# Important Notes

1. This Disaster Recovery Plan Template is intended for a technical audience. Use of this template should be delegated to your IT support team.
2. This Disaster Recovery Template is intended for technology, systems, or data required to enable critical public services or business functions. Create an instance of this plan for all critical technology resources.
3. Cities may have Business Continuity (or Continuity of Operations) plans that broadly define organizational priorities, critical services, and important business functions. IT Professionals should design Disaster Recovery Plans in context of existing documents and planning.
4. IT systems, solutions, and applications exist in a variety of formats. Consider modifying this template to suit, adding fields where needed, or removing fields that are not applicable.
5. Do you need assistance? League of Minnesota Cities Insurance Trust members can obtain free cybersecurity consultant support for IT security and resilience planning projects.

Table of Contents

[Important Notes 1](#_Toc159275099)

[Plan Purpose 3](#_Toc159275100)

[Scope & Profile 3](#_Toc159275101)

[Recovery Objectives 4](#_Toc159275102)

[Plan Roles & Responsibility 5](#_Toc159275103)

[Technical Documentation 7](#_Toc159275104)

[Backup Strategy 11](#_Toc159275105)

[Recovery Plans 13](#_Toc159275106)

[Document Management 16](#_Toc159275107)

# Plan Purpose

The purpose of this plan is to document system requirements, backup plans, and recovery procedures needed to restore IT systems and data during an outage or disaster event.

# Scope & Profile

**Organization Name:** Insert name of entity **Target System:** Insert IT system or software solution
**System Owner:** Insert the primary staff owner

**System Purpose**

In a few sentences, describe the purpose of this system. Include a high-level overview of how the system functions and what city services might be dependent on this technology.

**Dependent Services & Functions**

Document any city services or business functions that are wholly or partially dependent on this technology resource.

|  |  |  |
| --- | --- | --- |
| **Service Name** | **Level of Dependence** | **Service or Function Owner** |
|  |  |  |
|  |  |  |

 **Calendar Considerations:**

Describe any seasonal patterns, important dates, or cyclical patterns (if any).

# Recovery Objectives

**Recovery Timeframe Objective (RTO)**

If an incident or disaster occurs, what is the tolerable timeframe in which the IT System must be restored?

**Common RTO Values**

[ ]  1 Hour [ ]  1 Week [ ]  1 Month [ ]  1 Day [ ]  2 Weeks

**Custom Timeframe**

|  |  |  |
| --- | --- | --- |
| DaysDays | HoursHours | MinutesMinutes |

**Service Expectations:** RTO may be inherited from recovery and availability expectations defined for city services enabled by this technology system. Lower RTO values might necessitate robust recovery plans and redundant systems. Consult city services inventory or business continuity plans for guidance.

**Recovery Point Objective (RPO)**

Recovery Point Objective defines tolerable data loss and defines a point in time (relative to the incident) that it is acceptable to recover from.

**Common RPO Values**

[ ]  1 Hour [ ]  1 Week [ ]  1 Month [ ]  1 Day [ ]  2 Weeks

**Custom Timeframe**

|  |  |  |
| --- | --- | --- |
| DaysDays | HoursHours | MinutesMinutes |

**Example:** After each backup, any transactions or changes made in the system become susceptible to loss until the next backup occurs. If backups occur every Sunday morning your RPO must be 7 days or greater. If system failure occurs Monday morning, data loss is minimal; but if system failure occurs on Saturday night, an entire week of data could be lost.

**Assessing Value:** Consult with the service owner to determine how much data you can afford to lose, recreate, or reprocess. RPO should consider the value of data, including the volume or rate at which it is generated, and how difficult or costly it would be to replace or recreate.
 **Note:** Lower RPO values will necessitate more frequent backup intervals, which in turn increase storage requirements.

# Plan Roles & Responsibility

**System Architecture & Management Model**

Applications, systems, and solutions can be internally or externally managed. System design and architecture influences the management model and responsibility for disaster recovery planning. The most common models are included below.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [ ]  **(SaaS)**Software-as-a-Service application | [ ]  **(PaaS)**Platform-as-a-Service solution | [ ]  **(IaaS)**Infrastructure-as-a-Service solution | [ ] **(Hybrid)**Internal and external components | [ ]  **(Internal)**Conventional self-managed solution |

**Responsible Parties**

Define which entity is responsible for disaster recovery planning for the system, solution, or application.

[ ]  Vendor responsible[ ]  Shared responsibility [ ]  City responsible

If vendors are wholly or partially responsible, please consider the items below.

 **If Vendor or Shared Responsibility:**

[ ]  Contract exists and legal review has occurred.

[ ]  Service Level Agreements (SLAs) meet RTO/RPO.

[ ]  Vendor support and escalation process is defined.

[ ]  Vendor defines process to communicate maintenance, outages, and incidents.

**Note:** If vendor is wholly responsible for all aspects of disaster recovery planning, then the remainder of this template may be left blank.

**Shared Responsibility Matrix:** Not all vendor or cloud contract agreements guarantee configurations, settings, or data elements are retained in the event of a disaster. In addition, some cloud applications may depend on integration with other city managed systems. Consult your contract and ask your vendor for a “shared responsibility matrix” to determine what the vendor is and is not responsible for. Include any city responsibilities in this document.

**Plan Authority and System Owners**

Define individuals who own the management of this system and those authorized to order the execution of this plan (and under what circumstances):

| **Name, Title** | **Scenario**  |
| --- | --- |
|  |  |
|  |  |

**Responsible Personnel for Technical Operations**

List primary internal (or contract) staff responsible for the IT system in regular production and technical staff needed to recover during a disaster event.

| **Name, Title** | **Contact Information** | **Role Notes** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

**Third-Party Vendors**

What third-party vendor relationships support this system and how can the vendors be reached?

| **Entity/Name** | **Support Contact Information** | **Notes** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# Technical Documentation

**System Diagrams**

Define the storage location for relevant architecture diagrams for this system. Consider physical, logical, and data flow diagrams.

**Hardware Systems**

List fixed physical assets (computer or servers) that are part for this system.

| **Asset Host Name** | **IP** | **VLAN** | **Location** | **Notes** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

**Virtual Systems**

List persistent virtualized assets, that are part for this system.

| **Asset Host Name** | **IP** | **VLAN** | **Location** | **Notes** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

**Temporary Assets:** Virtualized or cloud assets may exist dynamically or programmatically. In these circumstances it makes sense to document the infrastructure-as-code, orchestration, and configuration logic that generate temporary or ephemeral assets, instead of the assets themselves. See below.

**Infrastructure-as-Code, Orchestration, and Configuration Management**

Identify relevant templates that are used to support the operation and deployment of this system and underlying dependencies.

| **Plan/Recipe/Playbook/Template** | **Platform** | **Owner/Author** | **Notes** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

**Automation Templates:** Automated orchestration can be a key strategy for disaster recovery, enabling quick provision of systems and shortened recovery timeframes. Cities leveraging virtualized or cloud environments are well positioned to take advantage of these strategies.

**Required Network Services**

What network services does this system depend on?

| **Network Service** | **Description**  |
| --- | --- |
|  |  |
|  |  |

**Examples:** Common examples might include internal or external network services such as Active Directory, DNS, DHCP, etc.

**Network Traffic Information**

Identify critical network communication ports and protocols used by asset and patron systems.

| **Port** | **Protocol** |  **Source** | **Destination** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

**Network Layer Configurations:** Consider backing up local or network firewall configurations, switch configurations, and other systems that process traffic between source and destination systems.

**Required Software**

What software is required to support this system?

| **Software Name** | **Manufacturer/Developer** | **Version** | **License Keys** | **Notes** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |

**Other Notes**

Include any other relevant information here (i.e., known issues, single points of failure, common mistakes operating this system, etc.)

**Other Documentation**

Define storage location for relevant contracts, procedures, manuals, documentation, or schematics.

**Master Accounts, Passwords, and Keys**

Document service accounts and other master (break-glass-in-case-of-emergency) accounts used to manage this solution.

| **Username** | **Account Type** | **System** | **Where to find password or key?** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

**Sensitive Information:** It is not recommended to store passwords or keys directly in this document. If doing so, take precaution to securely store and restrict access to this file. Consider using a dedicated password manager or key vault. Paper copies should be locked in secure storage and stored in geographic redundant locations.

# Backup Strategy

**Backup Storage Locations**

Backup strategies protect data and facilitate recovery efforts. Backup plans must meet expectations for acceptable data loss (RPO) and should occur within desired recovery timeframes (RTO).

| **Solution, System, or Data** | **Production Storage System** | **Primary Backup Location** | **Offsite Backup Location** | **Type/Frequency/Retention Period** |
| --- | --- | --- | --- | --- |
|  |  |  |  | [ ]  Full [ ]  Incremental[ ]  DifferentialFrequency:       Retention Timeframe:       |
|  |  |  |  | [ ]  Full [ ]  Incremental[ ]  DifferentialFrequency:       Retention Timeframe:       |

**Consider implementing a 3-2-1 backup strategy:**

* 3 copies, including live production copy of solution, system, or data.
(Protecting against failure or compromise of any given software or system.)
* 2 copies on different physical systems or storage mediums.
(Protecting against failure of any given hardware.)
* 1 copy existing offsite.
(Protecting against disaster at any given physical location.)

**Ransomware Protection:** Backups can be made unusable if malicious actors can tamper with backup files or backup systems directly. Pay special attention to the security and permission configurations to avoid exposing the system or backup files to the network or internet.

Ransomware can leverage the normal function of your backup system, which is often configured to backup changes to files. If not detected in time, your backup system could overwrite clean files with maliciously modified versions. This is where retention timeframes and file immutability become important. Backup solutions that offer Write-Once Read-Many (WORM) functionalities keep multiple versions of your files intact and reduce the likelihood that ransomed files and encrypted backups will propagate and overwrite clean copies of your data.

**Backup Restore Procedure**

In a disaster event, please detail the recovery procedure to restore the system to normal operation from backups.

| Step | Details |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Backup Testing**

[ ]  Test Meets RTO [ ]  Test Meets RPO [ ]  Restored Systems & Data are Validated

**Test Date:** Date of test.
**Attestation:** Name of person who conducted test

**Importance of Testing:** The most common pitfall organizations make when relying on backups is not testing and documenting the restore procedure. Backups are easy to create, but often difficult to restore. Recovery can be a fickle process and fail for a multitude of reasons. Therefore, it is highly recommended to test your restore process to confirm backup plans work as intended.

# Recovery Plans

**Offsite Operations**

If primary sites are unavailable, where can recovery systems operate from?

[ ]  Hot-Site Facility Name:       Facility Address:

[ ]  Warm Site Facility Name:       Facility Address:

[ ]  Cold Site Facility Name:       Facility Address:

**Alternative Sites:** Consider collaborating with nearby cities or other public entities to obtain formal agreements to host technology systems in the event of a disaster. Private data center space can also serve municipal needs, especially if one or more cities participate in an agreement for shared space. Cloud providers can also host technology in geographic redundant locations.

**Hot Sites:** Hot sites are fully functional IT networks that are pre-installed and ready for fail-over at a moment’s notice. Hot sites have all hardware, software, and data replicated in a ready to run state. Hot sites might be configured to automatically takeover without any human interaction if load balancing and high availability strategies are implemented. At worst, hot sites should become operational with minimal configuration. Hot sites are costly because they require double the equipment, software licenses, and technical support time, not to mention space and utility costs.

Hot sites could be a consideration for:

* Very large cities with large IT budgets and high workload demand that make multiple sites feasible or necessary.
* Mission critical workloads that council determines cannot have any downtime.
* Cities who are already operating technology systems in a cloud environment.
* Cities with an extremely limited amount of technical hardware where:
- City can or already does budget to purchase spare equipment.
- Equipment can easily fit at another location or city.
- Network bandwidth at alterative site can handle additional traffic load.

**Warm Sites:** Warm sites have all the needed hardware equipment pre-installed but differ from hot sites in that they do not have all data replicated. Systems are typically powered down and will require data restoration and some software configuration before they can be functional. Warm sites have networking, internet, and utility services pre-installed.

Cloud hosting providers such as Microsoft Azure, Amazon Web Services, and Google Cloud (among others) might be cost-effective methods of preparing a warm site without significant investment in hardware or software. Virtual systems can be preconfigured and then spun down to minimize spend rates. Costs to maintain system images in storage pales in comparison to keeping compute instances operational 24/7.

**Cold Sites:** Cold sites are defined spaces where IT equipment can be installed if needed. Typically, cold sites have internet and utility service preconfigured, but no hardware equipment or software is pre-installed. Cold sites take more staff support and time to get operational but have the lowest ongoing costs to operate.

If cities have any level of dependency on self-hosted IT systems, they should consider arrangements for a cold site as minimum level of preparation. Cold sites can be as simple as obtaining a memorandum of understanding (MOU) with nearby cities to host each other’s computer systems in the event of a disaster.

**Hardware Replacement**

Identify hardware requirements and replacement plans for physical systems.

| **Hardware System** | **Hardware Specs** | **Replacement Plan and Timeframe** |
| --- | --- | --- |
|  |  | Hardware Acquired: [ ]  Yes [ ]  No.Supplier:      Estimated Acquisition Time:       |
|  |  | Hardware Acquired: [ ]  Yes [ ]  No.Supplier:      Estimated Acquisition Time:       |

**Supply Chain:** Supply chain timelines should be considered when developing disaster recovery plans. Consider if hardware acquisition timelines for mission critical systems can meet the expected RTO. If not, consider negotiating arrangements for leased hardware, or purchasing spare systems or cloud hosting.

**Rebuild Procedure**

If backups of whole systems are not available, please detail the recovery procedure to rebuild the system from scratch.

| Step | Details |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Document Management

**Plan Approvals**

**Plan Author:** Insert name of author
**Plan Approver:** Insert name of approver
**Approval Date:** Insert date
**Next Review:** Insert date of next review

**Plan Storage Locations**

**Primary Disaster Recovery Plan Storage Location:** Insert file storage location:
**Offsite Disaster Recovery Plan Storage Location:** Offsite storage location

**Plan Accessibility:** Control for physical and digital disaster by keeping both physical and digital copies of the plan in multiple locations.

**Plan Security:** Disaster recovery plans contain sensitive data that might enable a malicious threat actor to disrupt recovery in a disaster scenario. Please consider how you might approach restricting access to these documents.

**Document History**

| **Version** | **Change Summary** | **Contributors** |
| --- | --- | --- |
| 1.00 | Document Template Created | League of Minnesota Cities |
|  |  |  |
|  |  |  |