2022

Emergency Response & Disaster Recovery Plan

Office of the Chapter 13 Trustee

This document explains what the office of a Chapter 13 Trustee needs to think about and do in order to prepare its own response and recovery plan. Whatever one chooses to call it – disaster planning, emergency preparedness, or business continuity – the goals are ultimately the same: to get an organization back up and running in the event of an interruption.

NACTT
CHAPTER 13 TRUSTEE
July 2022

TABLE OF CONTENTS

Document Edit Guide:

The following Headers have been formatted throughout this document
Heading 1 (Roman Numeral List, Bold, Left Justified)
Heading 2 (Lettered List, Bold, Left Justified)
Heading 3 (Bullets, All Justified)
Heading 4 (Numbers. Bold, Left Justified)
Appendix (Lettered List w/colon, Left Justified)

Each Appendix is referenced through an inserted Cross-Reference link
Table of Contents Displays Heading 1, Heading 2, and Appendix with click-through links
The Table of Contents can be updated using the following procedure:
CTRL-A (Select All)
F9 (Update Entire Table)

DISASTER PREPAREDNESS

I. Purpose & Objectives of Disaster Preparedness:

- To recognize potential disasters or emergencies.
- To analyze the full impact of each disaster as to life, operations, equipment, and data.
- To develop systems or procedures to either avoid a disaster or minimize the impact of a disaster.
- To prepare for the protection of life, assets, and data.
- To prepare for the recovery of data lost in a disaster.
- To quickly return to the normal operation of business.
- To increase employee awareness of potential disasters or emergency situations.
- To increase employee knowledge of appropriate safety precautions in the event of a disaster or an emergency.
- To establish expectations of what is required from staff members in disaster or emergency situations.

II. Description of Facility

The office is located at [*Enter your address and suite number here*].

Enter a paragraph describing the location of the parking facilities and how employees gain access to the office. Include a description of the location of all entrance points into the office area including any special instruction such as the presence of access control systems.

There are [*how many*] fire extinguishers in the office located at:

1. *Location one*
2. *Location two*
3. *Location ….*

Refer to Appendix A: to view the floor plan of the office suite and the location of fire extinguishers, the alarm keypad, panic buttons, and emergency exits.

III. The Plan Administrator and Disaster Team

A) Plan Administrator

The Plan Administrator is the Trustee; however, in his/her absence, the next person in the chain of command set forth below becomes the Plan Administrator with full authority to implement any and all provisions of the disaster plan, including, but not limited to; ordering an evacuation, issuing instructions, or delegating tasks to all employees. However, **THE TRUSTEE IS THE ONLY PERSON EVER AUTHORIZED TO TALK TO THE MEDIA UNDER ANY CIRCUMSTANCES.**

The Plan Administrator is:

1. *Trustee Name, Plan Administrator*
2. Trust Employee Name, *Backup Plan Administrator*

In anticipation of or during an emergency, the Plan Administrator may implement emergency action procedures. After a disaster, the Plan Administrator will implement the disaster recovery plan and will oversee the work of the Disaster Team.

Members of the Disaster Team (Appendix C:)

B) Disaster Team

The responsibilities of the Disaster Team include:

- Making sure everyone is aware of designated emergency meeting places when employed;
- Making sure everyone is out of the office and accounted for in the event an evacuation is necessary;
- Notifying the U.S. Trustee,[1] your banking institution, your case management vendor, the Clerk's office, and Judges' Chambers, and such other entities as are relevant to the Trustee's operations (Appendix I);
- Monitoring imminent weather conditions that might trigger a disaster;
- Preparing the office for emergency situations or disasters;
- Performing a damage assessment after a disaster;
- Notifying insurance companies and subsequently filing claims.

[1] In North Carolina and Alabama, all references to "U.S. Trustee" should be changed to "Bankruptcy Administrator."

- Implementing and executing the disaster recovery plan in an effort to achieve a quick return to normal business operations following a disaster;

- Designating the location for temporary and/or permanent office space;

- Notifying the Post Office of the new temporary and/or permanent address of office;

- Contacting vendors and making arrangements for temporary and/or permanent replacement equipment, furniture, and office supplies;

- Establishing a temporary work schedule for personnel; and

- Updating and maintaining this Manual regularly, recommending to the Trustee any changes in procedures, and providing periodic instructional information to all employees in the office.

IV. Loss Prevention

In order to prepare for emergency situations and to reduce downtime following a disaster, the following disaster preparedness and data loss prevention measures have been placed in effect:

A) Protection of Personnel

- The office is not accessible to the general public; the doors are locked at all times.

- A first aid kit is located (give location or locations).

- Employees are familiar with dialing 9-1-1 to report an emergency and to give the address of the office building.

- All employees have been instructed regarding the location of fire extinguishers, fire alarms, and emergency exit doors during the new employee orientation. Copies of Appendix A and B are located (provide location or locations) for quick reference.

- The Trustee's office and/or building management conducts regular disaster drills. At this time the emergency response procedures will be reviewed to make sure all employees are familiar with evacuation procedures.

- The Trustee recommends that each employee maintain a basic disaster kit in the event a disaster prevents them from going home. Kits should contain comfortable shoes and a three-day supply of prescription and non-prescription medication. Kits should include additional items based on individual needs.

- An “Employee Calling Tree” (Appendix E:) has been established to speed up the process of contacting employees by phone after normal work hours. Each person responsible for making phone calls has an offsite copy of the Employee Phone Directory and Contact Information (Appendix B:) listing at least one phone number at which each employee and emergency contact can be reached.

- The Employee Calling Tree is updated as needed by a designated member of the Disaster Team.

- Where applicable, process payroll off-site using a third party and direct-deposit.

- Contact the Foundation of the National Association of Chapter Thirteen Trustees (“NACTT”) to coordinate the temporary placement of employees at other trustee offices should a major natural disaster (such as a tornado that causes widespread damage) result in employees and their families having to move away from the area temporarily.

B) Natural Disaster Preparedness

- A weather alert radio, along with extra batteries, is kept on site in order to monitor impending storms and to prepare accordingly.

- The Trustee’s office has adequate hazard and liability insurance to provide funding to purchase replacement equipment, including computer equipment, in a timely manner. The amount of coverage necessary is reviewed at least annually. Policies will also respond to expenses associated with “business interruption” (or business continuity), such as rental of temporary office space.

- Where applicable the Trustee has a record of the office’s credit card number, expiration date, verification numbers and password available offsite so that it can be used to make online purchases of equipment.

- Vendors from whom computer equipment has been purchased would be able to provide the configuration of the servers and PCs so that replacement equipment can be ordered quickly.

- Electronic or paper copies of an inventory, disaster notification list, employee calling tree, and employee phone directory, as well as copies of insurance policies, are maintained and stored off-site and are updated at least annually. A copy of this Manual along with the inventory, disaster notification list, and employee phone directory, is kept on a jump-drive and/or disk, which is also stored offsite and is updated at least semi-annually.

C) Data and Financial Loss Prevention

1. Computer Hardware, Equipment, and Computer Network Access, Use, and Limitations

It is important to establish and clearly state limitations on what computer hardware and software may (and may not) be used, limitations on its use, and limitations on access and use of the office's computer network by the Trustee's employees. This is important to both prevention of and recovery from a disaster or emergency (whether cyber-related or otherwise) affecting the Trustee's operations. It is also important to ensure that maintenance and protection of an office's computer network and cyber environment meets all requirements of the office's cyber insurance coverage. Because cyber-security and insuring against cyber-risk are constantly evolving and improving, the office's related operational policies and limitations on computer use and network access should be reviewed, and if appropriate revised, at least annually.

- *Describe policies, requirements, and limitations related to computer hardware, equipmwent, and computer network use and access.*

  Following is an example of a computer policy:

  All computer hardware used in performing the business of the Trustee's office is owned by the Trustee and maintained by the Information Technology Manager ("IT Manager") or by vendors working under the IT Manager's supervision. *Except for use of a mobile telephone, personal computer, or handheld computer device used to enable use of Multi-factor Authentication and receipt of an authentication code necessary to enable connection to the office's Virtual Private Network (VPN), only computer equipment owned by the Trustee may be used to connect to the office computer network, and only equipment owned by the Trustee may be used by employees to perform their work as an employee of the Trustee*. Subject to the specific limited-use exception stated above, examples of equipment that my *not* be used by employees in performing their work or connecting to the office computer network include but are not limited to, any computer mouse, connection cable, keybaord, personal digital assistant, notebook computer, zip drive or thumb drive, or personally owned wireless device.

  Computer hardware owned by the Trustee may not be used for any other purpose than performing work of the Trustee's office, and only information directly related to operation of the Trustee's businees may be saved on any office equipment.

  No software may be installed or saved on any office computer equipment or the office computer network without the explicit permissioin of the IT Manager or the Trustee. No alterations may be

made to office computer equipment or systems in the office, unless explicitly permitted by the IT Manager or the Trustee. Examples of prohibited alterations include, but are not limited to: configuration changes to hardware; changes to cabling or network connections; and changes to software options or controls.

No employee may attach or install any computer equipment, software, connection devices, or services not owned or subscribe to by the Trustee on any Trustee-owned office equipment or the office computer network without the explicit permission of the IT Manager or the Trustee. Examples of the equipment employees may not install include, but are not limited to: docking stations or cradles, connection cables, personal digital assistants (PDA's) personally owned laptop or notebook computers; or personally owned wireless devices that might communicate with the Trustee's office network.

With the exception of personal preference settings which are an integral part of computer operating system software or updates thereof, such as computer screen background, alert sounds, color schemes, screen savers, or monitor view magnification, employees may not make any alterations to office computer equipment or systems, unless explicitly permitted by the IT Manager or the Trustee. Examples of prohibited alterations include, but aren't limited to: additional screen savers, color schemes, screen savers or sounds not included with a computer or part of computer software included with a computer when initially purchased or included in software purchased or installed by the IT Manager of the Trustee, configuration changes to hardware, changes to cabling or network connections, and changes to software options or controls.

Any breach of of these policies is cause for termination of employment.

2. Network Firewall

A network firewall acts as a gatekeeper at your computer's network entry point or port. This firewall acts as a barrier between your computer and another network such as the internet based on pre-established security rules. It helps to protect your network and information by managing your network traffic and allowing only trusted sources or IP addresses access. This includes, blocking unsolicited incoming network traffic, validating access by assessing network traffic, and searching for anything malicious such as hackers and malware.

Operating systems, security software, and individual employee computers usually come with a pre-installed computer firewall; check to make sure those features are turned on. **Security settings should be configured to run updates automatically.**

There are several different types of firewalls based on their structure and functionality, so it is important to research which type, or types of firewalls are suited for your office environment.

- *Describe network firewall protection(s) in use.*

3. Email Security Service

An Email Security Service (software firewall) works like spam filters, by regulating incoming email based on a set of rules established by the email server. An email security service analyzes email messages to determine if the message should be flagged as spam.

Email security services are set up to protect individuals or networks. It will filter incoming and outgoing email-server traffic based on a set of rules determined by the firewall administrator to deny problem senders based on IP address and domain name. Email firewalls do not function exactly the same. The main thing to know is that it monitors the behavior of other users on the server and communicates that information to other firewalls.

- *Describe email security protection(s) in use.*

4. Employee Email Use Policy and Security Awareness

Establish a company email use policy. This policy should make it clear to your employees that all office email is the property of the trust operation. Specifically, any email sent, received, created, or stored on the office computer system may be viewed and, in some cases, admissible in a legal case. As the employer, it is your right to monitor employee's use of email. It is also important to ensure employees are aware of potential monitoring.

A company email policy should address security awareness because emails provide the opportunity for security breaches. Training and enforcing smart email protocols should be included as a part of your email use policy.

Email security awareness training is essential to protecting an organization against common cyberattacks. Training your employees to recognize the signs of an email scheme (phishing), helps reduce the probability that they will click on a malicious link or open an attachment.

Teach employees the importance of reporting suspected phishing emails to your IT or security team. This enables them to investigate and respond in the event another employee fell for the phish.

- *Describe email use policy currently in place.*
- *Describe email security awareness training.*

5. Cyber Liability

Cyber Liability insurance provides the funding necessary to transfer the costs involved with recovery from a cyber-related security breach or similar events. Coverage will respond to a cyber event – such as network security failures, data breaches, malware, ransomware attacks, and business account, and email compromises. Policies will also respond to liability claims and ancillary expenses of an attack or breach. Costs can include lost income due to a data breach, costs associated with notifying customers affected by a breach, costs for recovering compromised data, and costs for repairing damaged computer systems.

- *Assess potential monetary damages resulting from data breaches.*
- *Review cyber liability insurance options and current coverage.*

The amount of coverage and what is covered under a policy should be reviewed at least annually. Coverage should address forensic investigations, litigation expenses, regulatory defense expenses/fines, crisis management expenses, business interruption, cyber extortion, and betterment.

Obtaining cyber liability insurance and recovering on a claim generally requires a business to establish compliance with industry standards for cyber security, including multi-factor authentication.

- *Identify all insurer security policy terms.*
- *Establish network IT security configurations that are compliant with policy terms.*
- *Run regular audits to ensure compliance with cyber liability insurance policy terms.*
- *Address compliance issues as they arise.*
- *Consider retention of external cyber liability risk professional.*

6. Multi-Factor Authentication

Multi-factor authentication (MFA) adds additional layers of security to inhibit cyber criminals' access to computer systems by requiring two or more means of identification and access control for computer systems, cell phones, and applications.

The factors used for identification can be referred to as "something you know, something you have, or something you are."

Simple user IDs, as well as easy to guess and static passwords, are often the weakest links in a business's cybersecurity.

A username and password is “something you know.” Requiring a code sent via text message (SMS) establishes “something you have,” (e.g., a mobile phone or laptop belonging to you).Biometric authentication, through a fingerprint or retina scan, establishes “something you are.” Multi-factor authentication is successfully enabled when at least two of these categories of identification are required in order to successfully verify a user’s identity when accessing systems.

- *Describe the MFA for remote network access through Virtual Private Networks (VPN):*
- *Describe the MFA for administrative access to servers and individual:*
- *Describe the MFA for remote access to email (e.g., cell phone or browser-based access):*
- *Describe the MFA for network access for 3rd party access.*

7. Data Backup and Recovery

Backup and recovery describes the process of creating and storing copies of data that can be used to protect against data loss. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), accidental deletion of data and natural disasters.

Storing a copy of the data on separate medium is critical to protect against primary data loss or corruption. This additional medium can be an external drive, disk storage system, cloud servers (cloud backups), or tape drive. The alternate medium can be in the same location as the primary data or at a remote location. **The possibility of weather-related events may justify having off-site backups in order to prevent data loss.**

Backup copies must be made on a consistent, regular basis to minimize the amount of data lost between backups. Retaining multiple copies of data provides redundancy assurance and flexibility to restore to a point in time not affected by data corruption or malicious attacks. Specifically, cloud backups can provide fully automated and continuous off-site daily data backups to ensure data loss prevention. The data backed up by cloud servers can be restored to new equipment quickly, enabling a Trustee’s office to rapidly gain access to the desired data and applications.

- *Describe the data backup and recovery strategy along with the location and retention period for backup storage.*
- *List the controls in place to ensure data integrity.*
- *List the controls in place to allow the trust operation to continue to operate from the cloud backups.*
- *Offsite virtualization of server backups to continue operations.*

- *List the controls in place to support bank reconciliation and the integrity of financial data.*

8. Other Provisions

A UPS (Uninterrupted Power Supply Device) is used constantly on the server(s) and all computers throughout the office. This reduces potential for damage from power fluctuations and failures.

Employee PC's and trust issued laptop is updated automatically by virus software.

Employee PC's and trust issued laptops are encrypted.

Employee PC's and trust issued laptops do not have administrative rights.

Employees are prohibited from downloading software off the internet, using data storage media including diskettes, CDs, DVDs, and USB thumb drives from outside sources unless authorized by the Trustee or Systems Manager.

Employees are prohibited from transferring trust operation data to their personal PC's, laptops, or tablets.

Employee PC's that are kept under desks on the floor should be kept on a rack to protect from damage that could be caused if the sprinkler system is activated.

Review on an as needed basis between the Trustee and key employees for disaster recovery and continuity of operations during long-term absences from physical office space.

Update employee workstation and network server inventory forms annually listing PC, laptop, printer, phone, and other items located in respective office and home workspaces. (Appendix L). Model and serial numbers should be included.

V. Director of Operations/HR Manager/Office Manager Responsibilities

It is important to consider how disasters impact employees' personal lives, as well as their work. Assisting employees in developing personal disaster recovery plans, consistent with the company's recovery plan, can make a critical difference in how quickly employees are able to return to work.

A) Preparation

- Ideally the office should implement and maintain a clear business continuity policy in the its policies and procedures handbook. This policy addresses how the company will respond to important human resources issues in the event of a prolonged disruption (including an emergency leave policy, remote working

procedures and communications procedures). However, there are so many different types of disasters that it would make for a very large policies handbook. We suggest keeping the Disaster Plan as a separate document with all emergency information and disaster plan for all types of disasters (tornado, fire, power outages, bomb, active shooter, pandemic, etc.).

- A copy of the Disaster Plan, with all Appendices, should be kept by all exits of the building so that anyone can grab it on the way out of the building

- Review business continuity policy and distribute Emergency Action Quick Reference Information (Appendix Q:) to all new employees during orientation.

- Drills should be completed each quarter with a focus on each type of disaster at least twice a year. Include disasters for your surroundings. (For instance, if you are located in the flight pattern of an airport plane, crashes might occur that involve fires).

- Maintain the contact information contained in the Emergency Action Quick Reference Information. Review regularly to ensure that it is accurate and current. Especially when changes are made to the Disaster Plan.

- **The Employee Phone Directory and Contact Information is not given to all employees for privacy reasons, but it is placed in the disaster packets at the exits.**

B) Response

- Implement communication procedures that may provide employees sufficient notice of important information in the event they are unable to work due to weather or building closures. Suggestion: **Plan Administrator keeps employees advised of developments during disaster and is reasonably available to answer employees' questions. Plan Administrator also confirms that each employee has received communication of an office closure when they are at home or off site.**

- Assist management in ensuring that all employees are accounted for.

- Notify an employee's emergency contact (Appendix B:) or provide emergency agencies with information relating to next-of-kin, as required. **We suggest more than one emergency contact person that can also contact next of kin. This contact information is in the disaster packets as our emergency agencies cannot possibly maintain this information for every employee.**

- Provide trauma or stress counseling services to stabilize the emotional reactions of employees in the aftermath of a disaster. In this regard the office should investigate questions such as**: Who authorizes this service. Most employer-provided health insurance coverage includes a number of**

mental health counseling visits each plan year. Coverage needs to be confirmed and additional questions of who pays for service not covered needs to be investigated, as well as whether wages are paid while an employee is recovering from psycological trauma. Is this workmen's compensation, short or long term disability (not full wage)? The office should also investigate the availability of no cost mental health services.

- Provide notification of the situation to all employees of any alternative work instructions. Example: **Disasters occuring at an out-of-town bank used by the Trusteeship would be cause to identify a backup plan for routine banking and debtors who make electronic payments going directly to a bank.**

- Understand the compliance issues that a disaster may bring, such as ADA (Americans with Disabilities Act), state laws, and reasonable accommodation.

- Understand and impliment, if necessary, terms of any applicable emergency legislation issued due to a disaster.

- Implement payroll procedures to assure employees are properly paid for time worked and in accordance with emergency leave policy standards.

- Provide information regarding the company's involvement in offering emergency assistance (child care, temporary shelter, financial aid) so employees are able to work. Keep in mind, employees may not return to work until their own homes and families are secured.

- Fill critical vacancies through temporary services.

- Provide management with issues and concerns that may need their attention regarding employees.

- Provide recognition for employees whom assisted and played key roles in the recovery process.

VI. Evacuation and Sheltering Plan

A) Evacuation Plan During Office Hours

In the event of an emergency, the Plan Administrator will determine whether an evacuation is necessary. If so, the Plan Administrator will direct an employee to read the Emergency Announcement (Appendix F:) over the office telephone paging system. If the building's fire alarm is sounded, the Emergency Announcement may not be read.

Enter a paragraph describing the location of all emergency exits.

- **Only** if time and safety permit, employees should take personal belongings (purse, coat, medical supplies) with them when evacuating the office.

- The IT Manager, or in his/her absence a member of the Disaster Team, will remove and carry the back-up tape and close the server room.

- A member of the Disaster Team will carry a copy of this Manual.

- Members of the Disaster Team are responsible for ensuring that their assigned areas are vacant.

- Members of the Disaster Team will assume responsibility for any disabled person in their area needing assistance and will appoint at least one employee to remain with the disabled person at all times.

- As soon as time permits, the Plan Administrator will contact the building management office and make them aware of the situation (Appendix I:). If necessary, the Plan Administrator will notify local authorities by dialing 9-1-1.

- Upon exiting the building, employees should stay away from the building to avoid falling glass or debris and report to the designated assembly area (Appendix B:). **Note: this location may be different if the disaster is criminal, such as an active shooter. Local authorities can assist in identifying this location.**

- The Disaster Team will assume responsibility for a head count and will immediately notify the Plan Administrator of any persons unaccounted for or injured.

- If possible, depending upon the type of disaster (such as Active Shooter), the Plan Administrator should attempt to inform building security and/or building management. If the building does not have on site security or management and **if possible**, the Plan Administration should attempt to inform other tenants in the office building of the situation. A contact list for building security, building management and/or the other tenants should be maintained.

B) Sheltering Plan

There may be situations where it is best to ***stay*** inside. The procedures will depend on the nature of the emergency or disaster. While any of these events are unlikely to occur or to result in a lengthy stay it is best to be prepared.

If an emergency requires a **sheltering** plan to be implemented, the Plan Administrator may direct the Disaster Team to be responsible for preparing the location as may be necessary and appropriate, such as:

- Having an emergency radio on hand, along with extra batteries;

- Mobile phones can be useful in providing communication **(the sheltering location should have access to an extension cord and charging cords for cell phones);**

- Connecting a computer to the internet for up-to-date information;

- Supplying the shelter-in-place location with adequate drinking water;

- Having the first aid kit and first aid guide on hand; **locate a first aid kit at each shelter location in your building**

- Collecting food and snacks to keep in a central location;

- Collecting supplies such as tape, plastic bags, paper towels, latex gloves, etc.; **these items should be part of an emergency first aid kit**

- Accounting for and monitoring the safety of all employees during the stay plan.

VII. Emergency Procedures for Various Events & Natural Disasters

A) Data Loss and Cyber-Related Security Breach

While the loss of data or a cyber-related security breach may not threaten the safety of office personnel, it is a potential disaster that can have devastating results in terms of lost work, down time, financial loss, and loss of public confidence in the trusteeship.

1. Data Loss and Data Corruption

Files may become corrupted, damaged, or lost as a result of a system crash, computer virus, or through normal business activity. The following steps should be followed to recover lost data and minimize down time:

- Determines whether computer and operating system should be shut down immediately to limit potential losses.

- Identify files that are lost or corrupted.

- Call, as applicable to the type of emergency or disaster: [*enter the names and contact information for each of the following]:*

    a. *your case management vendor,*

    b. *IT service provider,*

    c. *computer network security provider (e.g., STACS), and*

    d. *cyber-risk insurance agent*

for assistance in recovering lost data and to identify and eliminate the underlying source of the data loss (software failure, hardware failure, virus, malware, ransomware, email compromise, and/or firewall breach). This may include virus scans, reformatting hard drives, reinstallation of software, or replacement of hardware; and

e. local business property insurance agent, for assistance in meeting immediate business loss needs (e.g., assistance in locating and paying for new operating space, replacing computer equipment, meeting business loss-related payroll needs, etc.)

- Review the time of the most recent backup and the occurrence of the crash. This time differential will determine the extent of lost data.

- Restore the system from the most recent backup.

- A printed trace file after the most recent backup and before the system crash is the most valuable tool to use in re-entering lost data. If a trace file is not available, then each employee re-enters data (such as new cases, claims, and receipts).

- After all lost data has been restored or re-entered, run reports to verify the accuracy of the data on the case management system.

- Complete a full backup.

- Begin normal activity on the system.

2. Cyber-Related Security Breach

- Should a cyber-related security breach be detected or suspected, contact [*enter the names and contact information of the following*]:

  a. *your case management vendor,*

  b. *IT service provider,*

  c. *computer network security provider (e.g., STACS), and*

  d. *cyber-risk insurance agent*

  for assistance in identifying the type and severity of the breach, containing the breach, and eradicating the breach. If cyber liability insurance has been purchased, notify insurance vendor and request additional support.

- Determine the extent sensitive data was accessed. Data breach notification may be required by law for affected individuals of any unauthorized acquisition of their unencrypted personal information. *See*, National

Conference of State Legislatures, *Security Breach Notification Laws*, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited May 13, 2022).

- Contact the United States Trustee for additional guidance.

B) Internet/Email Loss

Because of Electronic Case Filing and the substantial reliance on email for communication, a failure in the office's connection to the internet could cause a significant disruption of normal operations. The risk of this happening is minimized by the following:

- Identify an alternate internet service provider, including cellular providers which can provide mobile hotspot connectivity.

- Contact your internet service provider to assist in re-establishing an internet connection.

C) Power Failure

- Flashlights should be kept close at hand during a power failure and provided to each Disaster Team member. They should be tested monthly along with smoke alarms.

- UPS (Uninterrupted Power Supply) devices are in use on the server(s) and [*specify any other devices protected by UPS*] will provide a battery backup for [*how long*]. In the event of a power failure, an alarm will sound on the UPS devices. All work-in-progress on the computer should be saved and computers should be shut down as soon as possible. The Systems Manager should shut down the server(s).

- If it is determined that power will not be restored for some time, the Plan Administrator (Appendix C:) will make a decision regarding evacuating employees.

- The building provides emergency lighting and battery backup for exit signs.

- If the power failure occurs after normal business hours the IT staff will contact the Trustee and the facility to determine the best course of action.

VIII. Threats

A) Active Shooter

In the event of an Active Shooter, quickly determine the most reasonable way to protect your own life and the lives of others in your office.

1. **Evacuate**

   - If possible, issue the Emergency Announcement (Appendix F) as quickly and quietly as possible.
   - Exit the office. Use pre-determined escape routes and meeting locations.
   - Help others escape, if possible.
   - Leave your belongings behind.
   - Once everyone has evacuated, if possible, block exit door to office using anything available, but do not waste time looking for such implements.
   - Once in the safe area, Call 9-1-1 and try to provide location of the active shooter, number of shooters, physical description, number and type of weapons, and number of potential victims.
   - Keep hands visible at all times.
   - Silence your cell phone and other sources of noise.
   - Follow the instructions of any police officer.

2. **Hide out**

   - If evacuation is not possible, hide in an office with a door opening inward.
   - Block door using desk, book shelf, or other means available.
   - Be out of active shooter's view.
   - Lie on the floor.
   - Silence your cell phone and other sources of noise.
   - Call 9-1-1 and try to provide location of the active shooter, number of shooters, physical description, number and type of weapons, and number of potential victims.
   - Do not open door for any reason, except as instructed by a police officer. First verify the officer's identity with the 9-1-1 dispatcher.

3. **Take action against the active shooter**

   - **AS A LAST RESORT, and ONLY WHEN YOUR LIFE IS IN IMMINENT DANGER**, attempt to disrupt and/or incapacitate the active shooter by:

- Acting as aggressively as possible against him/her.
- Throwing items and improvising weapons.

B) Fire

Treat all fire alarms seriously. If the fire alarm sounds, immediately proceed with the evacuation as quickly and safely as possible.

In case of fire, remember the acronym **RACE** for the correct priority of procedures to follow:

R – Rescue: Rescue anyone in immediate danger.

A – Alarm: Report the fire by using the nearest fire alarm pull station. If time permits, call 9-1-1 to report the emergency.

C – Contain: Contain the area by closing all doors where time and safety permits.

E – Extinguish: Extinguish the fire's spread by utilizing a fire extinguisher.

- When evacuating in case of fire, it is especially important not to panic. Do not run. Walk or crawl in a single file line, on the right side of the hallway if possible. This will allow firemen access to the same stairway or door. To prevent smoke inhalation, crawl along the floor in smoke-filled areas. Do not walk upright. Heavy smoke and poisonous gases collect first along the ceiling. Stay below the smoke at all times. Cover nose and mouth with a wet cloth.

- When approaching a closed door, use the palm of your hand and forearm to feel the lower, middle and upper parts of the door. If it is not hot, brace yourself against the door and open it slowly. If it is hot to the touch, **do not** open the door--seek an alternate escape route.

- Do not return to your desk or work area for personal belongings.

- If you are trapped by fire, it is vital that you remain calm so you can clearly think and take corrective action. Remember not to walk upright in smoke-filled areas.

- Put closed doors between you and the heat and smoke. If possible, seal off cracks around doors and vents with wet towels or clothing.

- If you become trapped in a building during a fire and a window is available, place an article of clothing (shirt, coat, etc.) outside the window as a marker for rescue crews.

- Upon exiting the building, report to the pre-determined location (Appendix B:).

C) Bomb Threat

A bomb threat warning may be received by anyone. Persons making such calls do not normally call anyone in particular and will deliver their message to the first person contacted.

The Bomb Emergency Threat Check List (Appendix G:) and the Bomb Threat Warning Card (Appendix H:) should be placed in a readily available location so that it can be pulled out immediately upon receiving such a threat. The Bomb Emergency Threat Check List will assist in asking the proper questions and paying attention to important details during the call.

The Bomb Threat Warning Card (Appendix H:) is a bright color to catch the attention of other personnel in the vicinity of the location where the threat is received. The person receiving the threat should wave this card in the air in order to notify other employees of the emergency. A person seeing this card being waved should immediately notify a supervisor.

There are only two purposes for a caller reporting a bomb threat:

1. The caller has definite knowledge of or believes that a bomb has been or will be placed. He wants to minimize personal injury or property damage. The caller may be the person who placed the bomb or someone else who has become aware of such information.
2. The caller wants to create an atmosphere of anxiety and panic that will possibly result in a disruption of the normal business activities in the building where the device is reported to be located.

Any employee receiving a bomb threat call should ask the caller to give his or her message to a person in a responsible position, preferably to the Trustee, or the next person in the chain of command in the absence of the Trustee. However, if the caller refuses to be transferred to another party, the employee receiving the call should try to obtain all the information listed on the Bomb Emergency Threat Checklist (Appendix G:). The caller should be kept on the line as long as possible. This will aid later in the identification of voice characteristics. If possible, record the call.

<u>If the caller does not state the location of the bomb or the time of possible detonation, you should ask the caller the following questions:</u>

1. <u>Where is the exact location of the bomb?</u>
2. <u>What time is it set for detonation?</u>
3. <u>What does it look like?</u>
4. <u>What is the explosive?</u>

5. Why was it placed?

Legitimate callers usually wish to avoid injury or death. Inform the caller that the building is occupied and the detonation of the bomb could result in death and serious injury of many innocent people. When requesting information, stress that you need the information in order to save lives. Ask the caller to repeat the message. If possible, write every word spoken by the caller on the bomb threat checklist (Appendix G).

Listen closely to the voice (male/female), voice quality (calm/excited), accents and speech impediments. Try to remember if the voice sounded young or old, the tone of the voice, and any other distinguishing characteristics about the person calling. If possible, try to determine the name of the caller, age, sex and mental condition.

Pay particular attention to peculiar background noises such as motors running, sirens, background music, or any other noise that may give a clue as to the origination of the call.

The time the call was received and the time that you hung up the phone are also important.

Immediately after the caller hangs up, you should report the call to the Trustee or your supervisor. The Trustee/Supervisor will immediately call 9-1-1, notify the fire department and law enforcement, and will then contact the property management office. Make yourself available for questions, since the law enforcement or fire personnel will want to talk first hand with the person who received the call.

If any bomb threat is received, building management will be contacted and will activate the fire alarms signaling evacuation. The Disaster Team (Appendix C:) will evacuate all personnel to a safe area. Do not re-enter the building until notified by the Fire Department or law enforcement that it is safe to do so.

D) Disgruntled Persons

An encounter with a disgruntled person may put the safety of the entire office at risk. The disgruntled person may be a debtor, a creditor (such as the ex-spouse of the debtor), or even a co-worker or former co-worker.

In general, there are different degrees of disgruntlement, ranging from mildly irritated to violently angry. A person in a fit of rage poses a threat to life and/or property.

The following are suggested guidelines for dealing with a disgruntled person:

- Remain calm.

- Listen carefully to what the person has to say.

- Be an active listener by stating your interpretation of the individual's point of view ("It sounds like you mean . . ." or "So are you saying . . .").

- Empathize with the person – tell the person "I understand how you feel" or "I realize this is as stressful time for you" or a similar message.

- Ask clarifying questions.

- DO NOT tell the person: "You shouldn't get mad" or "you shouldn't feel that way".

- Respond or talk to the individual rationally in a calm tone of voice. Speak more slowly and softly.

- Be cooperative. DO NOT be argumentative.

- Ask the person to tell you what s/he wants or what s/he wants you to do to resolve the dispute. If necessary to protect your safety, do what s/he wants or assure him or her that you will personally make sure the situation is taken care of.

- If possible and if the situation warrants, activate a silent alarm by pressing a panic button to alert authorities.

- If possible, evacuate the area; if not, have employees stay in their offices.

- If at any time a visitor becomes disruptive, unruly, harassing, uses abusive or threatening language or gestures, or in any way makes an employee uncomfortable or scared, the employee should not hesitate to ask the visitor to leave. In the alternative, the employee should remove himself/herself from the visitor and notify the Trustee, a supervisor (or a coworker if a supervisor is not available).

- All suspicious persons or activities should be reported as soon as possible to the Trustee and a supervisor. Do not place yourself in peril. If you see or hear a commotion or disturbance near your work station, do not try to intercede or see what is happening.

E) Hazardous Material

Combining certain cleaning materials may inadvertently produce a hazardous or toxic material.

In this event, a law enforcement officer or fire official will come to the building and inform employees of the need to evacuate the area. The Disaster Team and/or the building management office will consult with the law enforcement officer or fire

official to determine best possible routes to leave the area and the length of time evacuation may be necessary.

In the event an evacuation is necessary, the Plan Administrator will direct a member of the Disaster Team to issue the Emergency Announcement (Appendix F:). Upon hearing the Emergency Announcement, employees should remain calm and follow the Evacuation Plan or other special instructions.

In the event hazardous materials are received through the mail, an immediate evacuation may not be prudent. Instead, it may be safer for everyone to remain in their offices until the authorities have contained the hazardous material. In such an event, employees will be notified to stay where they are and avoid the potentially contaminated area.

F) Disease Epidemic or Pandemic

An epidemic (the rapid spread of a disease that affects some or many people in a community or region at the same time) or pandemic (an outbreak of disease that affects large numbers of people around the world) could result in high levels of absenteeism for extended periods of time. Employees could be absent because they are sick, or they must care for sick family members, or they must care for children if schools or day care centers are closed. An epidemic or pandemic could also affect the delivery of supplies and services to the Trustee's office. It could result in the rescheduling of creditor meetings and/or court hearings and cause delay in the normal progression of cases.

The most likely cause of a pandemic at this time would be influenza, COVID-19, or similar dangerous virus. A pandemic may be widespread, affecting multiple areas of the United States and other countries at the same time. A pandemic will also be an extended event, with multiple waves of outbreaks in the same geographic area; each outbreak could last from six to eight weeks or longer. Waves of outbreaks may occur over a year or more. A pandemic could affect as many as 40 percent of the workforce during periods of peak influenza illness.

Because of the extensive contact certain employees have with the general public at section 341 meetings and at court hearings, office personnel who must have face-to-face interaction with the general public are at a medium exposure risk of contracting a pandemic strain of influenza, COVID-19, or similar dangerous virus. In the event of a pandemic or epidemic, the Trustee may seek alternatives to minimize the risk of exposure, for example: increasing the distance between employees and the public (including the debtor, the attorney, and any creditor attending the 341) so that the attorney is more than six feet away; conducting more 341 meetings by interrogatories; conducting 341's via conference calls or web conferences; handling motions to dismiss by agreed orders with counsel; wearing masks and gloves to 341's and other hearings; requesting telephonic court hearings; etc.

In the event an epidemic or pandemic reduces the Trustee's staff levels for an extended period of time, the Plan Administrator will need to establish priorities of operation and change the essential job functions of the remaining employees to accomplish those tasks of highest priority. The Disaster Recovery section of this Manual contains more information regarding work priorities. It may be that some employees will be able to telecommute or otherwise work from home, even on a part-time basis.

Vaccines may protect employees from severe illness and death. After an employee is fully vaccinated, they should still wear a mask in indoor public places. Make sure the mask covers your nose and mouth and secure it under your chin.

G) Water Damage

In the event of water damage or broken pipes, the following risks to life and property may occur:

- Electrocution hazard to employees.
- Damages caused by an electrical short-circuit.
- Damage to computer and other office equipment.
- Damage to case files and other paper documents.

In the event of water damage from a broken pipe, the Disaster Team will immediately notify the building management office and request a maintenance team to evaluate the problem.

All employees should be extremely cautious around damp or wet computers, office equipment, electrical cords, and outlets due to danger of electrocution.

If there is no apparent threat of life, computers and office equipment should be protected by covering or removing them to a dry area.

If possible, remove any case files and business records from the area.

The Plan Administrator will determine whether an evacuation is necessary.

If the power failure occurs after normal business hours, the IT staff will contact the Plan Administrator and the facility to determine the best course of action.

H) Severe Weather or Natural Disasters

1. Tornado

There are two defined conditions recognized by the National Weather Service:

Tornado Watch: Although the conditions are right for a tornado to occur, none have been sighted in the area. In the event of a tornado watch, employees should remain at their desks and continue to work, as this is only a precautionary alert.

Tornado Warning: This means a tornado has actually been spotted in the local area.

In the event of a tornado watch affecting the immediate area, a member of the Disaster Team should turn on a battery-operated radio and make sure spare batteries are immediately available.

In the case of a ***tornado warning or an actual sighting***, the Plan Administrator will direct a member of the Disaster Team to issue a Tornado Emergency Announcement (Appendix F:). The following procedures should be followed:

- Remain calm.
- Do not attempt to evacuate the building unless instructed by the authorities.
- If time permits take the emergency action kit and move immediately away from the perimeter of the building and exterior glass.
- If applicable and possible, proceed to the nearest stairwell. A member of the Disaster Team will bring the radio to the stairwell. Wait until danger has passed.
- If time does not permit evacuation to the stairwell, move to an interior room or interior hallway.
- As a last resort, if time does not allow evacuation from exterior offices, position yourself under a desk or sturdy table.
- Wherever you are when a tornado strike is imminent, sit or kneel, and protect yourself by putting your head as close to your lap as possible.
- If you are caught outside and do not have time to reach a safe building, go to a low/safe place. Remember to be alert for flash floods that often accompany tornadoes.
- Provide first aid if needed.
- Call 9-1-1 if a tornado causes serious injuries.
- The assigned Disaster Team member will do a head count when danger has passed.

2. Earthquake

If you are indoors when an earthquake occurs, take shelter under your desk or a table. If this is not possible, stand in a doorframe, stairwell, or under any strong, sturdy object to protect yourself from falling debris. Keep away from areas containing glass. Avoid windows, outside doors, and shelving units or filing cabinets.

If you are trapped in debris: Use a flashlight. Stay in your area so that you don't kick up dust. Cover your mouth with a handkerchief or clothing. Tap on a pipe or wall to alert rescuers of your location. Use a whistle if one is available. Shout only as a last resort--shouting can cause a person to inhale dangerous amounts of dust.

If you are outdoors when an earthquake occurs, stay outdoors, preferably away from structures. Do not attempt to enter or leave a building until you are instructed to do so. Stay away from overhead electric wire, poles, or anything that might shake loose and fall.

Remain in your sheltered area until advised movement is safe. When it is safe to exit the building, employees should remain calm and follow the Evacuation Exit Plan.

Aftershocks can be as dangerous as the initial quake. Do not re-enter the building or work areas until the structure has been evaluated. Stay away from fallen or damaged electrical wires, and be aware of the smell of ruptured natural gas lines that have a potential to cause explosion or fire. A decision to re-enter the building and resume business will be made by the Plan Administrator (Appendix C:), building management, and/or local authorities.

3. Winter Storms

Winter storms may cause hazardous walking and driving conditions. If a major storm occurs or is imminent prior to the commencement of work, the Trustee may decide not to open the office location, but remote telecommuting may remain possible. If so, the Trustee will activate the calling tree (Appendix E:). Unless contacted, employees are to assume the office will be open and should report for work as usual.

If the storm occurs during the day while employees are at work, a decision will be made by the Plan Administrator as to the closing of business and allowing employees to return to their homes. Sometimes it is safer to remain in the building as opposed to venturing out into the elements.

If indoors:

- Stay calm and await instructions from the Plan Administrator, a member of the Disaster Team, State Emergency Management personnel, or law enforcement or fire department personnel.

- Stay indoors!
- If there is no heat:
  - Close off unneeded rooms or areas.
  - Stuff towels or rags in cracks under doors.
  - Cover windows at night.
- Eat and drink. Food provides the body with energy and heat. Fluids prevent dehydration.
- Wear layers of loose-fitting, light-weight, warm clothing, if available.

If outdoors:

- Find a dry shelter. Cover all exposed parts of the body.
- If shelter is not available:
  - Prepare a lean-to, wind break, or snow cave for protection from the wind.
  - Build a fire for heat and to attract attention. Place rocks around the fire to absorb and reflect heat.
  - Do not eat snow. It will lower your body temperature. Melt it first.

4. Flood

If indoors:

- Be ready to evacuate as directed by the Emergency Coordinator and/or the designated official.
- Follow the recommended primary or secondary evacuation routes.

If outdoors:

- Climb to high ground and stay there.
- Avoid walking or driving through flood water.
- If car stalls, abandon it immediately and climb to higher ground.

5. Hurricane

The nature of a hurricane provides for more warning than other natural and weather disasters. A hurricane watch is issued when a hurricane becomes a threat to a coastal area. A hurricane warning is issued when hurricane winds of 74 mph

or higher, or a combination of dangerously high water and rough seas, are expected in the area within 24 hours.

Once a hurricane watch has been issued:

- Stay calm and await instructions from State Emergency Management personnel, or local law enforcement or fire department personnel. .
- Moor any boats securely, or move to a safe place if time allows.
- Continue to monitor local TV and radio stations for instructions.
- Move early out of low-lying areas or from the coast, at the request of officials.
- If you are on high ground, away from the coast and plan to stay, secure the building, moving all loose items indoors and board up windows and openings.
- Collect drinking water in appropriate containers.

Once a hurricane warning has been issued:

- Evacuate inland if in the path of the storm or be ready to evacuate.
- Stay tuned to local television or radio weather reports to remain informed of imminent danger and any government-issued evacuation orders.
- Comply with orders issued by State Emergency Management personnel, or law enforcement or fire department personnel. Leave areas that might be affected by storm surge or stream flooding.

During a hurricane:

- Remain indoors and consider the following as the safest options for sheltering in place:
  - Small interior rooms without windows,
  - Hallways, away from doors and windows,
  - Rooms constructed with reinforced concrete, brick, or block with no windows,
  - Any of the foregoing on the lowest floor of the building in which you are located, provided flooding resulting from storm surge is unlikely.

I) Bioterriorism

1. Reporting Requirements and Contact Information

In the event a bioterrorism (BT) event is suspected, local emergency response systems should be activated. Notification should immediately include local infection control personnel and the community's administration, and prompt communication with the local and state health departments, FBI field office, local law enforcement and fire departments, CDC, and emergency medical services. **Each Chapter 13 office should include a list containing the following telephone notification numbers in its readiness plan**:

CONTACTS:

- STATE HEALTH DEPARTMENT
- FBI FIELD OFFICE
- CDC Emergency Response Office (770) 488-7100
- CDC HOSPITAL INFECTIONS PROGRAM (404) 639-6413

ADDITIONAL CONTACTS:

The following contacts may be provided if available in your area:

- INFECTION CONTROL EPIDEMIOLOGIST
- ADMINISTRATION/PUBLIC AFFAIRSLOCAL HEALTH DEPARTMENT
- BIOTERRORISM EMERGENCY NUMBER

2. Detection of Outbreaks Caused by Agents of BT

BT occurs as covert events, in which persons are unknowingly exposed and an outbreak is suspected only upon recognition of unusual disease clusters or symptoms. BT may also occur as announced events, in which persons are warned that an exposure has occurred. A number of announced BT events occurred in the United States during 1998-1999, but those were determined to have been "hoaxes;" that is, there were no true exposures to BT agents. A healthcare facility's BT readiness plan should include details for management of both types of scenarios: suspicion of a BT outbreak potentially associated with a covert event and announced BT events or threats. The possibility of a BT event should be ruled out with the assistance of the FBI and state health officials.

3. Infection Control Practices

Standard precautions prevent direct contact with all body fluids (including blood), secretions, excretions, nonintact skin (including rashes), and mucous membranes. Standard precautions routinely practiced by healthcare providers include:

- **Handwashing**

  Hands are washed after touching blood, body fluids, excretions, secretions, or items contaminated with such body fluids, whether or not gloves are worn. Hands are washed immediately after gloves are removed, between contacts, and as appropriate to avoid transfer of microorganisms to others and the environment. Either plain or antimicrobial-containing soaps may be used according to policy.

- **Gloves**

  Clean, non-sterile gloves are worn when touching blood, body fluids, excretions, secretions, or items contaminated with such body fluids. Clean gloves are put on just before touching mucous membranes and nonintact skin. Gloves are changed between tasks and between procedures on the same person if contact occurs with contaminated material. Hands are washed promptly after removing gloves.

- **Masks/Eye Protection or Face Shields**

  A mask and eye protection (or face shield) are worn to protect mucous membranes of the eyes, nose, and mouth while performing procedures and care activities that may cause splashes of blood, body fluids, excretions, or secretions.

- **Gowns**

  A gown is worn to protect skin and prevent soiling of clothing during procedures and care activities that are likely to generate splashes or sprays of blood, body fluids, excretions, or secretions. Selection of gowns and gown materials should be suitable for the activity and amount of body fluid likely to be encountered. Soiled gowns are removed promptly and hands are washed to avoid transfer of microorganisms to others.

  Local, state, and federal media experts can provide assistance with communications needs.

4. SPECIFIC BIOTERRORISM AGENTS

- **Anthrax**

  Anthrax is an acute infectious disease caused by *Bacillus anthracis,* a spore forming, gram-positive bacillus. Associated disease occurs most frequently in sheep, goats, and cattle, which acquire spores through ingestion of contaminated soil.

- **Botulism**

  Clostridium botulinum is an anaerobic gram-positive bacillus that produces a potent neurotoxin, botulinum toxin.

- **Smallpox**

  Smallpox is an acute viral illness caused by the variola virus.

  Smallpox is a bioterrorism threat due to its potential to cause severe morbidity in a nonimmune population and because it can be transmitted via the airborne route.

VIII. Disaster Recovery

The Plan Administrator is primarily responsible for overseeing and organizing loss recovery efforts. Given the many tasks that must be accomplished in a short amount of time following a disaster, the assistance of the Disaster Team is essential. The Disaster Recovery Plan (below) should be used as a guideline for quickly restoring normal business operations.

The short-term recovery objective is to restore critical functions of the office within a week following the disaster. The long-term recovery objective is to re-establish the Chapter 13 Trustee office to full capacity as quickly and efficiently as possible.

A) The Assessments

Following a disaster, the Disaster Team must perform a damage assessment (Appendix F:). The following **disaster levels** are listed in order of priority from lowest to highest.

0 - No damage

1 - Minimal destruction of property and/or data; and/or no injury to personnel; and/or minimal absence of personnel - minimal disruption of normal operations (estimated 5 business days or less to return to normal)

2 - Partial destruction of property and/or data; and/or minor injuries to personnel; and/or absences of multiple personnel - partial disruption of normal operations (estimated 6 to 10 business days to return to normal)

3 - Extensive or complete destruction of property and/or data; and/or major injuries or loss of life; and/or extended absences of multiple personnel - major disruption of normal operations (estimated 10 business days or more to return to normal).

In addition, the **scope** of the disaster may affect the recovery plan.

Local – damage is limited to the building and/or data and/or equipment and/or personnel.

Community – damage impacts the larger metropolitan or geographic area.

Regional – damage is widespread, extending throughout the region.

B) Disaster Recovery Plan

Initial Response (1-4 Completed Within 24 Hours of Disaster)

1. The Plan Administrator will assemble all available Disaster Team members for initial project planning.

2. The Plan Administrator will initiate a personnel assessment to determine from each employee if s/he is physically able to work and to travel to work. The Plan Administrator should also inquire regarding real or personal property damage sustained by the employees.

3. The Plan Administrator will notify the U.S. Trustee, your banking institution, the insurance companies, and the Judges' Chambers. The Plan Administrator will provide disaster information to the IT Manager. The IT Manager will notify your case management vendor and the Clerk's office.

   - *Trustee should determine and include in his or her Plan, the appropriate parties and the order in which they should be contacted based upon the nature of the emergency or disaster and its effect on the Trustee's ability to perform his or her statutory duties.*

4. The Disaster Team will perform a damage assessment in each area of the office, record the amount and type of damage on the Disaster Assessment Form (Appendix K:), and submit the completed forms to the Plan Administrator**.**

5. The Plan Administrator and IT Manager will determine what computer equipment is essential to restoring critical operations; and, if necessary, will begin purchasing the replacement equipment.

6. The IT Manager will assess the condition of the backup media and will begin the process of data recovery, if necessary.

7. The Plan Administrator, in consultation with building management and the Trustee's business insurance agent, will determine if temporary relocation of the office is necessary, and will determine an estimated duration of the relocation.

8. If relocation is necessary, the Disaster Team will search for temporary office space.

9. The Disaster Team will notify the Post Office and key vendors as necessary to maintain or restore continuity of operations.

10. If necessary, the Disaster Team may need to secure a new permanent office location if the existing office cannot be rebuilt in a reasonable amount of time. If so, the checklists used by the Trustee when the office moved to its present location may be helpful.

11. The Disaster Team will contact vendors and arrange for replacement equipment, furniture, and office supplies as necessary.

12. If necessary, the Disaster Team will purchase mobile telephones for office use and establish new mobile service. Where applicable, mobile broadband cards for laptop computers and mobile broadband service may be useful in resuming access to ECF and emails quickly.

Re-establishing Operations

The priorities will be set based on the nature of the emergency or disaster suffered and what is needed to get the office up and running as quickly as possible. It will be impossible to state what the priorities will be to get the office functioning; each scenario will be different based on the damages caused by the disaster. A typical set of priorities will focus on.

1. Determining the best method of and maintaining communication with employees, debtors, creditors, attorneys, the U.S. Trustee's office, and the court.

2. Restoring or replacing computer hardware, software, and other office equipment, and recovering and securing any physical assets and computer files.

3. Ensuring continued continuity of vendor service essential to the office's operation.

4. Establishing a secure way to handle incoming receipts and posting receipts to existing cases.

5. Establishing a secure way to disburse receipts.

6. Establishing a way to retrieve documents from the court and the creation and input of new cases, input of claims, amendments, motions, and orders, etc., received in the Trustee's cases.

7. Preparing and processing cases for confirmation, modification, dismissal, and closing.

8. Establishing a process to administer accounts payable and receivable and to maintain and process employee payroll.

9. Establishing a security system.

Appendix A: **Floor Plan**

Appendix B: **Designated Assembly Area**

- Indicate all locations if different for fire, bomb, or other threat.

Appendix C: **Disaster Team Members**

(Include all contact information for each)

1. *Member One*
2. *Member Two*
3. *Member Three*
4. *Member Four…*

PLAN ADMINISTRATOR (including all contact information for each):

1. Trustee, or in his/her absence, the next person in the following chain of command:
2. *Second in Command*
3. *Third in Command*
4. *Fourth in Command*

INFORMATION TECHNOLOGY MANAGER:

EVACUATION TEAM:

1. *Team Member1* – Responsible for Head Count
2. *Team Member2 – Responsible for Head Count in absence of Team* Member1

OFFICE EMPLOYEES:

List Employees Here

Appendix D: **Employee Phone Directory & Contact Information**

Name	**Home Address**	**Home Phone**	**Mobile Phone**	**Office & Home Email**	**Emer. Contact (name and contact info.)**

Appendix E: **Employee Calling Tree**

Appendix F: **Emergency Announcements**

Evacuation

In the event of an emergency **that requires evacuation of the building**, the Plan Administrator will issue the following announcement:

"Attention. Attention. An emergency has been reported. Please exit the office and evacuate the building immediately. Report to the assembly area at [*specify where*]. Repeat – an emergency has been reported. Please exit the office and evacuate the building immediately. Report to the assembly area [*specify where*]."

Active Shooter-if possible, issue the above announcement, specifying that the emergency is an active shooter.

Fire Alarm-no announcement necessary. See page 12.

Tornado

In the event of a **tornado** that does not require evacuation of the building, the Plan Administrator will issue or designate a member of the Disaster Committee to issue the following announcement:

"Attention. Attention. A tornado sighting has been reported. Please exit the office and meet [*specify where*]. Repeat – a tornado has been reported. Please exit the office and meet [*specify where*]. DO NOT LEAVE THE BUILDING. Repeat – DO NOT LEAVE THE BUILDING."

Remain in Building

In the event of an emergency that requires employees to remain in their offices until further notice (such as receipt of contaminated mail), the responsible person should make the following announcement:

"Attention. Attention. An emergency has been reported. Please *stay in your office* and close your door until further notice. Repeat – *stay in your office* and keep your door closed until further notice."

Appendix G: **Bomb Threat Emergency Checklist**

INSTRUCTIONS: **BE CALM, BE COURTEOUS. LISTEN.** ***DO NOT INTERRUPT THE CALLER*****.**

YOUR NAME: _____ TIME: _____ DATE: _____

CALLER'S IDENTITY SEX: Male _____ Female ____ Adult ____ Juvenile ____ APPROXIMATE AGE: _____

ORIGIN OF CALL: Local _____ Long Distance _____ Telephone Booth _____

VOICE CHARACTERISTICS		**SPEECH**		**LANGUAGE**	
___ Loud	___ Soft	___ Fast	___ Slow	___ Excellent	___ Good
___ High Pitch	___ Deep	___ Distinct	___ Distorted	___ Fair	___ Poor
___ Raspy	___ Pleasant	___ Stutter	___ Nasal	___ Foul	_____
___ Intoxicated	_____	___ Slurred	_____		Other
___ Agitated	Other		Other		

ACCENT		MANNER		BACKGROUND NOISES	
___ Local	___ Not Local	___ Calm	___ Angry	___ Factory	___ Trains
___ Foreign	___ Region	___ Rational	___ Irrational	___ Machines	___ Animals
___ Race	(_____)	___ Coherent	___ Incoherent	___ Music	___ Quiet
		___ Deliberate	___ Emotional	___ Office	___ Voices
		___ Righteous	___ Laughing	___ Machines	___ Airplanes
				___ Street	___ Party
				___ Traffic	___ Atmosphere

BOMB FACTS

PRETEND DIFFICULTY HEARING – or "We have a bad connection; Could you repeat that?" KEEP CALLER TALKING - IF CALLER SEEMS AGREEABLE TO FURTHER CONVERSATION, ASK QUESTIONS LIKE:

When will it go off? Certain Hour _____ Time Remaining _____

Where is it located? Building _____ Area _____

What kind of bomb? _____

What kind of package? _____

How big is it? _____

What does it look like? _____

Why was it placed? _____

How do you know so much about the bomb?_____

What is your name? _____ **and your address?** _____

If building is occupied, inform caller: **"Do you know that detonation could cause injury or death?"**

Activate malicious call trace: Hang up phone and do not answer another line. Choose same line and dial *57 (if your phone system has this capability). Listen for the confirmation announcement and hang up.

Call Security at _____ and relay information about call.

[continued on next page]

Did the caller appear familiar with building location or the area (by his/her description of the bomb location)? Yes ____ No ____ Could not tell _____

Write out the message in its entirety and any other comments on a separate sheet of paper and attach to this checklist.

Notify the Trustee and your supervisor immediately.

Appendix H: **Bomb Threat Warning Card**

BOMB THREAT WARNING CARD

BOMB
THREAT
WARNING

Caller is on the line.
Notify supervisor!

Appendix I: **Disaster Notification Phone Directory**

Office of the U.S. Trustee: *Enter name and address* Phone**:** Fax:	Financial Institution: *Enter name and address* Phone: Fax:
Case Management Vendor: *Enter name and address* Phone: Fax:	Office of the Clerk: United States Bankruptcy Court _____ District of _____ *Enter name and address* Phone**:** Fax:
Law Enforcement: *Enter name and address* Phone**:** Fax:	Fire Department: *Enter name and address* Phone**:** Fax:
Building Manager (if applicable): *Enter name and address* Phone**:** Fax:	Federal Protective Service: *Enter name and address* Phone**:** Fax:
Computer Network Security Provider (if applicable): *Enter name and address* Phone**:** Fax:	Cyber Risk Insurance Agent (if applicable): *Enter name and address* Phone**:** Fax:

Appendix J: **Vendor List**

Vendor	Address Phone	Account No.	Contact

Appendix K: **Disaster Assessment Form**

After a disaster, the following scale will be used to assess damage:

0 – No Damage.

1 – Minimal destruction of property and/or data (minimal disruption of normal operations).

2 – Partial destruction of property and/or data (partial disruption of normal operations).

3 – Extensive or complete destruction of property and/or data (major disruption of normal operations).

ITEM	**SCALE (0 – 3)**	**NOTES**
Computers and monitors	_____	_____
Server & Connectivity	_____	_____
Printers	_____	_____
Fax machine	_____	_____
Telephone system	_____	_____
Security system	_____	_____
Cubicles, desks, chairs	_____	_____
Office supplies	_____	_____
Filing cabinets & shelving	_____	_____
Case files	_____	_____

Appendix L: **System Hardware And Software List**

Appendix M: **Inventory (Asset) List**

Appendix N: **Emergency Action Kits**

Main Office Kit

- Helmets
- Rope
- Work Gloves
- Radio
- Flashlights (snap lights)
- Duct Tape
- Multi-head Screwdriver
- Insulated Blankets
- Vise-grips
- Goggles
- Crowbar
- Dust masks
- Ponchos
- Walkie Talkies (1 per disaster team member)

Employee Evacuation Kits

- First Aid Pack (wipes, ointment, Band-Aids)
- Gauze pads
- Burn gel
- Toothbrush
- Eye pads
- Tongue depressor, q-tips
- Insulated Blanket
- Toilet Pack (wipes, tissue, paper cups)
- Drinking Water Pouches
- Food Bars
- Snap lights
- Medical tape
- Dust mask
- Latex gloves
- Whistle
- Strike anywhere matches

Appendix O: **Form List**

1. Check Stock: Expense & Trustee Accounts
2. …..
3. ….

Appendix P: **Emergency Action Quick Reference Information**

IN CASE OF EMERGENCY:

- **CALL BUILDING SECURITY IF APPLICABLE**
- **DIAL 9-1-1**

FIRE EXTINGUISHERS:

- How many, location, expiration date, who monitors?

FIRE ALARM:

- How many and where are they located?

FIRST AID KITS:

- How many and where are they located?

DISASTER TEAM & PLAN ADMINISTRATOR:

1. Trustee Name, Plan Administrator, (Telephone Contact Number)
2. Team Member Name/Position (Back-up Plan Administrator) (Telephone Contact Number)
3. Team Member Name/Position, (Telephone Contact Number)
4. Team Member Name/Position, (Telephone Contact Number)

Appendix Q: **Evacuation Checklist**

Steps	**Action Complete**	**Actions Taken**
1		Take Emergency Action Kit (Appendix N:) and the Emergency Action Plan Handbook as you exit the building.
2		If time and safety permits, attempt to take the backup and/or hard drive storage media from the datacenter.
3		If time and safety permits, check the work areas to make sure everyone has exited.
4		Exit the building via the closest or safest exit route determined by the Plan Administrator or by building management/security.
5		After exiting the building, proceed immediately to the pre-determined assembly area to rejoin coworkers.
6		Upon arrival at the pre-determined assembly area, take a head count and identify anyone who is missing or injured.
7		Report any missing or injured individuals to the safety or rescue personnel as soon as possible.

Appendix R: **Sheltering Checklist Card**

Steps	**Action Complete**	**Actions Taken**
1		Take Emergency Action Kit (Appendix N:), Emergency Action Plan Handbook and **WEATHER RADIO**.
2		INSTRUCT STAFF NOT TO ATTEMPT TO LEAVE THE BUILDING FOR ANY REASON!
3		Move as far away from windows and exterior walls as possible.
4		If time and safety permits, attempt to take the backup and/or hard drive storage media from the datacenter.
5		If time and safety permits, check the work areas to make sure everyone has exited.
6		Meet at the pre-determined assembly area nearest to the center of the building.
7		Upon arrival at the pre-determined assembly area, take a head count and identify anyone who is missing or injured.
8		Report any missing or injured individuals to the safety or rescue personnel as soon as possible.