

Network Disaster Recovery Plan

Social Legends, LLC

Emergency notification contacts

Name	Home Phone	Mobile/Cell Phone
Kelly Frank	812.876.1282	317.435.2529
Matt Belsaas	317.912.3773	317.912.3773
Annie Cornett	812.361.5229	812.361.5229

Emergency response activities

	Action	Who Performs
1.	Identify and assess network outage	Matt Belsaas
2.	Review with IT management	Kelly Frank
3.	Evacuate area if necessary	All Staff
4.	Initiate remedial actions to recover network assets	Matt Belsaas
5.	Decision to invoke network DR plan	Kelly Frank
6.	Initiate DR plan activities	Matt Belsaas
7.	Contact appropriate vendors and carriers	Matt Belsaas
8.	Follow through on recovery procedures	Matt Belsaas, Annie Cornett

Revisions control page

Date	Summary of changes made	Changes made by (Name)

Purpose

The purpose of this network disaster recovery (NDR) plan is to prepare Social Legends, LLC in the event of disruptions affecting corporate local area networks (LAN), wide area networks (WAN), Internet access and wireless network services due to factors beyond our control (e.g., natural disasters or man-made events). This plan will also guide restoration of network integrity and normal operations to the widest extent possible in a minimum time frame. All Social Legends, LLC locations that are connected to the WAN are expected to implement preventive measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs.

This plan identifies vulnerabilities and recommends necessary measures to prevent extended network outages. It is a plan that encompasses all Social Legends, LLC network operations in all locations.

Scope

This is a disaster recovery (DR) plan, not a daily problem resolution procedures document.

Plan Objectives

- Serves as a guide for Social Legends, LLC's IT voice, data, Internet and wireless network recovery teams
- References and points to the location of network operational data outside this document
- Provides procedures and resources needed to assist in network recovery
- Identifies vendors and customers that must be notified in the event of a network outage
- Assists in avoiding confusion experienced during a network disruption by documenting, testing and reviewing recovery procedures
- Identifies alternate sources for network equipment, network services, power supplies and other resources
- Documents storage, safeguarding and retrieval procedures for vital network records and other relevant data

Assumptions

- Key people will be available following a disaster
- This plan and critical network documents are stored in a secure off-site location and not only survived the disaster but are accessible immediately following a disaster
- Other IT departments and support organizations will have their own DR plans

Disaster definition

Any loss of carrier services (such as local access, wide-area network channels or Internet access), voice/data connectivity (such as routers, switches, PBXs or VoIP systems), or natural or man-made disaster that causes an interruption in network connectivity relating to voice, data, Internet and wireless technologies provided by Social Legends, LLC's IT operations. This plan identifies vulnerabilities and recommends measures to prevent extended network outages.

Recovery teams

- Emergency Management Team (EMT)
- Disaster Recovery Team (DRT)
- IT Technical Support (IT) for Networking

See Appendix A for details on the roles and responsibilities of each team.

Team member responsibilities

- Each team member will designate an alternate/backup.
- All team members should keep an updated calling list of team members' work, home and cell phone numbers both at home and at work.
- All team members should keep this plan for reference at home in case a network disaster happens after normal work hours. All team members should familiarize themselves with the contents of this plan.

Instructions for using the plan

Invoking the plan

If an initial assessment of the network disruption indicates a potentially prolonged outage (e.g., longer than eight hours), this plan becomes effective when approved by senior IT management. The plan will remain in effect until network operations are resumed at all affected locations.

Disaster declaration

The President (Kelly Frank), with input from the Emergency Management Team, Disaster Recovery Team and IT Technical Support, is responsible for declaring a disaster and activating network recovery teams as outlined in this plan.

In a major disaster situation affecting multiple company locations, the decision to declare a disaster will be determined by Social Legends, LLC's president. The Emergency Management Team and Disaster Recovery Team will respond based on the directives specified.

Notification

Regardless of the network disruption circumstances, or the identity of the person(s) first made aware of the disaster, the Emergency Management Team (EMT) and Disaster Recovery Team (DRT) must be activated immediately in the following cases:

- Two or more systems and/or sites are down concurrently for three (3) or more hours.
- Five or more systems and/or sites are down concurrently for three (3) or more hours.
- Any problem involving a voice/data/Internet/wireless network facility that would cause either of the above conditions to be present or there is certain indication that either of the conditions is about to occur.

Emergency management standards

Backup policy

Full and incremental backups protect and preserve corporate network information and should be performed on a regular basis for system logs and technical documents that are not easily replaced, have a high replacement cost or are considered critical. Backup media should be stored in a secure and geographically separate location from the original and isolated from environmental hazards. Backup network components, cabling and connectors, power supplies, spare parts and relevant documentation should be stored in a secure area on-site.

Network-specific data and document retention policies specify what records must be retained and for how long. All network organizations are accountable for carrying out instructions for records management in their organization.

IT Technical Support follows these standards for data backup and archiving, particularly for networks:

System databases

- A copy of the most current network and system databases must be made at least twice per month or based on frequency of changes made.
- These backups must be stored offsite.
- The lead network administrator is responsible for this activity.

Offsite storage procedures

- Tapes, disks and other suitable media are stored in environmentally secure facilities.
- Tape or disk rotation occurs on a regular schedule coordinated with the storage vendor.
- Access to backup databases and other data is tested annually.

Emergency management procedures

The following procedures are to be followed by network administration and operations personnel and other designated Social Legends, LLC employees in the event of a network disruption or related outage. Where uncertainty exists, the more reactive action should be followed to provide maximum protection and personnel safety.

These procedures are furnished to Social Legends, LLC's personnel to take home for reference. Several pages have been included to supply emergency contacts.

In the event of any situation where access to a building housing network infrastructure equipment is denied, personnel should report to alternate locations or contact security for access if the location is not damaged or quarantined.

In the event of a network services provider outage

In the event of a network service provider outage, the guidelines and procedures in this section are to be followed.

Procedure	STEP	ACTION
	1	Notify senior management of outage. Determine cause of outage and timeframe for its recovery.
	2	If outage will be greater than one hour, route all calls via alternate services. If it is a major outage and all carriers are down and downtime will be greater than 12 hours, deploy satellite phones, if available.

Plan review and maintenance

This network disaster recovery plan must be reviewed semi-annually and exercised on at least an annual basis. The test may be in the form of a walk-through, mock disaster, or component testing. Additionally, considering the dynamic environment within Social Legends, LLC, it is important to review the listing of personnel and phone numbers contained within the network DR plan regularly.

The hard-copy version of the network DR plan will be stored in a common location where it can be viewed by site personnel and the EMT and DRT. Electronic versions will be available via Social Legends, LLC network resources as provided by IT Technical Support. Each recovery

team will have its own directory with change management limited to the recovery plan coordinator.

Notification of incident affecting the site

On-duty personnel responsibilities

If in-hours:

Upon observation or notification of a potentially serious network disruption at a company location, ensure that personnel on site have enacted standard emergency and evacuation procedures if appropriate and notify the EMT and DRT.

If out of hours:

IT Technical Support personnel should contact the EMT and DRT.

Provide status to EMT and DRT

1. Contact EMT and/or DRT and provide the following information when any of the following conditions exist:

- Network performance has sufficiently degraded to where normal operations are not possible for three or more hours.
- Any problem at any network infrastructure asset, system or location that would cause the above condition to be present or there is certain indication that the above condition is about to occur.

The EMT will provide the following information:

- Location of incident.
- Type of incident (e.g., fire, hurricane, flood).
- Summarize the damage (e.g., minimal, heavy, total destruction).
- Meeting location that is a safe distance from the disaster scene.
- An estimated timeframe of when a damage assessment group can enter the facility (if possible).
- The EMT will contact the respective team leader and report that a disaster involving network operations has occurred.
- The EMT and/or DRT will contact the respective Social Legends, LLC team leader and report that a disaster affecting network operations has occurred.

Decide course of action

Based on the information obtained, the EMT and/or DRT decide how to respond to the event: Mobilize IT Technical Support, repair/rebuild existing network operations with network technical and admin staff or relocate to a new facility.

Inform team members of decision

If a disaster is not declared, the location response team will continue to address and manage the situation through its resolution and provide periodic status updates to the EMT/DRT.

If a disaster is declared, the EMT and/or DRT will notify IT Technical Support immediately for deployment of network DR plans.

Declare a disaster if the situation is not likely to be resolved within predefined time frames. The person who is authorized to declare a network disaster must also have at least one (1) backup who is also authorized to declare a disaster in the event the primary person is unavailable.

Contact networking and equipment vendors

Disaster declared: mobilize incident response/technical support teams/report to command center

Once a network desk disaster is declared, the Disaster Recovery Team (DRT) is mobilized. This team will initiate and coordinate the appropriate recovery actions. Network technical and administrative employees should assemble at a designated location as soon as possible. See Appendix E for emergency locations.

Conduct detailed damage assessment (This should be performed prior to declaring a disaster)

1. Under the direction of local authorities, IT Technical Support and/or EMT/DRT, assess the damage to the network and related assets. Include vendors/providers of installed network services and equipment to ensure that their expert opinion regarding the condition of the network is determined ASAP.
 - A. Participate in a briefing on assessment requirements, reviewing:
 - (1) Assessment procedures
 - (2) Gather requirements

(3) Safety and security issues

NOTE: Access to the facility following a fire or potential chemical contamination will likely be denied for 24 hours or longer.

- B. Document assessment results using Assessment and Evaluation Forms contained in Appendix G:

Building access permitting:

- Conduct an on-site inspection of affected areas to assess damage to essential network records (files, manuals, contracts, documentation, etc.) and electronic data.
 - Obtain information regarding damage to the network, e.g., environmental conditions, physical structure integrity, furniture, and fixtures) from the DRT.
2. Develop a Restoration Priority List, identifying facilities, vital records and equipment needed for resumption of network operations that could be restored and retrieved quickly.
3. Recommendations for required resources.

Contact DRT: Decide whether to continue to business recovery phase

The EMT and DRT gather information regarding the event; contacts senior management and provides them with detailed information on status.

Based on the information obtained, senior management decides whether to continue to the business recovery phase of this network DR plan. If the situation does not warrant this action, continue to address the situation at the affected site(s).

Network recovery phase

This section documents the steps necessary to activate network recovery plans to support full restoration of systems and network functionality at either 1) the original company location or 2) an alternate/recovery site that would be used for an extended period of time. Coordinate resources to re-establish network operations at the primary site and reconstruct network operations at a temporary/permanent system location, and to deactivate recovery teams upon return to normal network operations in either scenario.

Social Legends, LLC System and facility operation requirements

The system and facility configurations for each location are important to re-establish normal network operations. **A list for each location will be included in Appendix F.**

Notify IT technical support staff and coordinate return to primary facility/location

See Appendix A for IT Technical Support staff associated with recovery of network operations at the original site.

Secure funding for return to work

Make arrangements in advance with network service carriers and equipment vendors to recover network operations at the primary site.

Notify IT technical support staff/coordinate relocation to new facility/location

See Appendix A for IT Technical Support staff associated with configuring network services at an alternate location (replacement for original site).

Secure funding for relocation

Make arrangements in advance with network service carriers and equipment vendors. Make arrangements in advance with local banks, credit card companies, hotels, office suppliers, food suppliers and others for emergency support.

Notify EMT and corporate business units of network recovery

Using the call list in Appendix B, notify the appropriate company personnel. Inform them of any changes to processes or procedures, contact information, hours of operation, etc. (may be used for media information).

Operations recovered

Assuming all relevant network operations have been recovered either to the original location or to an alternate site with employees in place to support network operations, the company can declare that its network is functioning normally.