**FRAMEWORK FOR DEVELOPING**

**A BUSINESS INTERRUPTION PLAN**

**FOR A CHAPTER 7 TRUSTEE OPERATION**

* **A business interruption, as used herein, may be caused by a storm, earthquake, fire, power surge or outage, hard disk failure, incapacity of the trustee or staff person, or similar event.**
* **This framework for developing a business interruption plan is offered to panel trustees to help them develop a plan for minimizing the risk of disruption or loss to their chapter 7 operation as a result of a business interruption.**
* **Unless otherwise indicated by a reference to the *Handbook for Chapter 7 Trustees (Handbook)*, the items and procedures listed below are suggestions, not requirements.**
* **Trustees are encouraged to consult additional information resources, such as** [**http://www.fema.gov/pdf/business/guide/bizindst.pdf**](http://www.fema.gov/pdf/business/guide/bizindst.pdf)**,** [**https://www.dhs.gov/hometown-security**](https://www.dhs.gov/hometown-security)**, and** [**https://www.ready.gov/business**](https://www.ready.gov/business)**.**

**I. Introduction**

The *Handbook for Chapter 7 Trustees* indicates that a trustee must develop and maintain a written business interruption plan for the estate financial and administrative records, as well as for the computer system and data. A printed copy of the plan should be stored in the trustee’s office and at an offsite location known to the trustee and staff. This framework for a business interruption plan has been developed in response to trustee requests for guidance in developing such a plan. The title “business interruption plan,” rather than “disaster recovery plan,” has been used to connote that the plan covers more than just disaster preparedness and recovery.

There is a wide variety of information resources on the topic of business interruptions and disaster recovery. The authors of this document consulted FEMA’s *Emergency* *Management Guide For Business and Industry*, articles from various trade publications, and United States Trustee Program employees. Trustees are not bound to and should not rely solely on this document to fulfill their business interruption planning responsibilities.

The type and extent of the business interruption plan is at the trustee’s discretion. While plans may vary widely among trustees, all plans will share the common goals of preventing business interruptions when possible and restoring operations promptly and economically when business interruptions occur.

**II. Business Interruption Considerations**

The trustee should take steps to avoid business interruptions and have a plan of action ready to follow in the event that a business interruption occurs. The trustee should conduct a risk assessment to identify areas of vulnerability such as incapacity or death of the trustee or an employee; sudden personnel changes; major computer malfunction; and natural or man-made disasters, and provide guidelines for addressing them.

Considerations for business interruption planning:

1. The plan should describe the appropriate safeguards to prevent or minimize interruptions and downtime. The trustee should review the safety and integrity of the building, records, and computer system and consider installing security alarms, smoke detectors, fire extinguishers, fire proof cabinets, surge protectors, an uninterruptible power supply, and other safety and protective equipment. Follow the computer security and back-up procedures listed in Chapter 5.G.3.e.

a. Obtain and review the building’s safety, security, and evacuation plan. If none exists, consider working with the landlord or building owner to develop one. Alternatively, develop such a plan for the trustee operation. The plan should include avoidance controls as well as recovery strategies.

b. Identify key records and sources for replacement.

c. Perform daily back-ups of case management records (in accordance with Handbook requirements) and frequent back-ups of other data. Keep the back-ups for several successive days. At least weekly, store a copy of the back-up offsite (also required per the Handbook).

(1) Back-up program and data files, word processing documents, and emails. If program files are not backed up, ensure they are easily and quickly available from other sources.

(2) Test the back-up files regularly.

(3) Periodically rotate and replace the back-up media to ensure its continued reliability.

e. Contact the software and hardware vendor(s) to determine if they will timely provide technical support and replacement computers and software. If a vendor system is not used or the vendor does not offer the support needed, develop an alternate plan, such as making arrangements with trustees or businesses in another city to assist each other in the event of a business interruption.

f. Obtain virus protection software and download updates from the manufacturer’s web site daily (as required per the Handbook). Determine how it works and use it routinely. Ensure that employees do likewise. If it is necessary to turn it off while loading other programs, be sure to turn it back on. Periodically check to verify that the software is turned on.

g. Only authorized users should be able to gain access to the chapter 7 case management system (as stated in the Handbook).

(1) Ensure that unique computer passwords are used, safeguarded, and changed at least quarterly or when an employee leaves or no longer has chapter 7 responsibilities. Change default passwords and passwords set up by the software provider during installation and training.

(2) To help prevent system and software access by hackers and other unauthorized users, turn off the computer after business hours or install a firewall or intruder detection software.

(3) Use the software’s built-in security access control features to limit access to key application functions, particularly when access is provided to individuals other than the trustee and the trustee’s primary assistant. These controls enable the trustee to define each person’s access to the application’s features. For example, the check writing function should be accessible only to the trustee and the person responsible for generating the checks for the trustee’s signature. Similarly, access to the operating system and the software application programming, as well as the ability to change the security access controls, should be limited to the trustee.

(4) Ensure that the trustee and at least one other employee (if any) know how to perform all key functions.

2. The plan should identify an alternate location where business operations can be resumed in the event the trustee and staff cannot access the office, and provide procedures for arranging for mail to be delivered to the alternate work site. Consider establishing an off-site storage location for keeping duplicate copies of irreplaceable records, an inventory of critical supplies that cannot be purchased and received within 2-3 days, a copy of an appointments/due dates/deadlines calendar that is updated weekly, as well as other important records. If possible, the off-site location should provide an emergency storage site to hold any salvageable equipment and records.

3. If applicable, the plan should include information regarding the trustee’s business interruption, valuable-papers, key employee, and other applicable coverage. Regularly review the adequacy of insurance coverage.

4. The plan should include a current list of key telephone numbers (e.g., insurance, police, fire, trustee, employees, computer vendors, landlord, utilities, vendors, UST). The list should be kept on- and off-site.

5. The plan should designate a place for staff to meet (or phone number to call) after the disaster.

6. The plan should identify other appropriate actions to take in the event that a disaster or other business interruption occurs.

7. Establish a salvage priority list (i.e., designate assets in order of importance).

8. Develop a “to do” list in case advance warning of a disaster is available (e.g. 24 hour advance notice of a hurricane warning).

a. Remove or safeguard the records and equipment listed on the salvage priority list.

b. Physically protect the premises (plywood or tape windows, wrap cabinets in plastic, etc).

c. Shut off utilities (if trained to do so).

9. Develop a list of procedures to perform after a disaster or business interruption. The list may include the following:

a. Gather staff to assign tasks and review salvage priorities. Notify appropriate parties on the emergency contact list.

b. Determine if the premises can be safely entered/used. If the premises can be safely entered, assess the damage to records and equipment. Document the damage for insurance purposes.

c. Retrieve and/or protect equipment and records. Prioritize between undamaged and damaged goods. Utilize the salvage priority list to protect the most vital records and equipment first. If necessary, move equipment and documents to the alternate work site.

d. Contact computer software providers, insurance agents, and appropriate vendors to assist in reestablishing operations. Contact the UST, Court, and trustee’s attorneys regarding acquiring copies of damaged records.

e. If applicable, arrange for mail to be delivered to the alternate work site.

10. Keep familiar with the contents of the plan by reviewing it at least annually. When systems and circumstances change, update the plan as appropriate.

11. Discuss the business interruption plan and contingency plans with family members. Include a discussion of the United States Trustee’s role in the event of incapacity or death of the trustee.

12. Notify the United States Trustee as soon as possible after a business interruption occurs, particularly when the computer system has been breached, if there has been a fire or other major catastrophe, and when there has been a break-in at the office.

**Note: As indicated throughout, trustees may use their discretion in developing a business interruption plan and in undertaking any additional safety and security measures that are appropriate for their trustee operation. Some of the items listed here are required by the *Handbook for Chapter 7 Trustees*, but most are suggestions to help the trustee plan ahead for a potential business interruption. Questions concerning these guidelines or business interruption plans, in general, should be directed to the United States Trustee.**