne MODEMs)	(800) 879-8795
Pinacor/Microage	PC hardware/software	(800) 528-1415
Printworks	Mike Olson	(801) 367-6172 (Cell) (801) 855-5556 (Office)
Provo City Power Outage		(801) 852-6868
Response Envelope	Randy Nelson Teresa Rivera	(801) 455-2151 (909) 923-1327
Robertson Electric	Jed	(801) 857-1771
Shazam-ITS Inc	Processor DPC 188	(800) 333-1204
Sirius Computer Solutions	Dan Jensen  Kevin Ririe	(801) 736-9109 (Office) (801) 964-4907 (Cell) (801) 485-6348 (Fax) (801) 231-8991 (Cell)
Skyline Computers	Chris Cortese Comm. Equip., Mainframes,	(800) 375-9546 (Main Office) (888) 730-9795 (House Office)
SkyMail	Jason Hermanson	(801) 557-1843 (801) 977-8900 (Office)
Sunbelt Software		(877) 673-1153
Sunco Electric	Will Sunderland	(801) 360-8553
State Farm Auto Ins.	Steve Wilson	(801) 798-9288 (801) 798-8170 (Home)
Symantec	Brian Bauman	(800) 388-3858 ext. 2346
Tech Connect	Chris	(801) 298-9087 (801) 718-6655 (Cell)
Tech Data	(PC hardware/software)	(800) 453-5978
ThyssenKrupp Elevator	Kyle	(801) 908-7433 (801) 509-0782 (Cell)

---



---

Top Gun	Connie Csizmadia	(203) 220-9436
Troy Systems International, Inc. Printer Vendor		(800) 944-6757
Vantiv-5/3	Processor FPS1 [FPS], FPS2 [GPS]	(866) 851-0026 opt. 3
Verizon		(800) 483-5000
Village Systems	Dan Mastenbrook	(800) 362-0321
Wall Data	Dan Outcault (Rumba software)	(800) 927-8622
Xerox	George Gastelo Mark Dixon  Consumables  Salt Lake City National Hardware Number National Software Number	(801) 216-4816 (Client Account Manager) (801) 641-8758 Customer ID 711103929 (800) 822-2200, option 2 then 1 Customer # 691-069-462 (801) 535-8521, contact Greg (800) 821-2797 (800) 822-2979
<b><i>Product</i></b>	<b><i>Vendor</i></b>	<b><i>Contact Information</i></b>
Elixir Suite for AFP	Xerox	Refer to information above
Kedit	Mansfield Software Group	(860) 429-8402 www.kedit.com
Textpad.com		www.textpad.com
Araxis Merge	BMT Micro, Inc.	(800) 414-4268
PC Anywhere	Symantec	(800) 388-3858 ext. 2346
WS_FTP Pro	Ipswitch, In.	www.ipswitch.com
Zip Magic	Ontrack	(800) 645-3649

## APPENDIX F EQUIPMENT CONFIGURATION – TONAQUINT SITE

Equipment Type	Name	Purpose/Function	Notes
Switch	Brocade 7800	Network switching	
Router	Cisco 4321	Network routing	
Switch	Cisco C9300	Replication	
Firewall	Cisco ASA5525	VPN concentrator	
Firewall	Cisco ASA5525	Web server firewall	
Firewall	Cisco ASA5545	Core firewall	
Switch	Cisco 9000	Fibre Channel Switch	
Switch	Cisco 9000	Fibre Channel Switch	
Switch	Cisco 9K	Core Switch	
Switch	Cisco 9K	Core Switch	
Switch	Cisco 2960	Management switch	
Switch	Cisco 2960-XR	Network connections	
Switch	Cisco 2960-XR	Network connections	
Disk Array	HDS G400	Backup Disk Array	150 TB
Cisco UCS	UCSB-B200-M4	Server Blade	16 cpu 512 gig
Cisco UCS	UCSB-B200-M4	Server Blade	16 cpu 512 gig
Cisco UCS	UCSB-B200-M4	Server Blade	16 cpu 512 gig
Cisco UCS	UCSB-B200-M4	Server Blade	16 cpu 512 gig
Cisco UCS	UCSB-B200-M4	Server Blade	16 cpu 512 gig
Cisco UCS	UCSB-B200-M4	Server Blade	16 cpu 512 gig
Cisco UCS	UCSB-B200-M4	Server Blade	16 cpu 512 gig
Cisco UCS	UCSB-B200-M4	Server Blade	16 cpu 512 gig
Cisco UCS	UCSB-B200-M4	Server Blade	16 cpu 512 gig
Cisco UCS	UCSB-B200-M4	Server Blade	16 cpu 512 gig
Rubrik	R348	Backup Appliance	96 TB

## **Appendix F – Equipment Configuration – Alternate Site**

---

**This page intentionally left blank.**

## APPENDIX G EQUIPMENT CONFIGURATION - PROVO SITE

Equipment Type	Name	Purpose/Function	Notes
Switch	Brocade 6510	Network switching	
Switch	Brocade 6520	Network switching	
Switch	Brocade 7800	Network switching	
Switch	Cisco 3750X	Network switching	
Switch	Cisco 9K	Client Vlans	
Switch	Cisco 9K	Client Vlans	
Router	Cisco 1921	Network routing	
Switch	Cisco C9300	Replication	
Firewall	Cisco ASA5525	VPN concentrator	
Firewall	Cisco ASA5525	Web server firewall	
Firewall	Cisco SFR4110	Core firewall	
Switch	Cisco 4500	Network switching	144 ports
Switch	Cisco 4500	Network switching	288 ports
Switch	Cisco 3850	Network switching	432 ports
Switch	Cisco 3750	Network switching	192 ports
Switch	Cisco 3560	Network switching	144 ports
Router	Cisco 2921	Internet routing	
Router	Cisco 3925	Internet routing	
Router	Cisco 2921	Internet routing	
Disk Array	HDS G400	Primary Disk Array	180 TB
Tape Library	IBM3310	Primary Backup Library	
Cisco UCS Main Cluster	UCSB-B200-M4	Server Blade	28 cpu 560 gig
Cisco UCS Main Cluster	UCSB-B200-M4	Server Blade	28 cpu 560 gig
Cisco UCS Main Cluster	UCSB-B200-M4	Server Blade	28 cpu 560 gig
Cisco UCS Main Cluster	UCSB-B200-M4	Server Blade	28 cpu 560 gig
Cisco UCS Main Cluster	UCSB-B200-M4	Server Blade	28 cpu 560 gig
Cisco UCS Main Cluster	UCSB-B200-M4	Server Blade	32 cpu 640 gig
Cisco UCS SQL Cluster	UCSB-B200-M4	Server Blade	16 cpu 256 gig

---

Cisco UCS SQL Cluster	UCSB-B200-M4	Server Blade	16 cpu 256 gig
Cisco UCS SQL Cluster	UCSB-B200-M4	Server Blade	16 cpu 256 gig
Cisco UCS SQL Cluster	UCSB-B200-M4	Server Blade	16 cpu 256 gig
Cisco UCS Voice Cluster	UCSB-B200-M4	Server Blade	20 cpu 128 gig
Cisco UCS Voice Cluster	UCSB-B200-M4	Server Blade	20 cpu 128 gig
Cisco UCS Voice Cluster	UCSB-B200-M4	Server Blade	20 cpu 128 gig
Cisco UCS Voice Cluster	UCSB-B200-M4	Server Blade	20 cpu 128 gig
Cisco Cluster	UCSB-B200-M4	Server Blade	16 cpu 256 gig
Cisco Cluster	UCSB-B200-M4	Server Blade	16 cpu 256 gig
Cisco Cluster	UCSB-B200-M4	Server Blade	16 cpu 256 gig
Rubrik	R348	Backup Appliance	96 TB
Rubrik	R3410	Backup Appliance	120 TB

## Appendix H – SOFTWARE CONFIGURATION

### Server Environment

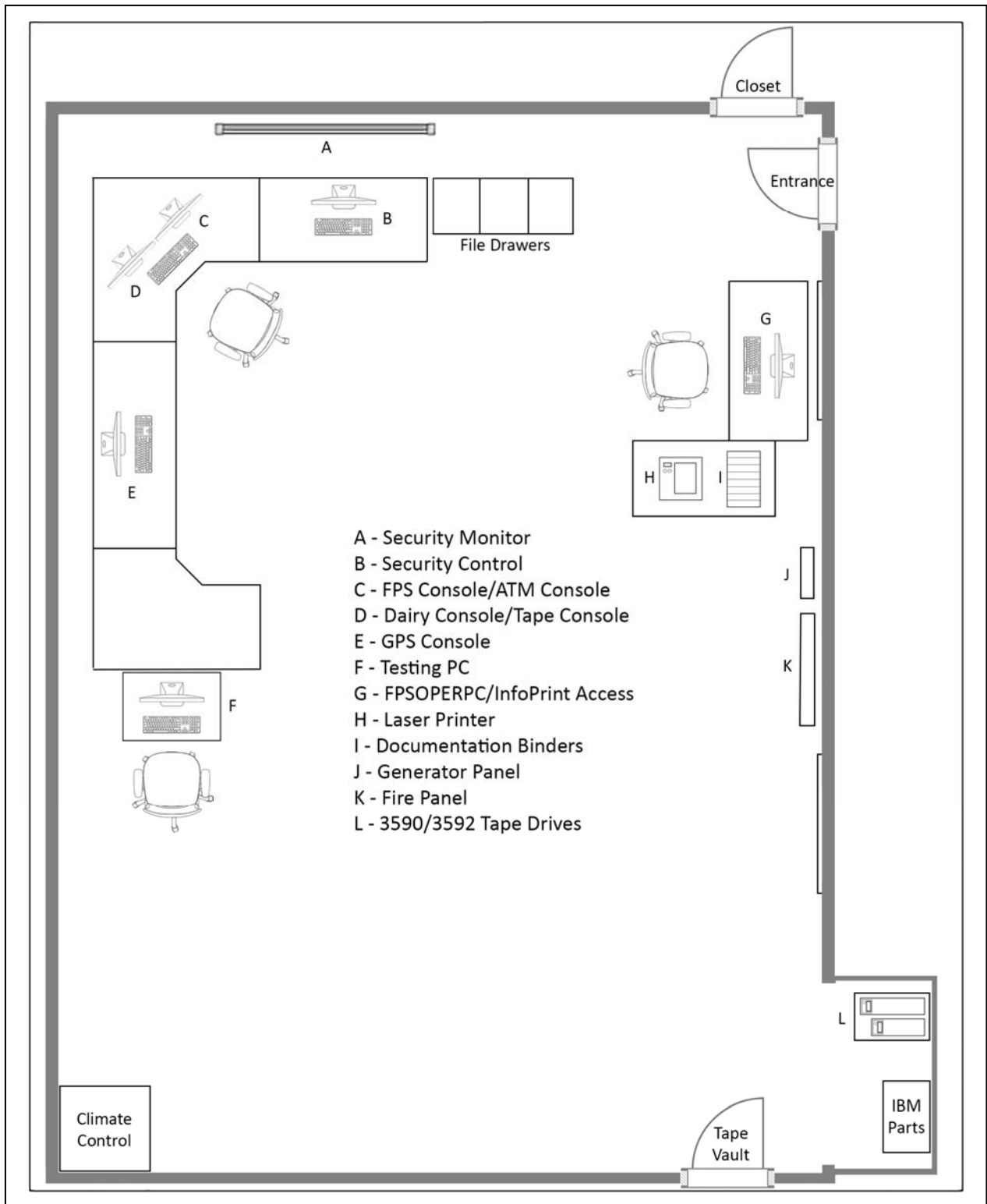
Quantity	Manufacturer	Item/Make-Model	Description
26	VMWare	VSphere Ent. Plus with operations manager	Per socket license 6 or newer
2	VMWare	VCenter 6.0 or newer	VCenter License
2	Microsoft	Window 2012 Standard Veeam backup	TivoliServ
26	Microsoft	Windows 2012 Data Center Licenses for	Per socket license VM guests
1	IBM	Tivoli Storage Manager Backup software	Extended edition V7.1
2	Microsoft	Windows 2012 R2	Provo and Tonaquint vCenter
2	Rubrik	R348 96 TB Backup Appliance	Provo and Tonaquint
1	Rubrik	R3410 120 TB Backup Appliance	Provo

Software/Application Name	Version(s)	Function/Purpose	Notes
Windows Server	2016 R2, 2012 R2	Operating System	26 CPU licenses
Windows Desktop	7, 8.1, 10	Operating System	300 licenses
vCenter		Virtualization Environment Manager	2 licenses
vSphere (ESXi)	6.0	Virtualization Hypervisor Enterprise Plus	26 licenses
vSphere (ESXi)	6.0	Virtualization Hypervisor Standard	8 licenses
vSphere client	6.0	Virtualization Management client	
Cisco UCS	2.2(3)N2(2.26e)	Chassis Management	
Cisco ASA	9.6(4)8	Network firewall/routing	
Cisco Router	15.4(3)M4	Network Routing	
Cisco Switch	152-4.E5	Network Switching	
Cisco 9K Switch	7.0.3.I5.2	Network Switching	
MS SQL Server	2014	DBMS	48 core licenses
MS IIS	8.5	Web Server	
Rubrik	8.1	Tape Backup System	
Viper Server (Management Console)	7.0.3.12	Workstation Antivirus	
Viper Client	Version 7.5.5839	Workstation Antivirus	
Cylance	10.2.434	Server Antivirus	
FortiSIEM Server	4.4.5(1003)	Logging and event correlation server	
FortiSIEM Agent	1.0.0	Logging agent	
SAINT	8.11.2	Vulnerability Scanning	
FireSIGHT	5.4.1.6	Network-based IDS	
Solar Winds	2.1.1.2005	Patch Management	
F5 BIG IP	12.1	Application Firewall	
Brocade Switch	7.0.1a	SAN Switch	
Hitachi VSP	70-06-32-00/00	SAN Chassis	

**This page intentionally left blank.**

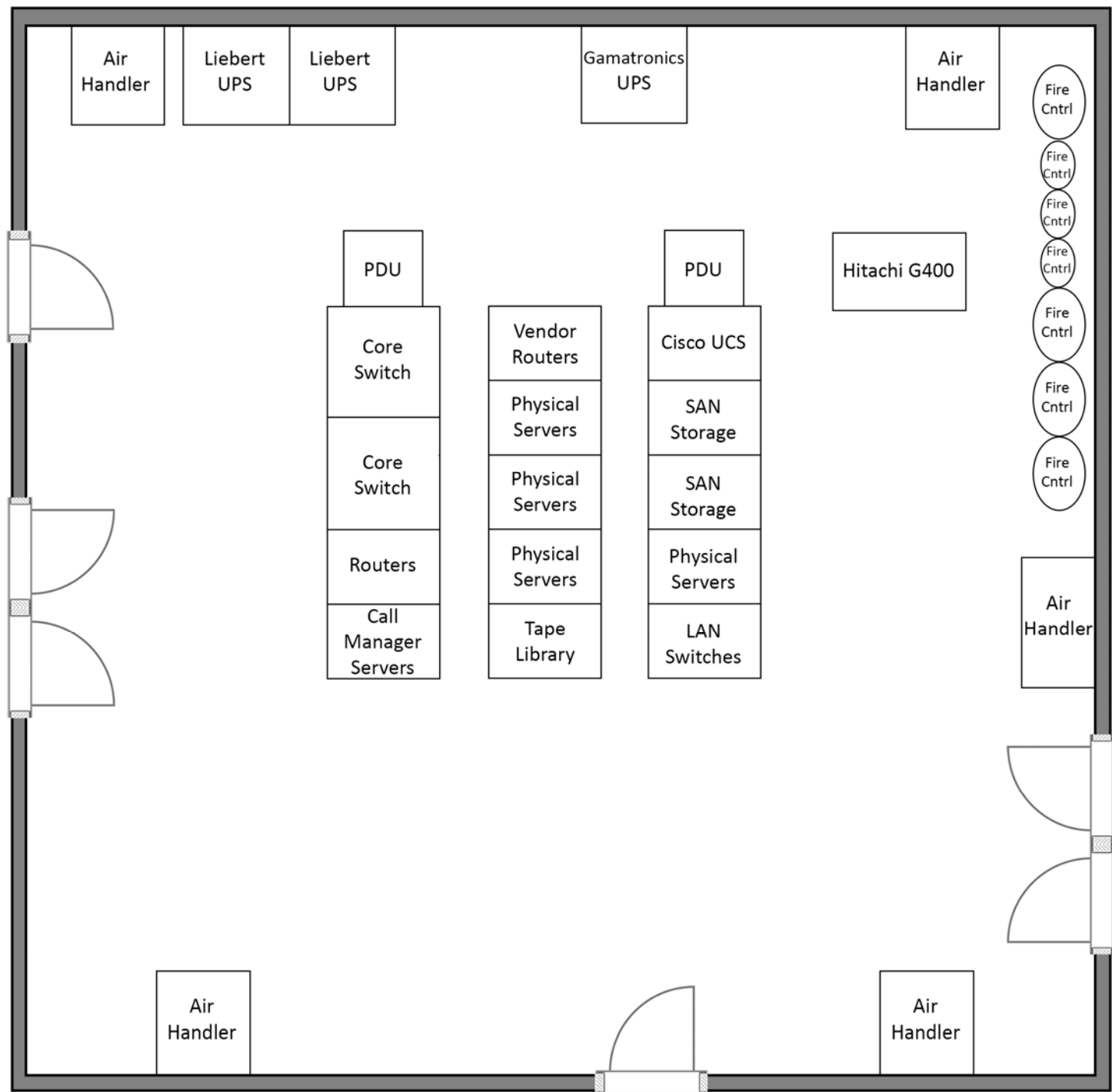
## APPENDIX I FLOOR AND EQUIPMENT LAYOUTS

### Operations Center Layout 05/2018





Appendix I – Floor and Equipment Layouts



## APPENDIX J      DISTRIBUTION LIST FOR THE CONTINGENCY PLAN

<u>Copy</u>	<u>Assigned to</u>
9000	Yancy Barnett
9001-2	Dirk Baum
9003-4	Doug Carpenter
9005	Melissa Carpenter
9006	Bob Chesworth
9007	Jeff Collinsworth
9008-9	Computer Room
9010-11	B. Lynn Crandall
9012	Ken Crandall
9013-14	Lee Day
9015	Burke Day
9016	Jesse Dean
9017	Matt De Visser
9018	Financial Applications
9019	FPS GOLD Deposit Customer Service
9020	FPS GOLD Education Department
9021	FPS GOLD Loan Customer Service
9022	GOLDPoint Systems Customer Service
9023	GOLDPoint Systems GOLDTrak PC
9024	David Harris
9025-26	Scott Howell
9027-28	Ken Jorgensen
9029	NCC
9030	Tonaquint (Disaster Recovery Box 1)
9031	Tonaquint (Disaster Recovery Box 2)
9032-33	Gil Porter
9034	Steven Smith
XXXX	Any client requesting a copy (by institution number)
9200	Cadence Assurance

**This page intentionally left blank.**

**APPENDIX K CERTIFICATION OF ANNUAL REVIEW****Certification of Annual Review**

I, \_\_\_\_\_ hereby certify  
(Name/Title)

that the Disaster Contingency Plan for \_\_\_\_\_  
(Institution Name)

\_\_\_\_\_ has been reviewed and updated, and that:

- This review included updates of employee lists, vendor information, and equipment changes. \_\_\_\_\_  
(Date Completed)
- Essential policy and procedural changes have been implemented and documented. \_\_\_\_\_  
(Date Completed)
- The senior management or Board of Directors of our institution has reviewed all changes. \_\_\_\_\_  
(Date Completed)
- The employees of our institution have reviewed the plan and know their duties in the event of a disaster. \_\_\_\_\_  
(Date Completed)
- Our Disaster Contingency Plan has been tested during the current calendar year. \_\_\_\_\_  
(Date Completed)

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
(Signature of Certifying Officer)

**This page intentionally left blank.**

## Exhibit 6



### **Servicing and Collection Policy**

Revision Date 02/28/2020

**CONFIDENTIAL – DO NOT DISTRIBUTE**

National Energy Improvement Fund, LLC (NEIF) will comply with all applicable Federal, State and Local regulations, including, but not limited to, the Consumer Credit Protection Act, the Equal Credit Opportunity Act, and all other laws and regulations regarding prohibited discrimination, fair lending, and loan disclosure.

No director, officer or employee of NEIF (in their capacity as originators of financing products, each an "Originator") will discriminate on a prohibited basis against any person who requests or receives credit, or against any person who is in any way involved in a credit transaction. No director, volunteer, officer or employee of Originator shall offer, grant or request preferential treatment or pricing for any applicant that is inconsistent with any credit and collections policies approved by NEIF.

**SECTION I: SERVICING PROGRAM REQUIREMENTS**

The loan collection and recovery functions are essential elements of the servicing operation. These functions have a key role in preserving the quality of the loan portfolio and in avoiding unnecessary loss of revenue. The collection policy of NEIF (in such capacity, "Servicer") is designed to ensure Servicer's collections program satisfies the following objectives:

- Collections are made in an expeditious and cost-effective manner in compliance with all State, Local and Federal laws and regulations
- Delinquencies and loan losses are managed within acceptable parameters as determined by NEIF
- Loss recoveries are maximized

**Payment Instructions**

Servicer shall instruct borrowers to make payments; (i) electronically (via direct debit); or (ii) by mail to a lockbox designated by NEIF. If payments are not made directly to the designated lockbox, Servicer agrees to immediately deposit the related receipts into the lockbox. Servicer will, not less often than every three months, instruct those borrowers whose payments were not directed to the designated lockbox to make payments as described above. If at any time, a borrower's direct debit is rejected more than once, Servicer may notify such borrower that it cannot make payment by direct debit and may be required to make payment to the lockbox by another method offered by Servicer.

**Overpayments**

In the event that a borrower overpays a monthly payment, the payment will be applied to principal unless instructed otherwise in writing by the borrower. No penalties will be assessed on partial or full prepayments.

**Service Members Civil Relief Act**

The Service Members Civil Relief Act was enacted to provide financial relief and legal protection for military personnel who have been called for active duty. Originator must apply a 6% interest rate limitation on all loans established by the borrower prior to active duty. The 6% rate limitation does not apply to debts incurred during or after active duty. Borrowers are required to submit copies of their orders to document that they are on active federal military duty. The interest rate reduction/limitation will be retroactive to the date the borrower entered active military duty. Any overpayment of interest during the active duty period must be credited back to the loan. The payment amount must be reduced based on the 6% rate for all installment loans. If Originator believes that the borrower's active duty status does not represent a material hardship to the borrower, Originator may petition the court for relief from the requirements of the Act.

**NSF Checks and Returned Items**

For each payment by a borrower, Servicer's bank shall submit all returned checks or drafts no more than twice, according to each individual bank's internal policy, to give the borrower an additional opportunity to make the funds available for the check or draft. However, Servicer will only assess one NSF or returned item fee in connection with each payment.

**Standard Servicing of all Loans**

A welcome email is sent to borrowers within 24 hours of the loan proceeds being disbursed to the contractor on behalf of the borrower. This email explains how to set up an online account and how to contact the NEIF Loan Servicing team with any questions.

All loans will have a statement generated 20 days before the monthly due date of the loan. The borrower has the option to receive a paper statement sent through USPS mail service, to receive an electronic statement through a link to their online account, or to receive both.

All borrowers receive an email 3 days prior to the monthly due date reminding them to make a payment by the due date. Borrowers have the option to make one-time payments or set up recurring payments.

**Management of Delinquent and Defaulted Loans**

Delinquent loans are those loans where more than 10% of a scheduled payment is not received by the end of the day on its due date. A loan that remains delinquent for more than 30 days becomes a defaulted loan. Servicer will engage in the following activities or will authorize third party vendors to engage in the following activities on its behalf to cure delinquent loans and maximize recoveries on defaulted loans.

- **3-Day Collection Letter:** Sent to any borrower(s) who is currently three days past due on his/her payment.
- **7-Day Collection Call:** A call to borrower(s) who is one week overdue on his/her payment.
- **15-Day Collection Letter:** Second written notice to the customer, sent to any borrower(s) who is 15 days overdue on his/her payment.
- **21-Day Collection Call:** A call to borrower(s) who is 21 days overdue on his/her payment.
- **28-Day Collection Call:** A call made to borrower(s) at home, work, or cell in order to speak with them before a default notice is sent out. Informs borrower that his/her loan is about to go into the default period.
- **30-day Default Notice:** Notice is sent once the loan payment is 30 days overdue. One letter is sent regular first-class mail and another is sent certified mail.
- **60-day Payment Letter:** If the borrower(s) makes no action after the default notice is sent, a payment letter is sent. The letter informs the borrower(s) of the amount due and that the default period is about to expire.
- **90 to 120 day Final Collection Call:** Before engaging a collection agency or pursuing any legal means of collection, a final collection call is made to the borrower(s).



- **90 to 120 days:** If a loan is not cured during the default period, Servicer may use a collection agency or pursue any legal means of collection.

## **SECTION II: Additional Collection Policies**

### **Restoration of Accounts**

A loan in nonaccrual status (starts at 90 days) may be restored to accrual status when all past due payments have been made and it is reasonable to expect the customer to continue to make their monthly payments.

### **Deferrals**

Delinquent account remediation shall be limited to deferrals. Deferrals may be granted provided that (i) at least 12 scheduled payments have been made in full before the first deferral is granted; (ii) no more than one deferral can be made in any calendar year; (iii) no more than three deferrals can be made over the life of any loan; and (iv) the maximum deferral period is no more than three months. Deferrals must be interest bearing.

### **Loan Modifications**

A loan modification may be negotiated and agreed upon when a (non charged-off) borrower is unable to pay the total amount due immediately. NEIF is under no contractual obligation to accept or offer payment arrangements to delinquent borrowers. All borrower loan modifications shall follow their unique Investor guidelines and be reviewed on a case by case basis. Borrowers who have previously broken promises to pay or who have a chronic delinquent payment history will not be automatically offered an extended payment arrangement. All loan modifications must be approved in advance by the Loan Servicing Manager, the Vice President of Accounting and Servicing or an officer of NEIF.

### **Charge Offs**

Loans are to be charged off in accordance with the following:

- Delinquent for 120 days (unless definite collection action is pending and NEIF has approved a delay) unless otherwise specified by the Investor
- If NEIF has accepted a settlement, the forgiven unpaid balance shall be charged off at the end of corresponding month of settlement
- Chapter 7 Bankruptcy filing or discharge, whichever occurs first.
- Loan balances that are included in a Chapter 13 bankruptcy are to be charged off when the payments become six months delinquent

### **Telephone Collections**

Telephone contact with delinquent borrowers is the most efficient and effective way of resolving default situations. Servicer's collection program will utilize all available resources to contact delinquent borrowers through phone calls to their homes and/or cell phones, places of employment, personal references or other message numbers, within the guidelines of all regulations and reasonable business practices.

### **Bankruptcies**

Servicer will protect its interest in all accounts where a bankruptcy has been filed by filing a proof of claim. Repayment plans under Chapters 11, 12 or 13 will be carefully scrutinized before acceptance. In accordance with the Bankruptcy Code neither Servicer nor any third-party subcontractors will make any collection contacts with a borrower. Servicer will protest any bankruptcy filing in which the borrower has knowingly and purposely attempted to defraud Servicer.

**Legal Remedies**

Servicer may utilize all legal remedies available to obtain payment of any amounts owed. These remedies include seeking legal judgment against the borrower for the purpose of executing the judgment against wages, cash assets, and consumer goods such as automobiles, real property or personal items. The use of legal action can be administered against individuals, community property estates, decedent estates or guarantors of the loan agreement. Resorting to legal action must provide a proven positive return to Servicer and cannot expose Servicer to additional risk or liability.

**Small Claims Court Action**

In cases of small balance accounts or debts, Servicer, at its discretion, may pursue legal action without the benefit of counsel. All of these actions must fall under the jurisdiction of small claims or justice court and each district's maximum dollar limits.

**Use of Collection Agencies**

From time to time it may become necessary to utilize the service of a collection agency when all internal avenues of collection have been exhausted or, because of balance owed, it is not practical to collect the account using additional Servicer resources. Agencies will be selected based on their contingency pricing, licensing, bonding and insurance coverage, reporting system and method of conveying funds to Servicer.

Any agreement with a collection agency will be made in accordance with Servicer's policy and executed by the proper authority level. Determination of which accounts should be assigned to collection agencies will be based on an analysis conducted by the COO and Vice President of Accounting and Servicing.

**Demand for Payment or Balance in Full**

Servicer may demand payment of all past due and currently due payments or the balance of the account in full if there has been no agreement to pay that amount or any contact with the borrower by the 60th day of delinquency. In situations of chronic delinquency, first payment defaults, previous broken promises to pay or previous payment extensions, demand must be made by the 30th day of delinquency and can be done, at collector discretion, at the earliest next delinquency occurrence.

**Consumer Credit Counseling**

Servicer is encouraged to cooperate fully with and encourage the use by borrowers of non-profit consumer credit counseling agencies where the interests of Servicer are protected. With the approval of NEIF, late charges or other fees may be waived.

**Credit Bureau Reporting**

In accordance with federal consumer law, Servicer may report only accurate and truthful information about borrowers to consumer credit reporting agencies. All credit related

loan or account status changes must be promptly reported. The scope of this reporting includes all charge offs, the inclusion of an account in a bankruptcy filing and any compromise settlement.

Any upgrade of previously reported information will promptly be changed to reflect the borrower's current situation. All disputes or inquiries referencing the above reporting or any reporting of delinquent status will be researched, responded to and resolved by Servicer within 30 days of receipt by Servicer.

**Parties to the Loan and Disclosure**

In accordance with Privacy Laws Servicer will only discuss the status and condition of loans and accounts with direct parties to the loan. Those parties include all signers of the contract, guarantors of the contract, and any parties retaining contingent liability through the assumption of the obligation. The account may be discussed with the borrower's attorney, personal representative or other party with documented permission from the borrower or other documentation establishing the attorney or representative relationship is in file.

Servicer can and will disclose pertinent loan and account information to anyone contracted to perform service for Servicer such as third-party collection service providers, outside counsel or collection agencies.

## Exhibit 7

### Required Insurances and Fidelity Coverage

NEIF shall maintain during the life of the Agreement, and pursuant to the requirements in Section 2.02 (h), the following insurances and bonds:

**GENERAL LIABILITY.** NEIF shall maintain a commercial general liability insurance policy in an amount of no less than **two million dollars (\$2,000,000) with a four million dollar (\$4,000,000)** aggregate limit. "Marin Clean Energy" shall be listed as a named insured as co-defendants on the commercial general liability policy and the certificate of insurance shall include an additional endorsement page (see sample form: ISO - CG 20 10 11 85).

**AUTO LIABILITY.** Where the Services to be provided under this Agreement involve or require the use of any type of vehicle by NEIF in order to perform said Services, NEIF shall also provide comprehensive business or commercial automobile liability coverage including non-owned and hired automobile liability in the amount of one million dollars combined single limit (\$1,000,000).

**WORKERS' COMPENSATION.** NEIF acknowledges that the State of California requires every employer to be insured against liability for workers' compensation or to undertake self-insurance in accordance with the provisions of the Labor Code. If NEIF has employees, it shall comply with this requirement and a copy of the certificate evidencing such insurance or a copy of the Certificate of Consent to Self-Insure shall be provided to MCE prior to commencement of Services.

**PROFESSIONAL LIABILITY INSURANCE.** NEIF shall maintain professional liability insurance with a policy limit of not less than \$1,000,000 per incident. If the deductible or self-insured retention amount exceeds \$100,000, MCE may ask for evidence that NEIF has segregated amounts in a special insurance reserve fund, or that NEIF's general insurance reserves are adequate to provide the necessary coverage and MCE may conclusively rely thereon. Coverages required by this subsection may be provided on a claims-made basis with a "Retroactive Date" prior to the Effective Date. If the policy is on a claims-made basis, coverage must extend to a minimum of twelve (12) months beyond termination of this Agreement. If coverage is cancelled or non-renewed, and not replaced with another claims made policy form with a "retroactive date" prior to the Effective Date, NEIF must purchase "extended reporting" coverage for a minimum of twelve (12) months after termination of this Agreement.

**PRIVACY AND CYBERSECURITY LIABILITY.** NEIF shall maintain privacy and cybersecurity liability (including costs arising from data destruction, hacking or intentional breaches, crisis management activity related to data breaches, and legal claims for security breach, privacy violations, and notification costs) of at least \$1,000,000 US per occurrence.

**FIDELITY COVERAGE.** NEIF shall maintain a Fidelity policy in the amount of one million dollars (\$1,000,000).

### **Exhibit 8- Program Setup Services**

NEIF will provide BUYER with advisory services related to the design and set-up of the various financing mechanisms that BUYER will use to support financing elements of BUYER's residential and commercial energy storage programs. Such services shall include but not be limited to:

- Advise on appropriate loan underwriting criteria
- Advise on appropriate structure for BUYER participation in loan program offerings
- Provide background on expected defaults and charge offs  
Advise on appropriate loan administration including BUYER staff roles and responsibilities related to loan origination and loan servicing
- Provide appropriate and related set-up for any commercial financing for energy storage, although it is understood that BUYER will provide none of the capital to fund or enhance such commercial energy storage financings

**NEIF Financing for MCE Residential Energy Storage Loan Program****Origination & Servicing Operational Details****LOAN ORIGINATION PROCESS**

- 1) **Underwriting Criteria:** NEIF will use the criteria set forth in the MCE Energy Storage Loan Program Credit Guidelines (Credit Guidelines) when evaluating applications for loan approval (Exhibit 1).
- 2) **Trade Ally/Developer Vetting:** NEIF will conduct its normal vetting process for all Trade Allies, developers and/or subcontractors, as appropriate, who will be participating in the MCE Energy Storage Loan Fund Program and who will have access to the online developer portal. If NEIF discovers during this process that a Trade Ally, developer or subcontractor does not pass this vetting process, it shall notify MCE and TRC of this and provide the reason(s) why they did not pass this process.
- 3) **Training:** NEIF shall conduct training for all trade allies, developers and/or subcontractors who will be participating in the program and marketing to, communicating with or enrolling customers into MCE's Energy Storage Program. The training will be recorded for future viewing by new staff or Trade Allies, developers and/or subcontractors, as well as MCE and TRC staff. The training will cover the details of the program offering, loan application process, use of the developer portal, process for submitting required loan documentation, and loan disbursement process and additional program related information related to the financing program. NEIF shall also provide information on what the Trade Ally/developer should and should not be saying with regard to financing to ensure compliance with all applicable Federal and State laws and regulations.
- 4) **Application Process**
  - a) **Customer Category Determination:** MCE will provide a customer category code on the Energy Storage Program Agreement to indicate the category for which the customer is eligible under the program (e.g., Priority Low-Income, Priority Other, or General Market). This will let NEIF know the appropriate interest rate and term for which the customer is eligible, as described in the Credit Guidelines document.
  - b) **Loan Approval:** NEIF shall follow the online loan application process outlined in the Service Agreement for all residential loans. Once NEIF reviews and approves the customer for a loan using the underwriting criteria outlined in the Credit Guidelines, the customer shall be notified that the loan approval is valid for a period of 120 days from the date of approval. With written approval from MCE, NEIF may extend this period so long as NEIF is reasonably satisfied that there have been no material changes in the customer's financial situation that would otherwise make them ineligible for the loan. If NEIF is not reasonably certain that this is the case, they shall request that the customer reapply for the loan.

## 5) Loan Disbursements

A Customer Journey process flow diagram has been attached to this document to illustrate the timing and triggers for loan disbursements to approved residential customers in MCE's Energy Storage Program.

- a) First Payment: Once a loan has been approved by NEIF, fifty (50) percent of the funds will be paid directly to the developer or installer, as appropriate, when the developer uploads a copy of a valid and approved permit from the local Authority Having Jurisdiction (AHJ) via NEIF's online contractor portal established for MCE's Energy Storage Loan Program. The loan applicant or an authorized representative may also submit a copy of the valid and approved permit issued by the AHJ via email to NEIF, at which point NEIF will release fifty (50) percent of the funds directly to the developer within 10 days of receipt of the copy of the document.

NEIF will not charge any interest to the customer for this first payment, nor will NEIF send any bills or demands for payment to the customer at this time. NEIF will charge to MCE an enrollment fee of \$50 per approved and funded customers, to be collected as described below. NEIF will not charge the customer any fees for originating or servicing of the loan for any customer in good standing in the program.

- b) Final Payment: Once the building inspector from the AHJ has inspected and approved the installation of the Battery Energy Storage System (BESS) and issued a signed inspection report, and the developer has uploaded a valid and complete copy of the report via NEIF's developer portal designed for this program, NEIF shall disburse the second and final payment directly to the developer within 10 days of receipt of the document. Alternatively, the customer or authorized representative may submit a copy of the valid and complete inspector's report approving the project via email to NEIF.
- c) Responsibilities: It is the responsibility of the developer, installer or Trade Ally managing the installation of the BESS to submit all required documents in a timely manner to NEIF via the online portal created for this program in order for the funds to be disbursed. The customer or authorized representative may also submit the required documents via email directly to NEIF as well. However, NEIF shall not disburse any loan funds until valid and complete copies of the required documents have been submitted and reviewed by NEIF.

## 6) Loan Funds Bank Account

- a) Account Establishment: NEIF will establish a Loan Proceeds account, pursuant to the terms of the Loan Origination and Servicing Agreement Executed on May 6, 2021, for the benefit of MCE at a bank specified by NEIF, Firsttrust Bank. MCE will deposit funds into the Loan Proceeds account directly to the contractor on behalf of the customer per the disbursement schedule in section 5 above. NEIF will have access to this account and be authorized to disburse loan funds

as described above. MCE shall make an initial deposit in the amount of \$400,000 to this account for this purpose.

- b) Loan Fund Replenishment: When the amount in the Loan Fund falls below a level that NEIF deems to be too low to continue disbursing funds without significant disruption or delays, and based on the anticipated customer application pipeline, NEIF shall send to MCE an email with an invoice to replenish the funds back to the \$400,000 level. MCE shall transfer funds for the invoiced amount, not to exceed \$400,000, within 2 business days via electronic funds transfer/ACH. At no time shall the amount in the Loan Fund fall below \$50,000 without the written consent or instruction from MCE.

## 7) Loan Servicing Bank Account

- a) Account Establishment: Pursuant to the terms of the Loan Origination and Servicing Agreement Executed on May 6, 2021, NEIF shall open and maintain a bank account in its selected bank on MCE's behalf to deposit customer loan principal and interest payments from customers enrolled in MCE's Energy Storage Program and the Loan Fund Program.
- b) Payments to MCE: On the 15<sup>th</sup> of the month following receipt of loan payments, NEIF shall transfer to MCE all loan payments received from customers during the prior calendar month, less the agreed upon amount of the loan origination and servicing fee (set at 2.5% per annum) and less any customer enrollment fees for loans approved during the prior month (\$50/approved loan), via electronic funds transfer/ACH.

## 8) Reporting/Auditing

- a) Loan Origination Reports: NEIF shall send to MCE weekly loan origination reports, which shall include anonymized data on the number of loans approved and dollar amounts of the loans by customer category and FICO scores to help MCE manage portfolio risks, along with any other relevant data on loan originations. NEIF shall assist MCE in evaluating its current and projected portfolio risk and provide recommendations for mitigating risks, such as lowering loan default rates by adjusting minimum credit scores, adjusting interest rates, and/or targeting specific customer categories to cover loan defaults and offset below-cost interest rates charged to Priority customers. At its discretion, MCE may request that reports be submitted monthly instead of weekly.
- b) Loan Servicing Reports: NEIF shall send to MCE monthly loan servicing reports by the 15<sup>th</sup> of the month following loan servicing activity. In addition to monthly loan repayment information, these reports shall include, among other things, information on loan defaults, missed payments, late payments and any other information to help MCE evaluate and manage its loan portfolio risks.



- c) Audits: NEIF shall have an independent annual audit conducted by a professional, reputable, independent auditor and share the results of the audit with MCE. MCE, at its sole discretion, may conduct an independent audit by an auditor of its choosing.
  - d) Regulatory Reporting and Compliance: NEIF shall be solely responsible for preparing and submitting any required reports regarding MCE's Energy Storage Loan Program to the appropriate regulatory oversight agency as required by Federal or State Law, Rule or Regulation. NEIF will, for the duration of its participation in this program, and for as long as it continues to receive loan repayments from program participants, maintain compliance with any and all applicable Federal, State or local law, rule or regulation, including, but not limited to the Truth In Lending Act, California Consumer Financial Protection Law, and California Financing Law.
- 9) MCE Customer Engagement Protocol: NEIF shall comply at all times during the Agreement with any MCE-provided MCE co-branding and/or customer engagement protocol that provides MCE's expectations for customer interactions by NEIF. This includes the following:
- a) Treat prospective and enrolled Participants/Customers fairly and deliver promised services in a timely, professional and responsible manner.
  - b) Ensure Customers are aware the loan Program is a MCE-sponsored Program.
  - c) Materials that contain MCE's logo will follow MCE's branding standards.
  - d) Respond to Customer inquiries timely from the date of the request.
  - e) Any other customer service protocol mutually agreed upon between the parties.

This FIRST AMENDMENT is made and entered into on May 19, 2021, by and between NATIONAL ENERGY IMPROVEMENT FUND, LLC (hereinafter referred to as “NEIF”) and MARIN CLEAN ENERGY, (hereinafter referred to as “BUYER”).

WHEREAS, BUYER and NEIF entered into an agreement on May 6, 2021, for NEIF to originate and service Energy Storage Loans on behalf of BUYER (“Agreement”); and

WHEREAS, Exhibit 7 to the Agreement specified the required insurance coverages for NEIF to maintain throughout the life of the Agreement; and

WHEREAS the parties desire to amend the Agreement to modify the Fidelity Coverage listed in Exhibit 7.

NOW, THEREFORE, the parties agree to modify Exhibit 7 as set forth below.

1. The Fidelity Coverage requirement of Exhibit 7 shall be amended as follows:

**FIDELITY COVERAGE.** NEIF shall maintain a Fidelity policy in the amount of five hundred thousand dollars (\$500,000).

2. Except as otherwise provided herein all terms and conditions of the Agreement shall remain in full force and effect.

IN WITNESS WHEREOF, the parties hereto have executed this FIRST Amendment on the day first written above.

MARIN CLEAN ENERGY

DocuSigned by:  
Dawn Weisz  
By: A59878416ERC4E8

Date: 5/17/2021