BUSINESS CONTINUITY POLICY

City of Helena/Lewis and Clark County IT&S

Information Security Policy Manual

Version Control

Policy Code:	ITSEC008	Approved By:	IT&S Steering Committee 3/24/2021 IT Board 4/8/2021
Owner:	IT&S	Effective Date:	4/8/2021

Revision History

Date	Version	Created by	Description of change

Table of Contents

1. Purpose and Scope

The purpose of this document is to provide guidelines for preparing for and responding to unforeseen or unexpected emergencies or other occurrences (e.g., fire, vandalism, system outage, natural disaster) that pose a potential threat to the availability of City of Helena/Lewis and Clark County systems and operations.

The following policy is applicable to all Lewis and Clark County IT&S (IT&S) employees and relevant third party personnel. The scope of this policy covers any IT systems or services that are essential to operations.

2. Types of Disaster

This policy encompasses any type of disaster that could impact system and service availability. The types of disasters that could occur are varied, and each situation or particular disaster could include different variables and impacts. Disasters could include the following:

- Equipment failure
- Power outages
- Fire
- Flood or water leakage
- Severe weather

Disasters could also include those experienced by vendors or critical infrastructure upon which IT&S relies, such as cloud-based applications hosted by third-parties or an internet service provider.

3. Roles and Responsibilities

Roles and Responsibilities	
IT Director	Ensures that the Business Continuity Policy is in alignment with the overall organization's mission and strategy and includes involvement from all areas of the organization.
Security Officer	Oversees the "day-to-day" management of the Business Continuity Policy and is the *lead* for policy implementation. Performs "day-to-day" activities of the Business Continuity Policy including but not limited to: • Participation in the development and update of the Business Continuity Policy (especially as it relates to contact details and associated responsibilities). • Initiating test exercises of the Business Continuity Policy. Completing training on best practices of Business Continuity on a regular basis. Responsible for using individuals' knowledge of their departments to develop and maintain each department's Response and Recovery

	plan using the tools and templates provided by the Program Coordinator (role identified above)

4. Business Continuity Controls

The following sections outline the controls and procedures implemented to mitigate the operational impact of unforeseen disasters or emergencies and facilitate recovery of affected systems and business units.

4.1 Backup Plan

This section provides guidelines to ensure that all sensitive information is being backed up and can be restored.

4.1.1 Backup Requirements

Senior Network Managers are responsible for the overall backup process, including performing, cataloging, inspecting, storing, and securing backups. Senior Network Managers may delegate responsibilities as necessary.

Vendors are also responsible for backups, including processes and procedures to ensure data is secure and available when requested. Vendor backup and availability controls will be evaluated and reviewed by the Security Officer as part of initial due diligence and ongoing vendor management activities (refer to the Vendor Management Policy). Vendor responsibilities, including any unique backup or availability requirements, will be established as part of service-level-agreements and/or contracts with the vendor. This may include specific terms regarding backup and restoration methods, retention periods, safeguards, and more.

Backups will be performed according to a consistent schedule using an approved backup software. Backup software will be configured to provide alerts or reports for both successful and unsuccessful completion of backups. Senior Network Managers will maintain a “Backup Requirements Spreadsheet” containing the different levels of backups associated with the different criticality of systems. Each level of backup will contain the backup methods, technology to be used, retention period, and the frequency of performing the backups (e.g. daily, weekly, monthly). The Backup Requirements Spreadsheet will be maintained as an internal document for reference.

As necessary, all systems must be backed up prior to movement of the system.

Encrypted backup media are picked up weekly and stored in a secure offsite location.
If data backups occur over the Internet to a remote data center, all transmission of data must be encrypted accordance with the Data Integrity and Encryption Policy.

At least once a year, the Security Officer must create a “Backup Report” that details precisely which systems are backed up and the level of backup for each system. This will be used to ensure backup schedules and the scope of included assets are appropriate and that backups are available for each.

4.1.2 Backup Testing

Senior Network Managers are responsible for testing the integrity of backups to ensure they are intact and ready for use when needed. Backup copies and the process of their restoration must be tested at least once every six (6) months by implementing the data restore process and verifying that all data has been successfully recovered. A test log must be maintained by the Security Officer and Senior Network Managers that includes the following information:

- Name of person restoring

- Name of backup being tested
- Results
- Specific issues/problems with restoration
- Date and time of backup

Testing should be done in a testing environment whenever possible.

5. Disaster Recovery Planning

The principal objective of the Disaster Recovery Plan is to develop, test, and document a well-structured and easily understood plan, which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency that interrupts information systems and business operations. Additional objectives include the following:

- Ensuring that all employees fully understand their duties in implementing the plan.
- Ensuring that operational policies are adhered to within all planned activities.
- Ensuring that proposed contingency arrangements are cost-effective.
- Establishing disaster recovery capabilities as applicable to key customers, vendors and other parties.

5.1 Scope of DR Plans and Criticality Analysis

An integral part of DR planning is determining what DR plans should cover. This includes identifying and prioritizing what IT services and supporting functions need to be the focus of DR plans. This process will be informed by performing a criticality analysis of the IT services and supporting functions that are essential to operations.

IT&S will maintain a list of critical systems that will be prioritized for restoration during a disaster or emergency. This list should include details such as system name, type, and function, as well as priority or criticality levels, recovery time objective, supporting vendors, and other details to assist recovery personnel.

The list of Critical Systems includes, but is not limited to, the following:
Core Network Services
Internet Services
AD Services
Duo Services
O365(Email, office products, but mainly email(communications)
Scott's (SSD)Services (Please list the servers needed)
Central Square (AS400)
Phone Systems

Secondary Systems
Proxy Server/Web Server/Services

If for some reason, the Senior Network Manager is unable to perform the responsibilities associated with Disaster Recovery, Senior Network Staff will assume responsibility or designate another individual with the requisite technical skills, as is appropriate.

6. General Response and Recovery Strategy

This section provides general steps for disaster recovery. However, the specific order of operations and individual recovery activities will be determined by the cause and severity of the outage or disaster, and the specific recovery procedures established for each critical system.

Once the IT Security Committee has determined that a declaration of disaster is required, the following procedures will be executed:

- Perform an initial assessment of the damage and potential length of outage. This may include reviewing written or verbal damage assessment reports. The IT Security Committee should assess the condition of equipment and identify equipment that is unusable and must be replaced. Any hardware or equipment should be salvaged for future use if possible.
- Activate or identify alternate sites – employees may be instructed to work from a temporary location until the affected facilities are recovered. Simultaneously, a list of needed equipment/hardware will be created and procurement processes will be initiated.
- A plan and timeline for recovery of systems and services will be developed by the IT Security Committee and distributed to internal and external stakeholders. This will include details related to whether restorations will occur at primary or alternate sites. If services and/or operations will be temporarily restored at an alternate site, plans should include estimated timelines for transferring services back to the primary site.
- The IT Security Officer will contact vendors and other external stakeholders as needed, either by e-mail or phone, to alert them to the disaster/outage and provide an initial timeline of service recovery.
- The plan for recovery will be implemented including:
  - IT Security Committee will begin prioritizing the recovery of information systems according to the criticality of the systems. This includes referencing the list of critical systems (Asset Management Policy) as input.
  - Security Officer will retrieve and distribute the individual recovery procedures for the impacted systems to individuals who will be performing IT recovery tasks.
  - Backups will be retrieved for the systems that have been prioritized for restorations.
  - IT recovery staff will begin set up of new equipment and restoring critical backups.
  - Prior to placing systems into production, IT recovery staff will verify that technical safeguards are functioning adequately. For example, firewalls, intrusion detection/prevention systems, antivirus protections, authentication controls are demonstrated to be working effectively.
- As critical systems are successfully restored, the IT Security Committee should be notified so that they can contact relevant departments and teams. External stakeholders who were previously notified should also be informed of any updates to recovery timelines or that services have been successfully restored.
- If systems are restored to an alternate site, the IT Security Committee will convene to evaluate the operational readiness of the primary site. Once the primary site is verified, the IT Security Committee will work with the Security Officer to finalize plans and timelines for migrating systems and operations back to the primary site.

6.1 Recovery Procedures

The Security Officer is responsible for maintaining detailed disaster recovery procedures for each major system containing sensitive and business critical data. This must be documented in the Systems Recovery Procedures document.

7. Testing and Revision

Testing of the Disaster Recovery Plan will be conducted on an annual basis, in either the form of a “table top” exercise or “fire drill” exercise. The Security Officer is responsible for planning and coordinating tests. Tests will include a “lessons learned” component to identify gaps or areas for improvement that should be incorporated into the plan.

The Security Officer must review and update all recovery plans whenever a new system is added to IT&S’s IT infrastructure, a significant change occurs to facilities, a significant change occurs in threat or business environments, or a significant change occurs in organizational structure.

8. Response to Media

In the case of a disaster or emergency, media outlets may contact IT&S to discuss the incident. The media outlet may ask a series of questions, such as:

- What happened?
- How did it happen?
- What is IT&S going to do about it?

All media response shall be handled by the Communication and Community Outreach Coordinator/City Public Information Officer only. It is the responsibility of all other IT&S’ employees to direct media questions to the them.

9. Notification and Communication

In the event that critical IT&S systems and services are unavailable, relevant parties and stakeholders must be notified and updated throughout recovery efforts. The Security Officer is responsible for compiling and maintaining a list of contact information for vendors, clients, business associates, and other relevant stakeholders. In the case an emergency or disaster, a Disaster Recover Contact List will be used to communicate with various IT&S stakeholders.

A physical copy of the contact list must be stored in a secure, off-site location.

10. Availability and Access to Plans

Any teams and personnel who are involved in recovery processes should be able to access written disaster recovery plans in the midst of a disaster, even if primary systems are unavailable or facilities are inaccessible. Copies of disaster recovery plans and individual system recovery procedures should be stored in more than one location and maintained in both printed and electronic form.

11. Policy Maintenance and Management

The Owner of this document must evaluate and perform any necessary updates to this document annually. The owner may delegate tasks related to this policy as appropriate.

- The Security Officer will adhere to the continual validation, review, and updating of this policy.
- In order to determine the validity of this policy any changes in technology or business processes affecting the scope of this policy must be considered.

- Upon the evaluation of this policy, the Security Officer and IT&S Steering Committee should perform any necessary revisions and proceed to properly communicate policy changes throughout the organization as necessary.

12. References

NIST Cybersecurity Framework References

- ID.BE – Business Environment
- ID.AM- Asset Management
- PR.IP – Information Protection Processes and Procedures
- RS.CO - Communications
- RC.RP – Recovery Planning
- RC.IM – Improvements
- RC.CO - Communications

Policy References

- Information Security Policy
- Physical Security Policy
- Systems Recovery Procedures
- Backup Report