ENTERPRISE SECURITY MANAGEMENT PLAN

ACME CORP

Gabrielle Decker

OKLAHOMA CITY COMMUNITY COLLEGE | CS-2743-MW01F

Table of Contents

1 Introduction

1.1 Purpose

The purpose of the Enterprise Security Management Plan (ESMP) is to provide ACME Corp with a comprehensive security framework that will ensure the protection of all information assets from unauthorized access, modification, or destruction. The ESMP will include an Incident Response Plan (IRP), Disaster Recovery Plan (DRP), and Business Continuity Plan (ESMP). The ESMP will also provide guidance on how to protect the confidentiality, integrity, and availability of all information assets, as well as how to respond to security incidents, how to recover from disasters, and how to maintain business continuity.

1.2 Scope

The ESMP applies to ACME Corp, a federal contractor that manages information assets for agencies in the U.S. and EU. This ESMP covers all of ACME Corp's operations, systems, equipment, personnel, and locations. The ESMP covers the following systems and equipment:

- Windows 3.1 through Current
- Windows Server 2000 through Current using Active Directory Domain Services for security domain management such as user management, etc.
- Microsoft Azure for managing the storing, and access of data
- Linux kernel 2.6 through Current running in Red Hat Enterprise Linux (Server Edition being used as Firewalls and Application Layer Proxies)
- Smartphones using the Android Platform
- Cisco Routers and Switches using Cisco’s IOS Platform

This ESMP will cover the following personnel:

- CEO
- CIO/CISO
- Security Managers
- Security Technicians
- IT Managers
- IT Technicians
- System Administrators
- Network Administrators

This ESMP will cover all of ACME Corp’s locations, including all its offices, data centers, and other facilities.

1.3 Applicable Laws and Regulations

The following laws and regulations are applicable to incident planning:

- Federal Information Security Management Act (FISMA) of 2002 [Title III, PL 107-347]
- Management of Federal Information Resources [OMB Circular A-130]
- Records Management by Federal Agencies [44 USC 31]
- Safeguarding Against and Responding to the Breach of Personally Identifiable Information [OMB Memo M-07-16]

2 Incident Response

2.1 Purpose

The purpose of this document is to define processes and procedures in the event of a cyber-incident occurring on any of the systems maintained by ACME Corp for multiple agencies in the U.S. and in the European Union. This Incident Response Plan (IRP) is an actionable strategy that outlines the life cycle of handling cybersecurity incidents in four phases:

- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity

2.2 Types Of Incidents

> Example scenarios and their attack profiles can be found in Appendix 5.3 Incident Scenarios.

ATTACK VECTOR	DESCRIPTION	EXAMPLE
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The attack vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.
Web	An attack executed from a website or web-based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Email/Phishing	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected flash drive.
Impersonation/Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute	Spoofing, man in the middle attacks, rogue wireless access points, and

		structured query language injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack method does not fit into any other vector	Miscellaneous

Table 1 Attack Vectors for US-CERT Reporting

2.3 Incident Response Team Structure

> A table and contact list with the current personnel is in Appendix 5.1 Key Personnel and Team Members.

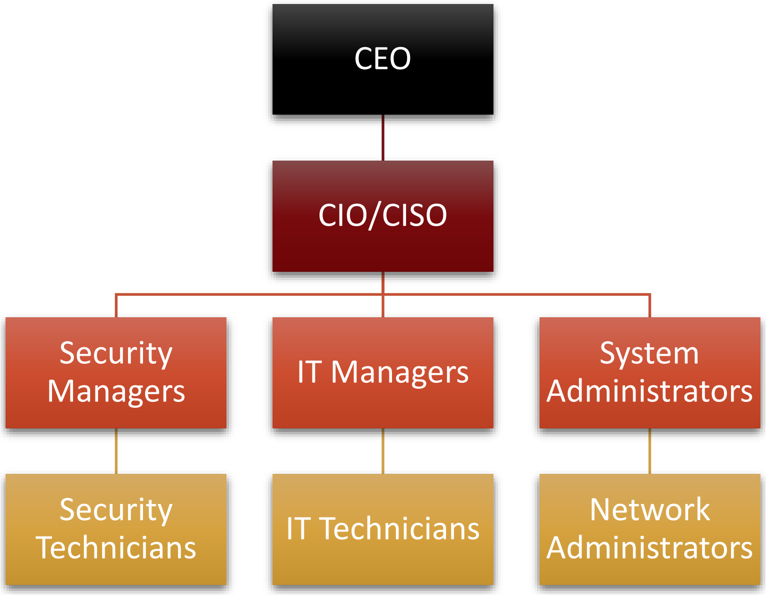

Figure 1 ACME Corp Incident Response Team Structure

2.4 Roles And Responsibilities

ACME Corp will establish multiple roles and duties for responding to interruptions, outages, and disasters. The Incident Response Team (IRT) is comprised of individuals who are assigned positions for recovery operations and who receive annual training for their responsibilities. IRT members are selected based on their abilities and expertise.

ROLE	RESPONSIBILITIES
Incident Commander	Advise on immediate mitigation actions Develop & maintain IRP Coordinate & exercise IRP Update IRP based on lessons learned

	Identify/implement hardware/software roles to facilitate security management
IRT Members	Verify & identify cyber incidents/events Develop & approve triage & incident management mitigation strategies Assess operational impacts of incidents Provide SME guidance & recommendations Record & maintain security incident records
Help Desk	Receive reports of security events/incidents Report to Incident commander Record in log file
Information System Security Manager (CIO/CISO)	Oversee all aspects of information security. Ensure incident response policy complies with organizational policies, standards, and procedures.
System Administrators	Coordinate & cooperate with IRT on mitigation actions Develop security policies & procedures Implement security controls
Users	Report suspicious activity to Help Desk/security officer Provide input to Incident/Event Report Log Perform mitigation actions Take only actions directed by Help Desk/CIO/CISO Coordinate & cooperate with Help Desk/CIO/CISO

Table 2 Incident Response Roles and Responsibilities

2.5 Incident Response Framework

2.5.1 Incident Response Process

Maximizing the effectiveness of the IRP can be established and characterized through four phases defined in *NIST SP 800-61 (Computer Security Incident Handling Guide)*:

Preparation: ACME Corp will create and implement a comprehensive incident response plan that outlines the roles, technologies, and procedures used to detect and respond to security incidents.

Detection and Analysis: ACME Corp will use a combination of technologies, such as IDS, IPS, SIEM, and host-based security solutions, to detect and analyze malicious activity and suspicious behavior on their systems and networks.

Containment, Eradication, and Recovery: ACME Corp will assess the risks associated with a security incident to determine its severity and impact, take remediation actions such as disabling user accounts, applying patches, and deploying additional security solutions, and take recovery steps such as restoring data, reimaging systems, and deploying additional security solutions.

Post-Incident Activity: ACME Corp will report the security incident to affected customers, federal agencies, and other relevant stakeholders within 72 hours of the incident. In addition, ACME Corp will perform an After-Action Review to assess the effectiveness of their incident response process.

2.5.2 Preparation

> A quick action checklist for the Preparation phase can be found in Appendix 5.2 Incident Response Process Checklists

ACME Corp is taking steps to protect their system from security incidents by establishing an IRT and adhering to all applicable laws and regulations. The team will have the necessary resources and tools to respond to any security incidents that may occur. ACME Corp should also reduce incidents through appropriate security functions, risk management, training, and continuous monitoring. Periodic vulnerability assessments should be conducted to identify security weaknesses and prioritized based on the severity of the findings. Additionally, ACME Corp should consider deploying additional hardware and roles for system components, as well as other location necessities, to facilitate security management. Lastly, keeping end users informed of current and future threats can help improve the response time and remediation of a presented threat.

2.5.2.1 Incident Response Personnel Training

ACME Corp is providing training for all employees related to cybersecurity incident response and is also providing continuous learning programs to ensure its IRT is up to date on the latest attack vectors and incident handling processes. The CIO/CISO will oversee the training standards and review the incident response plan, while also taking part in an annual security incident response exercise involving scenario-based tabletop exercises.

ACME Corp evaluates the efficiency of their incident response process every year through a security incident response exercise. The CIO/CISO is responsible for reviewing the results and the exercise should include testing the organization's ability to respond to various security incidents, such as malware and malicious insiders, using the tools and technologies introduced by ACME Corp. Any shortcomings found during the exercise are documented and assigned to the correct stakeholders in SharePoint entries.

2.5.3 Detection And Analysis

2.5.3.1 Detection

> A quick action checklist for the Preparation phase can be found in Appendix 5.2 Incident Response Process Checklists
>
> The Incident Response Form can be found in Appendix 5.4 Incident Response Form.

ACME Corp's incident detection and analysis phase starts when an incident is reported and ends when the Incident commander creates an incident record. It is monitored 24/7/365 in response to automated system alerts, customer reports, and administrator incident reports, and employees are encouraged to report any potential security events.

ACME Corp has implemented Microsoft Azure Sentinel to monitor their security environment and quickly detect and respond to security incidents. This system collects and analyzes data from all systems and devices, as well as provides additional hardware and roles to ensure proper security management.

2.5.3.1.1 Incident Reporting

> A quick action checklist for Reporting can be found in Appendix 5.2 Incident Response Process Checklists

ACME Corp must report any security incidents involving Government information or systems to customer agencies within 60 minutes and notify any affected customers immediately if sensitive information has been or will be misused. Personally identifiable information (PII) must **not** be added to incident submissions.

2.5.3.2 Analysis

> A quick action checklist for the Preparation phase can be found in Appendix 5.2 Incident Response Process Checklists

IRT will use incident analysis to troubleshoot, document, and identify the root cause of an incident. They will analyze:

- The impact of the incident on the organization
- The potential risk
- The affected systems, applications, data, and users

Security events will be classified and escalated to the CEO, CIO/CISO, and Security Managers.

For federal customers, the IRT will alert the appropriate personnel within each affected agency and notify them of the incident and the actions taken.

System Administrators, Network Administrators, IT Managers, and IT Technicians will provide technical expertise and troubleshooting support to the IRT.

2.5.3.2.1 Severity Rating

ACME Corp management uses security incident classification to determine the severity and criticality of a security incident. Incidents are categorized into four severity levels based on the impact to ACME Corp and can be expressed in terms of financial impact, impact to services and/or performance of mission functions, image, or trust by customers and citizens. These severity levels and their definitions are listed in the table below.

SEVERITY LEVEL	DESCRIPTION
0 (Low)	Incident where the impact is minimal. Examples may be e-mail SPAM, isolated virus infections, etc.
1 (Medium)	Incident where the impact is significant. Examples may be a delayed or limited ability to provide services, meet ACME Corp's mission, delayed delivery of critical electronic mail or data transfers, etc.
2 (High)	Incident where the impact is severe. Examples may be a disruption to the services and/or performance of mission functions. ACME Corp's proprietary or confidential information has been compromised, a virus or worm has become widespread and is affecting over 1 percent of employees, Public Safety systems are unavailable, or ACME Corp's Executive management has been notified.

3 (Extreme)	Incident where the impact is catastrophic. Examples may be a shutdown of all ACME Corp's network services. ACME Corp's proprietary or confidential information has been compromised and published in/on a public venue or site. Public safety systems are unavailable. Executive management must make a public statement.

Table 3 Incident Severity Rating

If there is a potential data breach, the CIO/CISO must declare the incident and the IRT will take steps to contain the incident and investigate its extent. They will also notify the appropriate personnel and agencies of the incident, including the actions taken to mitigate and remediate it.

2.5.4 Containment, Eradication, And Recovery

2.5.4.1 Containment

> A quick action checklist for the Preparation phase can be found in Appendix 5.2 Incident Response Process Checklists

ACME Corp must take appropriate action to limit the damage of a security incident. The Incident Commander should be consulted for assistance in determining the best strategy. This can include shutting down the affected system, disconnecting it from the network, or leaving it powered on and running. If the incident is deemed severe and a wide-scale attack is suspected, ACME Corp may consider additional hardware and/or roles for system components.

2.5.4.2 Eradication

> A quick action checklist for the Preparation phase can be found in Appendix 5.2 Incident Response Process Checklists

The primary objective in executing the eradication activities is to remove the security exploit and restore the affected systems to their normal operating condition.

Service Team

The Service Team will identify and present long-term fixes to the Incident Commander to prevent further incidents. Repairs involving code and configuration changes should be tracked in the SCOM Incident Tracking Entry; automated methods to validate the repair should be implemented when possible and documented in the SCOM Incident Tracking Entry.

Incident Commander

The Incident Commander will coordinate the decision-making process for implementation and validation strategies.

2.5.4.3 Recovery

> A quick action checklist for the Preparation phase can be found in Appendix 5.2 Incident Response Process Checklists

Once the affected device has been quarantined and the threat has been eradicated, the next step is to restore it to operational status. If the security incident has affected the system or data, a complete restoration from backups will be required after determining the integrity of the backup itself. Once the restore procedures have been performed, ACME Corp should verify that the restoration was successful, and that the system is back to its normal condition.

Service Team

The Service Team should verify service restoration through monitoring, partners, and customers and validate that the system is back to its normal condition.

Help Desk

The Help Desk should validate service restoration. ACME Corp requires that an incident be fully investigated and documented, the affected systems must be returned to a secure state, the Incident commander and CISO must approve the incident closure, and the incident report must be reviewed and approved before the incident can be closed.

2.5.5 Post-Incident Activity

> A quick action checklist for the Preparation phase can be found in Appendix 5.2 Incident Response Process Checklists

The Post-Incident Activity phase of IR for ACME Corp will involve a review and analysis of the activities that occurred leading up to and during the security incident, and the actions taken by those involved in the incident, including the incident response team. This includes a reflection on what happened and at what times, how well staff and management performed in dealing with the incident, what information was needed sooner, and what corrective actions can prevent similar actions in the future. The review will reflect on:

- Any precursors or indicators that should be watched for in the future
- What additional tools or resources are needed
- What new security measures should be implemented
- What additional personnel and/or roles should be considered

A report must be produced within 14 days of completion of the investigation for any customer impacting incidents, which must include:

- Customer/business impact
- Incident severity
- Root cause description
- Repair items
- Timeline
- External public statement (if necessary)
- Security measures taken for multi-platform systems
- Additional hardware and/or roles for system components
- Processes implemented to prevent a similar incident

2.6 Escalation

> A quick action checklist for the Preparation phase can be found in Appendix 5.2 Incident Response Process Checklists

The escalation process will be initiated to involve other appropriate resources as the incident increases in scope and impact. Incidents should be handled at the lowest escalation level that can respond to the incident with as few resources as possible to reduce the total impact and maintain limits on cyber-incident knowledge.

The IRT will consider several characteristics of the incident before escalating the response to a higher level, such as:

- How widespread it is
- What the impact is
- How difficult it is to contain
- The financial and image impact
- The rate of propagation

3 Disaster Recovery

3.1 Purpose

This Disaster Recovery Plan (DRP) outlines procedures for ACME Corp to quickly and effectively recover from any service disruptions that may occur. It is critical for these systems to be in place to ensure ACME Corp's services remain operational and effective.

This DRP outlines procedures for recovering ACME Corp following a disruption, including activating and notifying personnel, restoring operations, validating normal operations, and assigning specific responsibilities to personnel. Necessary equipment and staff are identified, as well as coordination with external points of contact and vendors.

3.2 Assumptions

When constructing this DRP, the following presumptions were made:

- For this system, additional processing facilities and offsite storage have been developed.
- At the off-site storage facility in Washington, D.C., there are current backups of the system software and data that are both intact and accessible.
- If ACME Corp. needs to relocate, alternative facilities have been constructed and are available.
- The ACME Corp’s system is down and cannot be repaired in time for the next four hours.
- The equipment and staff indicated in the scenario are available and prepared to be employed. Key ACME Corp workers have been identified and trained in their emergency response and recovery duties; they are available to activate the ACME Corp Contingency Plan.

- The Disaster Recovery Response Plan must be carried out in line with the "Contingency Planning Guide for Federal Information Systems" included in NIST Special Publication 800-34 Rev. 1.

3.3 Roles And Responsibilities

Teams or individuals allocated DRP roles have received training on how to react in case ACME Corp. is affected by a contingency event.

- The **DRP Coordinator** oversees monitoring the recovery and reconstitution process, starting any necessary escalations or awareness communications, and, as necessary, establishing coordination with other recovery and reconstitution teams. The DRP Director oversees overall plan management.
- The **System Owner or Business Unit Point of Contact** oversees supplying the recovery team with information and direction unique to the system and making sure that system recovery and reconstitution are in line with the organization's business goals and objectives.
- The **Recovery Coordinator** oversees organizing the system's recovery, which includes planning recovery activities, monitoring recovery progress, and making sure the recovery is carried out in line with the DRP.
- The technical components of recovery, such as installing, configuring, and testing system hardware and software as well as data restoration, are handled by the **Technical Recovery Point of Contact**.
- The **Security Managers** oversee creating and putting into place security measures to safeguard the system from unwanted access, as well as making sure the system is configured and managed in compliance with security policies and procedures.
- The management of the system, including the installation and configuration of hardware and software, the upkeep of system documentation, and the administration of system resources, is the responsibility of the **IT managers**.
- The day-to-day operations of the system, including the installation and configuration of hardware and software, the upkeep of system documentation, and the administration of system resources, are the responsibility of the **IT technicians**.
- • The installation, setup, upkeep, and data restoration of the system's hardware and software are under the purview of the **system administrators**.
- The **Network Administrators** are in charge of installing, configuring, and maintaining the network infrastructure, which includes routers, switches, and firewalls.
- The **Security Technicians** are in charge of implementing and maintaining security controls like user authentication, access control, and encryption.

3.4 Activation And Notification

When a system disruption is identified or seems imminent, the Activation and Notification Phase describes the initial steps that are conducted. This stage involves contacting the recovery team, evaluating the outage, and activating the DRP. The DRP team at ACME Corp will be ready to carry out recovery actions once the Activation and Notification Phase is over.

3.4.1 Activation Criteria and Procedure

If one or more of the following conditions are satisfied, the ACME Corp DRP may be activated:

1. Given the sort of outage, ACME Corp.'s systems are likely to be unavailable for longer than the Recovery Time Objective (RTO) hours
2. The facility housing those systems is damaged, so it's possible that it won't be ready in time for the RTO hours

The following persons or roles may activate the DRP if one or more of these criteria are met:

1. CEO
2. CIO/CISO
3. Security Managers

3.4.2 Notification

When the ACME Corp DRP is activated, the first action is to notify the appropriate business and system support staff. Appendix 5.5 Personnel Contact List contains contact details for the relevant POCs.

To guarantee that every employee is informed of a disaster recovery event, notification protocols should be implemented. The system owner should be notified first, followed by the technical point of contact (POC), the DRP coordinator, the POC for the business unit or user unit, and the POC for the recovery team. A call list, automated notification system, or email blast should be used for notification. The notifications should be sent out in the following order:

1. **System Owner**: The system owner should be the first to be notified of a disaster recovery event.
2. **Technical POC**: The technical POC should be notified next and should be responsible for coordinating the technical response to the event.
3. **DRP Coordinator**: The DRP Coordinator should be notified next and should be responsible for coordinating the overall response to the event.
4. **Business Unit/User Unit POC**: The business unit or user unit POC should be notified next and should be responsible for coordinating the response from the business or user unit.
5. **Recovery Team POC**: The recovery team POC should be notified last and should be responsible for coordinating the recovery efforts.

3.4.3 Outage Assessment

After notification, a complete outage assessment is required to ascertain the degree of the disruption, the amount of any damage, and the anticipated time of recovery. The ACME Corp Recovery Team is responsible for conducting this outage evaluation. The DRP Coordinator receives assessment data to help with planning the restoration of ACME Corp systems.

Systems will be evaluated by the ACME Corp Recovery Team. The Recovery Team will also determine whether any additional hardware and/or system roles are required to support security management or other location requirements.

1. **Determine the Cause of the Outage:**
    a. Identify the source of the disruption or damage

   b. Analyze the impact of the disruption or damage
   c. Identify the root cause of the disruption or damage
   d. Identify the scope of the disruption or damage

2. **Identify Potential for Additional Disruption or Damage:**
   a. Identify any additional risks or threats
   b. Identify any additional areas of impact
   c. Assess the potential for further disruption or damage
3. **Assess Affected Physical Area(s):**
   a. Identify the affected physical area(s)
   b. Assess the extent of the disruption or damage
   c. Identify any additional risks or threats
   d. Identify any additional areas of impact
4. **Determine Physical Infrastructure Status:**
   a. Identify the physical infrastructure components
   b. Analyze the status of the physical infrastructure components
   c. Identify any additional risks or threats
   d. Identify any additional areas of impact
5. **Determine IS Equipment Functionality:**
   a. Identify the IS equipment components
   b. Analyze the status of the IS equipment components
   c. Identify any additional risks or threats
   d. Identify any additional areas of impact
6. **Determine Inventory:**
   a. Identify the inventory components
   b. Analyze the status of the inventory components
   c. Identify any additional risks or threats
   d. Identify any additional areas of impact
7. **Replace Items and Estimate Time to Restore Service:**
   a. Identify the items that need to be replaced
   b. Estimate the time to replace the items
   c. Estimate the time to restore service to normal operations
   d. Identify any additional risks or threats
   e. Identify any additional areas of impact

3.5 Recovery

After the DRP has been activated, outage assessments have been finished (if possible), workers have been contacted, and the relevant teams have been recruited, the Recovery Phase offers official recovery activities. Activities during the recovery phase are concentrated on putting recovery plans into action to repair damage, restore system functionality, and restart operational capabilities at the original or a different site. The systems of ACME Corp. will be operational and able to carry out tasks.

3.5.1 Sequence Of Recovery Activities

During the recovery of ACME Corp's systems, the following operations take place:

1. Locate the recovery site (if not at original location)
2. Determine the resources needed to carry out recovery processes.
3. Obtain backup and installation media
4. Restore hardware and the operating system (if required)
5. Recover the system from backup and installation media
6. Restore personnel authentication and access
7. Retrieve lost data and apps
8. Check the system's operation.
9. The document recovery procedure
10. Inform personnel of the successful recovery.

3.5.2 Recovery Procedures

The processes listed below are for restoring ACME Corp's systems in the original or established alternate site. Recovery methods are specified for each team and should be followed in the order offered to ensure an efficient recovery effort.

- The CIO/CISO will oversee determining the degree of the disaster and the breadth of system recovery.
- The Security Managers will oversee assessing the disaster's security threats and establishing a plan to minimize such threats.
- The IT Managers will oversee determining the hardware and software required to restore the system.
- System Administrators will oversee restoring the system from backup media.
- Network Administrators will oversee setting the network to enable secure system access.
- Security Technicians will oversee monitoring the system for security concerns.
- IT Technicians will oversee testing the system to verify its effective operation.
- The CEO will oversee restoring the system to its pre-disaster state.

The following steps will be taken during the recovery process:

1. Determine the reason of the system failure and the procedures required to resolve the problem.
2. Make a backup of the system data and configuration information to guarantee that no information is lost during the recovery procedure.
3. Restore the system to its original state by installing the appropriate hardware and software components.
4. Configure the system and network components to ensure correct operation.
5. Test the system to confirm that it is secure and functional.
6. Inform users about the condition of the system and provide information on how to access it.

3.5.3 Recovery Escalation Notices/Awareness

1. **Problem Escalation:**

   a. When a problem is identified, the IT Technician will immediately notify the IT Manager.
   b. The IT Manager will then notify the CIO/CISO and Security Managers.
   c. The CIO/CISO and Security Managers will assess the situation and determine the appropriate response.
   d. The CIO/CISO will then notify the CEO of the issue and the proposed response.
2. **Status Awareness:**
   a. The IT Manager will be responsible for providing status updates to the system owners and users.
   b. The Security Managers will be responsible for providing status updates to the CIO/CISO and CEO.
   c. The CIO/CISO will be responsible for providing status updates to the CEO.

3.6 Reconstitution

Reconstitution is the process of completing recovery actions and restoring regular system functionality. ACME Corp will install, maintain, and safeguard all information assets for several agencies in the United States and the European Union. The system will be evaluated to see if there has been significant change that necessitates reconsideration and reauthorization. The phase is divided into two parts: confirming successful reconstitution and deactivating the plan.

3.6.1 Validation Data Testing

Validation data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely. The following procedures will be used to determine that the recovered data is complete and current to the last available backup:

1. **Data Integrity Testing**: Data Integrity Testing is conducted to ensure that the data has been properly restored and is not corrupted or incomplete. Data integrity tests may include checksum, data comparison, and data verification.
2. **Data Verification**: Data Verification is conducted to ensure that the data is accurate, up-to-date, and matches what is expected. Data verification tests may include comparison of known data with the recovered data, or manual review of the recovered data.
3. **Functionality Testing**: Functionality Testing is conducted to ensure that the data can be used in the manner expected. Functionality tests may include tests of the user interface or web services, or automated testing of data processing.
4. **Security Testing**: Security Testing is conducted to ensure that the data is secure and has not been compromised. Security tests may include penetration testing, vulnerability scanning, and security audits.

The teams responsible for each procedure should include:

1. **Data Integrity Testing**: The IT technicians and system administrators should be responsible for conducting data integrity tests.
2. **Data Verification**: The IT Managers and Security Managers should be responsible for conducting data verification tests.

3. **Functionality Testing**: The IT technicians, system administrators, and IT managers should be responsible for conducting functionality tests.
4. **Security Testing**: The Security Managers and Security Technicians should be responsible for conducting security tests.

The recovery process should be tested and validated multiple times to ensure the data is accurate and up to date. The results of the tests should be documented and reported to the CEO and CIO/CISO.

3.6.2 Validation Functionality Testing

Validation functionality testing is the process of verifying that ACME Corp's systems functionality has been tested, and the system is ready to return to normal operations.

1. **Verify application availability**: Check whether the application is available to users. This can be done by checking logs, monitoring response time, and other appropriate tests.
2. **Verify access control**: Test whether the access control system is configured correctly. This can be done by logging in with different user accounts and ensuring that access is being granted and denied as expected.
3. **Verify data integrity**: Run checksums or other appropriate tests to ensure that the data stored in the system is not modified or corrupted.
4. **Verify performance**: Measure the performance of the system under various scenarios. This can be done by running automated scripts to perform tasks and measuring the response time.
5. **Verify security features**: Test the security features of the system such as encryption, authentication, authorization, and audit trails.
6. **Verify user acceptance**: Test the system with actual users to ensure that the system meets their needs and expectations.
7. **Verify system backups**: Verify that backups of the system are being performed as expected and that they are restorable.
8. **Verify system maintenance**: Test that the system is being maintained and updated as expected.
9. **Verify system monitoring**: Verify that the system is being monitored as expected and that any alerts are being responded to in a timely manner.

Responsible Teams/Persons

1. **Application Availability**: IT Manager and IT Technician
2. **Access Control**: Security Manager and Security Technician
3. **Data Integrity**: IT Manager and IT Technician
4. **Performance**: System Administrator and Network Administrator
5. **Security Features**: Security Manager and Security Technician
6. **User Acceptance**: IT Manager and IT Technician
7. **System Backups**: System Administrator and Network Administrator
8. **System Maintenance**: IT Manager and IT Technician
9. **System Monitoring**: System Administrator and Network Administrator

3.6.3 Recovery Declaration

Upon successfully completing testing and validation, the CIO/CISO will formally declare recovery efforts complete, and that ACME Corp's systems are in normal operations. ACME Corp's business and technical point of contacts (POCs) will be notified of the declaration by the Disaster Recovery Plan (DRP) Coordinator.

3.6.4 Notifications (Users)

Users of ACME Corp will be informed by the System Administrator once normal system functions have resumed using preset notification protocols (e.g., email, broadcast message, phone calls, etc.).

3.6.5 Cleanup

Cleaning up or dismantling any temporary recovery sites, stocking up on supplies that were used, returning manuals or other paperwork to its original locations, and getting the system ready for a potential future contingency event are all parts of cleanup.

All installation or backup media will be put back in its proper place, and all manuals and papers will be put back where they belong, according to ACME Corp. All temporary recovery sites will also be demolished, and all utilized materials will be replenished.

3.6.6 Offsite Data Storage

It is crucial that all installation and backup media used during recovery be delivered back to the offsite data storage facility. To restore backup and installation media to its offshore data storage location, the steps listed below should be followed.

1. Log the retrieved backup or installation media:
    a. Record the name of the media, its type, its size, and any other relevant information.
    b. Note the date and time the media was retrieved.
2. Package the retrieved media:
    a. Place the media in an appropriate container for transport.
    b. Label the container with the name of the media, the date and time it was retrieved, and any other relevant information.
3. Prepare the media for transportation:
    a. Ensure the container is secure and will not be damaged during transportation.
    b. Ensure the data is secure and will not be accessed during transportation.
4. Transport the media to the offsite storage location:
    a. Utilize a secure transportation method (e.g., truck, courier, etc.)
    b. Ensure the media is securely stored at the offsite location.
5. Validate the media is securely stored at the offsite location:
    a. Verify that the media has been correctly stored in the correct location.
    b. Confirm that the media is secured and cannot be accessed by unauthorized personnel.
    c. Record the date and time the media was stored at the offsite location.

3.6.7 Data Backup

The system should be completely backed up as soon as is practical after recovery, and a fresh copy of the currently functional system should be kept for potential future recovery attempts. The other system backups are then stored with this complete backup. The steps to take while performing a full system backup are:

1. Ensure that all systems are powered down and unplugged.
2. Check all systems to ensure that all data has been saved and all services have been stopped.
3. Ensure that the system is correctly identified, and that all necessary information has been recorded.
4. Ensure that all necessary media and backup devices are available and ready.
5. Start the full system backup process.
6. Depending on the backup medium, create a full system image backup or create a full system backup that includes all data, system settings, and applications.
7. Ensure that the backup is completed and that the medium is properly labeled and stored.
8. Log the details of the backup and store the log in the appropriate location.
9. Perform periodic tests of the full system backup to ensure that the backup is valid and can be used for recovery purposes.
10. Store the backup medium offsite with the other backups in Section 5.7.

3.6.8 Event Documentation

It is crucial that all recovery events, including the steps taken and issues encountered during the recovery and reconstitution attempt, be thoroughly documented to include and update this DRP with any new information. Each DRP team or individual must keep a record of their activities during the recovery and reconstitution process and submitting that record to the DRP Coordinator.

1. **CEO**: The CEO is responsible for providing executive oversight and guidance in the development, implementation, and maintenance of the disaster recovery plan. They must provide their expertise in the assessment and prioritization of risks, and the development of strategies for mitigating those risks. They must also provide information about the company’s objectives and the resources available for implementing the plan.
2. **CIO/CISO**: The CIO/CISO is responsible for ensuring the technology, security, and continuity of the company’s operations in the event of a disaster. They must provide information about the company’s systems, technology infrastructure, and security protocols. They must also provide technical expertise for ensuring the systems and data can be recovered quickly and efficiently.
3. **Security Managers**: Security Managers are responsible for providing information about the security protocols and procedures that must be followed in the event of a disaster. They must provide guidance on access control measures, authentication methods, and other security procedures that must be implemented to ensure the safety and integrity of the company’s data and systems.
4. **Security Technicians**: Security Technicians are responsible for providing technical assistance in the implementation and maintenance of the company’s security protocols and procedures. They

must provide expertise in the configuration and implementation of security systems, as well as providing technical support in the event of a disaster.

5. **IT Managers**: IT Managers are responsible for providing information about the systems and applications that must be recovered in the event of a disaster. They must provide expertise in the assessment of risks and recovery strategies, as well as providing guidance on the implementation and maintenance of the disaster recovery plan.
6. **IT Technicians**: IT Technicians are responsible for providing technical assistance in the implementation and maintenance of the disaster recovery plan. They must provide expertise in the configuration and implementation of systems and applications, as well as providing technical support in the event of a disaster.
7. **System Administrators**: System Administrators are responsible for providing information about the hardware and software that must be recovered in the event of a disaster. They must provide expertise in the assessment of risks and recovery strategies, as well as providing guidance on the implementation and maintenance of the disaster recovery plan.
8. **Network Administrators**: Network Administrators are responsible for providing information about the network systems that must be recovered in the event of a disaster. They must provide expertise in the assessment of risks and recovery strategies, as well as providing guidance on the implementation and maintenance of the disaster recovery plan.

3.6.9 Deactivation

The CEO of ACME Corp will formally deactivate the DRP recovery and reconstitution effort once all tasks have been finished and the necessary documentation has been updated. All business and technical POCs, as well as any additional people participating in the recovery operation, shall be informed of this declaration.

4 Business Continuity

4.1 Overview

ACME Corp is a federal contractor that offers installation, maintenance, and security services for agencies in the US and the EU. This Business Continuity Plan (BCP) aims to provide a comprehensive framework to guarantee the continuity of operations in case of a disruption. The plan outlines the strategies, procedures, and resources necessary to maintain critical operations in the face of a wide range of potential disruptions. It includes a risk assessment, a business impact analysis, and a recovery strategy. The plan also specifies the roles and responsibilities of personnel, the equipment and systems required, and the staff needed to ensure the successful execution of the plan. The plan is flexible and scalable to accommodate the changing needs of the organization.

4.1.1 Business Continuity Program Policy

ACME Corp is dedicated to keeping a comprehensive Business Continuity Program (BCP) to guarantee the continued availability and security of our systems and services. The BCP is meant to safeguard our information assets from any potential threats or disruptions.

The Chief Information Officer/Chief Information Security Officer (CIO/CISO) oversees the BCP and is responsible for its development, implementation, and upkeep. The CIO/CISO reports to the CEO regarding the successful execution of the BCP.

ACME Corp's BCP has the necessary resources, maintenance, and budget allocated for its successful implementation and execution. All personnel, suppliers, subcontractors, and vendors are informed about the BCP to ensure everyone understands its expectations and requirements.

The BCP is designed to ensure the continued availability and security of our systems and services through detailed plans and procedures for each functional area within the organization. The BCP provides the necessary guidance and direction to ensure its successful execution in case of potential threats or disruptions.

4.1.2 Planning Assumptions

- The Business Continuity Plan will be reviewed and updated as necessary.
- There will be sufficient resources to carry out the Business Continuity Plan.
- All stakeholders will be notified of the Business Continuity Plan and its goals.
- The Business Continuity Plan will be tested and assessed regularly.

4.1.3 Objectives

The purpose of ACME Corp's BCP is to maintain operations and safeguard information assets in case of a disruption. The BCP will provide a comprehensive system for managing the organization's information systems and assets, and will include the following components:

- **Risk Management**: Identifying and evaluating risks related to the organization's information systems and assets and creating strategies to minimize those risks.
- B**usiness Impact Analysis**: Examining the potential impact of a disruption on the organization's operations and assets.
- **Contingency Planning**: Creating plans to maintain operations and protect information assets in case of a disruption.
- **Training and Awareness**: Developing and implementing training and awareness programs to ensure personnel are knowledgeable about the organization's BCP.
- **Testing and Exercises**: Developing and implementing testing and exercise programs to ensure the effectiveness of the BCP and personnel familiarity with its procedures.
- **Maintenance**: Developing and implementing procedures to keep the BCP up to date.

4.1.4 Risk Assessments

Key

PROBABILITY SCALE	BUSINESS IMPACT SCALE	CONTROL SCALE
1 – 2 – 3 – 4 – 5	1 – 2 – 3 – 4 – 5	1 – 2 – 3 – 4 - 5
Low…………………High	No Impact………..High Impact	Good……………..Poor

Table 4 Risk Assessment Scale

Probability Scale: The likelihood that an event will occur.
Business Impact Scale: The degree to which the event will affect your business.

Control Scale: How much control you have in preventing the event

Assessment Table

Threat	Probability Scale	Impact Scale	Control Scale	Ideas for Mitigation
Natural Disaster	1	4	4	Establish an emergency plan and ensure that all personnel are aware of it. Ensure that all necessary equipment is stored in a secure location.
Cyber Attack	2	5	4	Implement a robust security system that includes firewalls, antivirus software, and intrusion detection systems. Ensure that all personnel are trained in cyber security best practices.
Data Loss	3	4	3	Implement a reliable backup system and ensure that all data is regularly backed up. Implement a data recovery plan in case of data loss.
Power Outage	4	3	3	Install a backup power supply and ensure that all personnel are aware of the procedure for using it.
Security Breach	5	2	2	Implement a robust security system that includes firewalls, antivirus software, and intrusion detection systems. Ensure that all personnel are trained in cyber security best practices.
Hardware Failure	1	3	3	Implement a reliable maintenance system and ensure that all hardware is regularly inspected and serviced.
Software Failure	2	4	2	Implement a reliable maintenance system and ensure that all software is regularly updated and tested.
Communication Interruption	3	5	2	Establish an emergency communication plan and ensure that all personnel are aware of it.
Regulatory Change	4	2	1	Monitor regulatory changes and ensure that all personnel are aware of any changes that may affect operations.
Personnel Change	5	3	1	Establish a personnel change management system and ensure that all personnel are aware of it.

Table 5 Risk Assessment Table

4.1.5 Business Impact Analysis Summary

ACME Corp will conduct a business impact analysis by determining the mission-critical business processes and their recovery criticality. This will involve assessing the potential impact of a disruption or failure on the organization's ability to achieve its goals and objectives. The necessary resources, including personnel, equipment, software, and data, will be identified to support these processes. Recovery priorities will also be determined for the system or business resources, considering factors such as regulatory requirements, risk assessment, and criticality of the process.

BIA Summary

Business Unit	Manager	Process	RTO	Daily Loss	Function	Risks	Comment
IT Department	CIO/CISO	System Maintenance	24 Hours	$10,000	Ensure systems are	Security breaches, data loss,	All systems must be regularly

					up-to-date and secure	system outages	monitored and updated to ensure security and reliability.
IT Department	IT Managers	Network Administration	12 Hours	$5,000	Ensure network is secure and functioning	Network outages, security breaches, data loss	All network components must be regularly monitored and updated to ensure security and reliability.
IT Department	System Administrators	Data Backup	8 Hours	$2,000	Ensure data is backed up and secure	Data loss, security breaches	All data must be regularly backed up and stored securely.
IT Department	Security Technicians	Security Monitoring	4 Hours	$1,000	Monitor for security threats	Security breaches, data loss	All systems must be monitored for potential security threats.

Table 6 Business Impact Analysis Summary

4.1.6 Business Continuity Strategy

ACME Corp provides its customers with safe and dependable services. As such, the company has created a detailed Business Continuity Strategy to maintain operations in case of an emergency or disaster. This strategy is based on the NIST Special Publication 800-34 Rev. 1 "Contingency Planning Guide for Federal Information Systems" and includes the following principles:

1. **Risk Management**: ACME Corp will identify, assess, and prioritize risks to its operations. Risk assessments will be conducted on a regular basis and risk mitigation strategies will be developed and implemented.
2. **Business Resilience**: ACME Corp will develop and implement plans and procedures to ensure the continuity of operations in the event of an emergency or disaster. These plans and procedures will include backup and recovery plans, disaster recovery plans, and business continuity plans.
3. **Security**: ACME Corp will ensure the security of its information systems by implementing security controls and procedures in accordance with NIST Special Publication 800-53.
4. **Communication**: ACME Corp will ensure that all stakeholders are informed of the status of its operations in the event of an emergency or disaster.
5. **Training and Awareness**: ACME Corp will provide training and awareness programs to ensure that all personnel are aware of the Business Continuity Strategy and are prepared to respond to an emergency or disaster.

6. **Testing and Exercises**: ACME Corp will conduct regular tests and exercises to ensure that the Business Continuity Strategy is effective and that personnel are prepared to respond to an emergency or disaster.
7. **Documentation**: ACME Corp will document all aspects of the Business Continuity Strategy and ensure that all personnel are aware of the documentation. The Business Continuity Strategy will be reviewed and updated on a regular basis to ensure that it remains effective and up to date.

4.1.7 Emergency Operations Center (EOC) Locations/Contacts

EOC LOCATION	ACME Corp Business Office Facility
EOC POINT OF CONTACT	ACME Corp CIO/CISO
POC PHONE NUMBER	(XXX) XXX-XXXX
EOC LOCATION	ACME Corp Alternate Site Facility
EOC POINT OF CONTACT	ACME Corp Security Manager
POC PHONE NUMBER	(XXX) XXX-XXXX

4.1.8 Alternate Site Locations and Contacts

ALTERNATE SITE	ACME Corp Headquarters, US.
ALTERNATE POC	CEO
CONTACT PHONE NUMBER	(XXX)XXX-XXXX

OFFSITE STORAGE	ACME Corp Data Center, US.
OFFSITE STORAGE POC	CIO/CISO
CONTACT PHONE NUMBER	(XXX)XXX-XXXX

4.1.9 BCP Team Descriptions and Organization Chart

Additional responsibilities for some teams are discussed in the Disaster Recovery Plan for information technology.

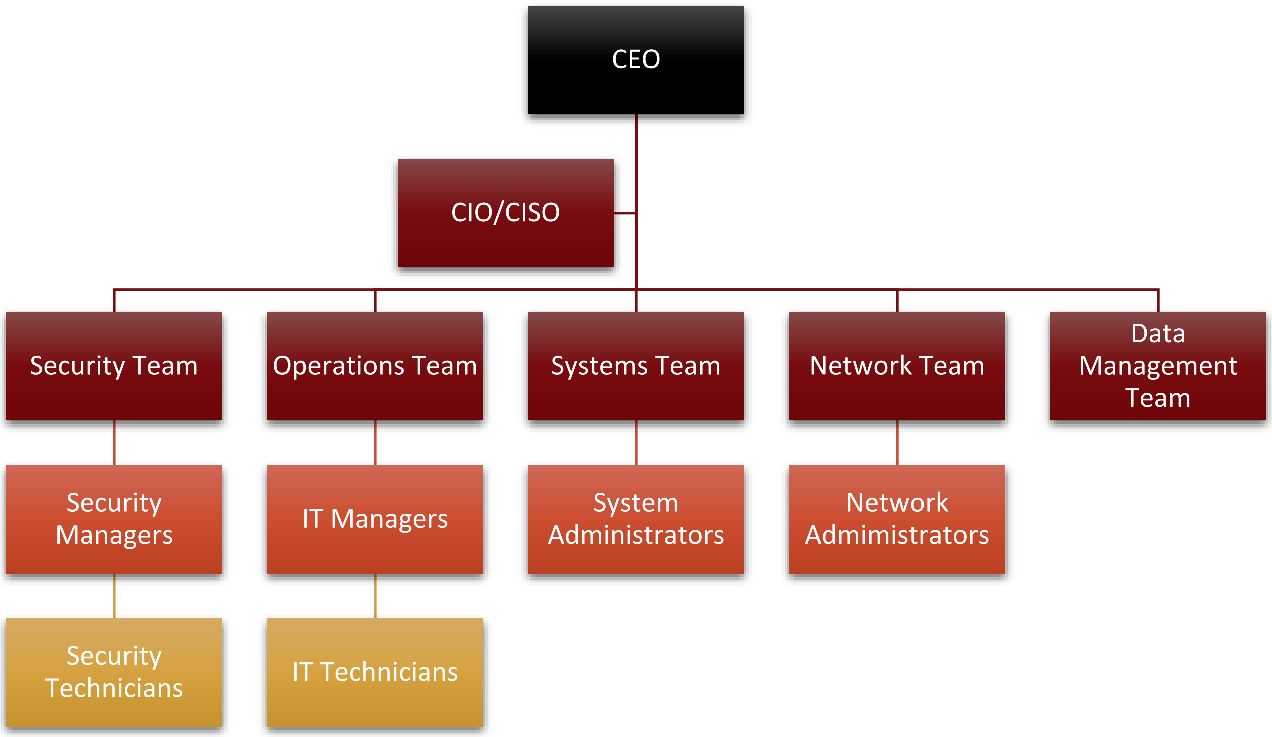

Figure 2 Business Continuity Organization Chart

Security Team

This team will be responsible for ensuring the security of the organization's systems, networks, and data. This team will be responsible for developing, implementing, and maintaining security policies, procedures, and controls.

Operations Team

This team will be responsible for the day-to-day operations of the organization's systems, networks, and data. This team will be responsible for monitoring system performance, troubleshooting issues, and responding to incidents.

Systems Team

This team will be responsible for the installation, configuration, and maintenance of the organization's systems, networks, and data. This team will be responsible for ensuring the systems are up-to-date and secure.

Network Team

This team will be responsible for the installation, configuration, and maintenance of the organization's networks. This team will be responsible for ensuring the networks are up-to-date and secure.

Data Management Team

This team will be responsible for the storage, backup, and recovery of the organization's data. This team will be responsible for ensuring the data is up-to-date and secure.

4.1.10 Emergency Response Plan Summary

ACME Corp has an approved emergency response plan that is routinely reviewed, exercised, and updated. This plan is designed to ensure that the company is prepared to respond to any emergency.

The plan includes the following key elements:

- Procedures for notifying and working with emergency responders, including local law enforcement, fire departments, and other emergency services.
- Guidelines for making a company disaster declaration, including when to declare a disaster and how to communicate the declaration to staff and other stakeholders.
- Procedures for notifying staff and maintaining lines of communication, including how to contact staff in the event of an emergency and how to keep them informed of the situation.
- Procedures for triggering implementation of the BCP, including how to identify when the BCP needs to be activated and how to ensure that all staff are aware of the activation.
- Procedures for how and when to move to an alternate site, including how to identify an appropriate alternate site and how to ensure that all staff are aware of the move.
- Procedures for how to access data stored off site, including how to identify which data needs to be accessed and how to ensure that the data is securely accessed.

4.2 Critical Business Information

4.2.1 Team Call List

NAME	MOBILE PHONE NUMBER	EMAIL	WORK UNIT / DEPARTMENT
Security Manager			Security
Security Technician			Security
IT Manager			IT
IT Technician			IT
System Administrator			Systems
Network Administrator			Network
Data Manager			Data Management

Table 7 Business Continuity Team Call List

4.2.2 Team Task List

Security Team Task List

TASK	ASSIGNED	FREQUENCY
Develop and implement security policies, procedures, and controls	Security Managers	As needed
Monitor system performance and respond to incidents	Security Technicians	Daily
Install and configure security systems	Security Technicians	As needed
Maintain security systems	Security Technicians	As needed
Perform security audits	Security Managers	Quarterly
Conduct security training	Security Managers	Quarterly
Test security systems	Security Technicians	Quarterly
Investigate security incidents	Security Managers	As needed
Develop and implement security plans	Security Managers	As needed
Develop and implement security awareness programs	Security Managers	As needed

Operations Team Task List

TASK	ASSIGNED	FREQUENCY
Monitor system performance and respond to incidents	IT Technicians	Daily
Install and configure systems	IT Technicians	As needed
Maintain systems	IT Technicians	As needed
Perform system audits	IT Managers	Quarterly
Conduct system training	IT Managers	Quarterly
Test systems	IT Technicians	Quarterly
Investigate system incidents	IT Managers	As needed
Develop and implement system plans	IT Managers	As needed
Develop and implement system awareness programs	IT Managers	As needed

Systems Team Task List

TASK	ASSIGNED	FREQUENCY
Install and configure systems	System Administrators	As needed
Maintain systems	System Administrators	As needed
Perform system audits	System Administrators	Quarterly
Conduct system training	System Administrators	Quarterly
Test systems	System Administrators	Quarterly
Investigate system incidents	System Administrators	As needed
Develop and implement system plans	System Administrators	As needed
Develop and implement system awareness programs	System Administrators	As needed

Network Team Task List

TASK	ASSIGNED	FREQUENCY
Review and update network diagrams	Network Technicians	Monthly
Test and update network configurations	Network Technicians	Monthly
Test and update network segmentation	Network Technicians	Monthly
Review and update network policies	Network Technicians	Monthly
Monitor network security events	Network Technicians	Daily
Test and update intrusion detection systems	Network Technicians	Monthly
Review and update disaster recovery plans	Network Technicians	Quarterly
Test and update backup systems	Network Technicians	Monthly
Test and update failover systems	Network Technicians	Monthly
Test and update network redundancy	Network Technicians	Monthly

Data Management Team Task List

TASK	ASSIGNED	FREQUENCY
Create a backup and storage strategy	Data Management Team	Weekly
Test the backup and storage strategy	Data Management Team	Monthly
Develop and implement an incident response plan for data loss	Data Management Team	Quarterly
Review the backup and storage strategy	Data Management Team	Yearly
Create a disaster recovery plan for data loss	Data Management Team	As needed
Monitor and review changes to the data management system	Data Management Team	Monthly
Train personnel on data management best practices	Data Management Team	Quarterly

4.2.3 Team Action Plan

Response Team Action Plan

BUSINESS CONTINUITY RESPONSE TEAMS		
Security Team	Operations Team	Systems Team
Network Team	Data Management Team	

4.2.3.1 Response Team: Security Team

- Security Managers
- Security Technicians

Responsibilities:

- Coordinate with other teams and departments to implement and maintain the company's security policies and procedures
- Monitor the company's systems and networks for security threats and vulnerabilities, and take appropriate action to mitigate or respond to any identified risks
- Provide security training and education to employees to ensure they are aware of and adhere to the company's security policies and procedures
- Develop and maintain the company's incident response plan, disaster recovery plan, and business continuity plan
- Maintain and update the company's security policies and procedures based on industry best practices and changes in the company's technology infrastructure

Tasks: (Primary Facility)

- Monitor the company's systems and networks for security threats and vulnerabilities using a variety of tools and techniques
- Respond to security incidents and breaches, including investigating the cause, determining the impact, and implementing appropriate countermeasures to prevent further harm
- Coordinate with other teams and departments to implement security controls and safeguards, such as access controls, encryption, firewalls, and intrusion detection systems
- Provide security training and education to employees on a regular basis to ensure they are aware of the company's security policies and procedures and how to protect company assets
- Develop and maintain the company's incident response plan, including the roles and responsibilities of the response team, the steps to be taken in the event of an incident, and the communication and reporting procedures

Tasks: (Alternate Site)

- Review and update the company's disaster recovery plan on a regular basis to ensure it is up to date and effective in the event of a disaster
- Coordinate with the Operations Team, Systems Team, and Network Team to ensure that the company's critical systems and data are regularly backed up and can be restored at the alternate site
- Develop and maintain the company's business continuity plan, including the roles and responsibilities of the response team, the procedures for maintaining business operations at the alternate site, and the communication and reporting procedures

- Test the company's disaster recovery and business continuity plans on a regular basis to ensure they are effective and can be successfully implemented in the event of a disaster.

4.2.3.2 Response Team: Operations Team

- IT Managers
- IT Technicians

Responsibilities:

- Coordinate with other teams and departments to ensure that the company's business operations are running smoothly and efficiently
- Develop and implement procedures and processes to ensure that the company's systems and networks are operating at peak performance
- Develop and maintain the company's disaster recovery plan, including the roles and responsibilities of the operations team, the procedures for restoring systems and data in the event of a disaster, and the communication and reporting procedures
- Monitor the company's systems and networks for potential performance issues and take appropriate action to resolve any identified issues
- Provide support and assistance to employees to ensure they can use the company's systems and networks effectively

Tasks: (Primary Facility)

- Monitor the company's systems and networks for performance issues using a variety of tools and techniques
- Respond to incidents and outages, including investigating the cause, determining the impact, and implementing appropriate countermeasures to restore service as quickly as possible
- Coordinate with other teams and departments to implement processes and procedures for maintaining and improving system and network performance, such as capacity planning, performance tuning, and troubleshooting
- Provide support and assistance to employees who are experiencing issues with the company's systems and networks, including answering questions, providing guidance, and escalating issues as necessary
- Develop and maintain the company's disaster recovery plan, including the procedures for restoring systems and data in the event of a disaster and the communication and reporting procedures

Tasks: (Alternate Site)

- Review and update the company's disaster recovery plan on a regular basis to ensure it is up to date and effective in the event of a disaster
- Coordinate with the Systems Team and Network Team to ensure that the company's critical systems and data are regularly backed up and can be restored at the alternate site
- Test the company's disaster recovery plan on a regular basis to ensure it is effective and can be successfully implemented in the event of a disaster

- Develop and implement procedures and processes for maintaining business operations at the alternate site, including establishing communications, providing support and assistance to employees, and coordinating with other teams and departments as necessary.

4.2.3.3 Response Team: Systems Team

- System Administrators

Responsibilities:

- Coordinate with other teams and departments to design, implement, and maintain the company's systems and networks
- Monitor the company's systems and networks for potential performance and security issues, and take appropriate action to resolve any identified issues
- Provide support and assistance to employees who are experiencing issues with the company's systems and networks, including answering questions, providing guidance, and escalating issues as necessary
- Develop and maintain the company's disaster recovery plan, including the roles and responsibilities of the systems team, the procedures for restoring systems and data in the event of a disaster, and the communication and reporting procedures

Tasks: (Primary Facility)

- Monitor the company's systems and networks for performance and security issues using a variety of tools and techniques
- Respond to incidents and outages, including investigating the cause, determining the impact, and implementing appropriate countermeasures to restore service as quickly as possible
- Coordinate with other teams and departments to design, implement, and maintain the company's systems and networks, including hardware, software, and networks
- Provide support and assistance to employees who are experiencing issues with the company's systems and networks, including answering questions, providing guidance, and escalating issues as necessary
- Develop and maintain the company's disaster recovery plan, including the procedures for restoring systems and data in the event of a disaster and the communication and reporting procedures

Tasks: (Alternate Site)

- Review and update the company's disaster recovery plan on a regular basis to ensure it is up to date and effective in the event of a disaster
- Coordinate with the Operations Team and Network Team to ensure that the company's critical systems and data are regularly backed up and can be restored at the alternate site
- Test the company's disaster recovery plan on a regular basis to ensure it is effective and can be successfully implemented in the event of a disaster
- Develop and implement procedures and processes for restoring systems and data at the alternate site in the event of a disaster, including coordinating with other teams and departments as necessary.

4.2.3.4 Response Team: Network Team

- Network Administrators

Responsibilities:

- Monitor network traffic and system performance in real time
- Identify and diagnose network-related issues or disruptions
- Implement and maintain network security controls and protocols
- Coordinate with other teams and emergency responders in the event of a disaster or incident
- Develop and maintain documentation of network architecture and configuration
- Ensure network connectivity and availability at both primary and alternate sites

Tasks: (Primary Facility)

- Continuously monitor network traffic and system performance using network monitoring tools
- Identify and troubleshoot network-related issues or disruptions, and take corrective action as needed
- Implement and maintain network security controls, such as firewalls and intrusion detection systems
- Coordinate with the Operations Team and other response teams in the event of a disaster or incident
- Maintain documentation of network architecture and configuration, including backup copies of all critical data
- Ensure that all network devices and systems are operational and properly configured

Tasks: (Alternate Site)

- Coordinate with the Operations Team and other response teams to establish network connectivity at the alternate site
- Configure network devices and systems at the alternate site, as necessary
- Test network connectivity and availability to ensure that it meets the requirements of the business continuity plan
- Develop and maintain documentation of the network architecture and configuration at the alternate site, including backup copies of all critical data
- Monitor network traffic and system performance at the alternate site, and take corrective action as needed.

4.2.3.5 Response Team: Data Management Team

- IT Managers
- System/Network Administrators

Responsibilities:

- Develop and maintain data backup and recovery plan
- Monitor and review data backup processes
- Coordinate with other teams to ensure data integrity and availability
- Test and evaluate data recovery processes

Tasks: (Primary Facility)

- Develop a list of critical data and systems
- Implement data backup processes
- Monitor and review data backup processes
- Test and evaluate data recovery processes

Tasks: (Alternate Site)

- Coordinate with other teams to ensure data is being backed up and restored properly at the alternate site
- Test and evaluate data recovery processes at the alternate site
- Ensure data is being backed up and restored to the alternate site in a timely manner
- Coordinate with other teams to ensure data is being properly accessed and used at the alternate site.

4.2.4 Mission Critical Equipment List

ITEM NAME	QTY	SRC	NO.	COST	TOTAL
Active Directory Domain Services for security domain management					
Firewalls and application layer proxies running Red Hat Enterprise Linux					
Cisco routers and switches using Cisco's IOS platform					
Windows 3.1 through current and Windows Server 2000 through current					
Smartphones using the Android platform					

Table 8 Mission Critical Equipment List

4.2.5 Vendor List

CUSTOMER NAME	PHONE NUMBER	EMAIL ADDRESS	MAILING ADDRESS	PRODUCT
Microsoft				
Red Hat				
Cisco				
Android				

Table 9 Vendor List

4.3 Plan Administration and Maintenance

The BCP will be managed by the CIO/CISO in collaboration with the Security, Operations, Systems, Network and Data Management teams. This plan will be created to protect ACME Corp's sensitive data and systems. The BCP will be reviewed and updated annually or when a significant change occurs within the organization. Any changes and updates to the BCP will be reviewed by the CIO/CISO and approved by the CEO.

Planning Team

The planning team for the BCP will include the CIO/CISO, Security Managers, Security Technicians, IT Managers, IT Technicians, System Administrators and Network Administrators. These individuals will be responsible for developing, reviewing, and updating the BCP.

Planning Process

The planning process for the BCP will involve the following steps:

1. Identify the resources necessary to protect ACME’s sensitive data and systems.
2. Develop, review, and update the BCP.
3. Ensure the plan meets the requirements of applicable laws, regulations, and industry standards.
4. Test the BCP to ensure it is effective.
5. Monitor the BCP to ensure it is up-to-date and effective.
6. Review the BCP on an annual basis, or when a significant change occurs in the organization.

Meeting Frequency

The planning team will meet bi-monthly to review the progress of the BCP and make any necessary changes.

Training

All personnel involved in the BCP should be trained in the use of the plan. Training should be provided annually or when a significant change occurs within the organization. This training should include an overview of the plan and its components, as well as instructions for testing and monitoring the plan. Training should be updated regularly.

4.3.1 Business Continuity Plan Administration

ACME Corp will ensure the administration of the BCP is carried out efficiently and effectively to ensure the successful implementation and maintenance of the organization's information system security. The BCP will be managed by the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) in collaboration with the Security, Operations, Systems, Network and Data Management Teams.

The BCP will include a training and awareness program designed to ensure all employees are familiar with the organization's security policies, procedures, and controls. The organization will also establish a review process for the BCP to ensure the plan is up to date with changes to the organization's systems, networks, and data. The CIO and CISO will conduct regular reviews of the BCP and provide periodic status reports to the organization's leadership.

The organization will also develop and maintain documentation on the BCP to ensure the plan is updated and maintained. The documentation will include an overview of the organization's security posture, the risk assessment process, the security policies and procedures, and the response and recovery plans. The documentation will also include a list of all the organization's security controls and their associated systems, networks, and data.

Finally, the organization will establish a method of communication to ensure the BCP is communicated to all employees. This communication will include but not be limited to emails, newsletters, and intranet postings. The organization will also establish a contingency plan to ensure the communication of the BCP in the event of an emergency.

4.3.2 BCP Awareness and Training

AWARENESS ACTIVITY	FREQUENCY	RESPONSIBLE OFFICE	REQUIRED MATERIALS	COMMENTS
Security Awareness Training	Annually	Security Team	Videos and presentations	Will provide regular training for employees to keep them informed about the latest security threats and best practices.
Operations Awareness Training	Annually	Operations Team	Videos and presentations	Will provide regular training for employees to keep them informed about the latest operational threats and best practices.
Systems Awareness Training	Annually	Systems Team	Videos and presentations	Will provide regular training for employees to keep them informed about the latest systems threats and best practices.
Network Awareness Training	Annually	Network Team	Videos and presentations	Will provide regular training for employees to keep them informed about the latest network threats and best practices.
Data Management Awareness Training	Annually	Data Management Team	Videos and presentations	Will provide regular training for employees to keep them informed about the latest data management threats and best practices.
BCP Awareness Training	Annually	All teams	Videos and presentations	All teams will provide regular training for employees to keep them informed about the Business Continuity Plan and how it applies to them.

Table 10 BCP Awareness and Train

4.3.3 Exercising (Testing) The BCP

At least 2 exercises shall be conducted every year.

EXERCISE TYPE	PURPOSE	PARTICIPANTS
Tabletop Exercise	Review and test the organization's response to a simulated incident	Security Team, Operations Team
Full-Scale Exercise	Validate the Business Continuity Plan with a real-world event	All Teams

Table 11 BCP Exercises and Training

4.3.4 Business Continuity Plan Maintenance

The Business Continuity Committee (BCC) is responsible for maintaining the BCP and ensuring it is updated as needed. This includes establishing a timetable for updates, completing the necessary updates, and distributing the updated plan to the Distribution List at the beginning of the document. The plan is updated in response to changes in the organization, business processes, and test results, as well as based on lessons learned and annual plan reviews. When updates are made, the revised sections are provided to BCP team members and plan holders, and they are notified of the changes. The plan will also be updated after an actual disaster occurs.

The BCC is also responsible for maintaining and updating the Business Impact Analysis (BIA). This includes establishing a timetable for updates, completing the required updates, and generating BCP updates, if necessary, based on the new data collected. A BIA update is needed annually and in response to significant changes in the organization or events. The BCP will be updated to reflect changes in the BIA.

4.4 Exercise Plans and After-Action Reports

The overarching objectives of a BCP exercise program are to:

- Create a learning environment for all participants to learn about the BCP
- Document changes and updates (including omissions) to the BCP

4.4.1 Business Continuity Plan Exercise Methodology

The Business Continuity Plan can be verified and validated using any one of the following methodologies:

- Tabletop Exercise - key personnel discussing simulated scenarios in an informal setting
- Functional Exercise - simulates the reality of operations in a functional area by presenting complex and realistic problems
- Full Scale Exercise - real operations in multiple functional areas present complex and realistic problems that require critical thinking, rapid problem solving, and effective responses by trained personnel
- Drill - coordinated, supervised activity usually used to test a single specific operation or function

4.4.2 Exercise Objectives

The overarching objectives of a Business Continuity Plan Exercise are to:

- Determine the state of readiness of your BCP by creating a learning environment for all participants to learn about the plan.
- Validate the BCP resource lists -- people and inventories are sufficient to effect recovery of business operations and/or IT services as appropriate. Document changes and updates (including omissions) to the BCP.
- Verify the information in the BCP is current and accurately reflects the organization’s requirements.

After the exercise, make certain that all changes and updates are completed, and distribute those updates to your Distribution List as described in Chapter One.

90 Days Prior	
☐	Determine resource needs and identify constraints (room sizes available, etc.) in coordination with other participants (e.g., key suppliers, customers, local emergency responders) based on estimated attendees.
☐	Identify and distribute invitations to facilitators, scribes, and other support personnel required in consultation with other participants (e.g., key suppliers, customers, local emergency responders).
☐	Establish a registration cut-off date for any outside invitees, like customers, vendor support, call center representatives, or emergency responders.

☐	Distribute invitations and registration questionnaires to participants and observers via letter or email. Display posters, if applicable.
☐	Complete follow-up phone calls to prospective attendees if resources are still available.
30 Days to 10 Days Prior	
☐	Schedule facilitator training (if required).
☐	Determine the most effective way to categorize attendees (e.g., grouping participants based on similar Department, BCP responsibilities).
☐	Finalize PowerPoint™ presentation and exercise documentation.
☐	Confirm facilitators, scribes, and other support personnel attendance and responsibilities.
10 Days Prior to Exercise Start	
☐	Confirm registrant attendance through emails or phone calls.
☐	Create name tags.
☐	Conduct dry run.
Post-Exercise	
☐	Conduct Exercise Hot Wash/plenary session.
☐	Collect and analyze scribe data collection forms and produce an After-Action Report.
☐	Formulate lessons learned and next steps to address areas of improvement identified during the exercise.

5 Appendices

5.1 Key Personnel and Team Members Contact List

Role	Name	Email	Phone
CEO			
CIO/CISO			
Security Managers			
IT Managers			
System Administrators			
Network Administrators			

5.2 Incident Response Process Checklists

Preparation

☐ Create an Incident Response Team (IRT) with roles and responsibilities for each position.
☐ Assign a Primary and Secondary Point of Contact for the IRT.
☐ Develop an Incident Response Plan (IRP) detailing the procedures for responding to an incident.
☐ Identify and document the assets, systems, and systems of record that are at risk.
☐ Identify any additional hardware or roles for system components that are needed to facilitate security management.
☐ Establish processes and procedures for responding to incidents, including notification and escalation.
☐ Implement system monitoring and logging tools to aid in incident detection and analysis.
☐ Provide IRT members with the necessary resources and tools to respond to security incidents.
☐ Perform risk assessments to identify potential threats and select appropriate controls to mitigate them.
☐ Ensure all IRT members adhere to the training standards.
☐ Review the Incident Response Plan (IRP) with IRT members.
☐ Conduct regular security audits and vulnerability assessments.
☐ Train staff on incident response policies and procedures.
☐ Conduct annual security incident response exercises involving scenario-based tabletop exercises.
☐ Document and assign any shortcomings found during the exercise to the right stakeholders in SharePoint entries.
☐ Review the results of the security incident response exercise with the CIO/CISO.
☐ Develop an incident response exercise schedule and conduct drills to test the IRT's response time and effectiveness.

Detection

☐ Monitor 24/7/365 for events
☐ Respond to input sources
☐ Utilize Microsoft Azure Sentinel to monitor security of environment

- □ Investigate suspicious activity
- □ Run security scans and vulnerability assessments
- □ Check system logs and audit trails
- □ Analyze network traffic
- □ Acknowledge and document events in the incident management SharePoint
- □ Report security events, such as automated warnings, reports from external parties, personal observations, or indications of virus, malicious software, or hacker activity
- □ Notify leadership, system owners, customer agencies, and ACME Corp of security events
- □ Report security incidents involving Government information or systems to customer agencies within 60 minutes
- □ Notify any affected customers immediately if sensitive information has been or will be misused

Analysis

- □ Troubleshoot the incident using out-of-band steps
- □ Document troubleshooting actions taken in the SCOM incident tracking entry
- □ Document the Reason-for-Incident (RFI) with as much technical detail as possible
- □ Bring in additional technical and business expertise as needed
- □ Classify security events as false positives, security incidents, customer-reportable security incidents, or privacy incidents
- □ Escalate all security events to CEO, CIO/CISO, and Security Managers
- □ Identify and address root cause for false positives in a systematic way
- □ Handle privacy incidents in the same way as security incidents
- □ Determine US-CERT notification requirements for security incidents with potential impact to US Federal Customers
- □ Provide technical expertise and troubleshooting support to the IRT
- □ If a data breach is suspected, formally declare the incident by the CIO/CISO
- □ Execute Security Breach Response sub-process in the event of a data breach

Containment

- □ Identify and document the incident’s priority level.
- □ Identify and document the incident’s source, scope, and potential impact.
- □ Identify and document the incident’s affected systems and users.
- □ Identify and document any emergency mitigation action needed.
- □ Identify and document any customer impact and/or reported incidents.
- □ Identify and present mitigation options to the Incident Commander.
- □ Ensure that mitigation options are described in the SCOM Incident Tracking Entry.
- □ Ensure automated methods are identified to validate the mitigation is in place.
- □ Ensure that detection methods are documented in the SCOM Incident Tracking Entry.
- □ Coordinate mitigation decision-making regarding implementation and validation strategies.
- □ Assign system administrators to investigate and monitor assets in the secure VPC.
- □ Notify security team of any suspicious activity.
- □ Use firewalls and application layer proxies to block unauthorized access and malicious activities.

□ Manage and monitor network traffic and block any suspicious traffic.
□ Manage smartphones and other mobile devices with MDM solutions to control access and detect malicious activities.
□ Manage Cisco routers and switches with Cisco IOS to control access and detect malicious activities.
□ Implement endpoint protection solutions such as antivirus, anti-malware, and intrusion prevention systems.
□ Implement intrusion detection systems to detect and alert on malicious activity.
□ Implement network segmentation and other network security measures.
□ Use network sniffers to monitor network traffic and detect malicious activity.

Eradication

□ Identify and document the incident’s source, scope, and potential impact.
□ Identify and document the incident’s affected systems and users.
□ Identify and document any emergency mitigation action needed.
□ Identify and document any customer impact and/or reported incidents.
□ Determine the cause of the incident.
□ Eliminate the problem.
□ Close the point of entry based on the severity level.
□ Implement and document long-term fixes to the Incident Commander to prevent further incidents.
□ Validate repair using automated methods when possible and document in the SCOM Incident Tracking Entry.
□ Coordinate decision-making process for implementation and validation strategies.

Recovery

□ Verify that the incident is contained and isolated.
□ Identify and document the incident’s source, scope, and potential impact.
□ Identify and document the incident’s affected systems and users.
□ Identify and document any emergency mitigation action needed.
□ Identify and document any customer impact and/or reported incidents.
□ Assess the security incident and determine the risk to the organization.
□ Develop a response plan and timeline.
□ Eradicate the threat by disabling or removing malicious components from the system.
□ Identify evidence to preserve for further analysis.
□ Remove the infected device from the network.
□ Confirm that the threat is eliminated.
□ Provide status, impact assessment, and next steps to the Communications Manager.
□ Identify and present long-term repair items to the Incident Commander.
□ Track any repair items requiring code changes in the appropriate bug tracking system.
□ Track repair items involving configuration changes in the SCOM Incident Tracking.
□ Identify automated methods to validate the repair is in place.

- □ Verify successful eradication with appropriate personnel.
- □ Send final notification to all sources (unless directed otherwise by the Security Incident Manager).

Post-Incident Activity

- □ Gather all relevant data such as customer/business impact, incident severity, root cause description, repair items, timeline, external public statement (if necessary), security measures taken, and any processes implemented to prevent similar incidents.
- □ Analyze the data gathered and create a comprehensive after-action report (AAR) detailing the incident and its resolution.
- □ Share the AAR with the appropriate stakeholders for review and approval.
- □ Ensure that all repair items have been addressed and their owners, and completion dates are documented.
- □ Document all security measures taken for multi-platform systems, including Windows, Linux, Android, Cisco Routers and Switches, and Microsoft Azure.
- □ Document any additional hardware and/or roles for system components that were identified during incident review.
- □ Document all processes implemented to prevent a similar incident.
- □ Update the Microsoft SharePoint with the AAR, repair items, security measures, and processes.
- □ Draft a postmortem of the incident.
- □ Maintain an inventory of all repair items, their owners, and completion dates.
- □ Finalize the post-incident activities by submitting the postmortem and inventory to all necessary stakeholders.

Reporting

- □ Identify and document the affected system(s) and affected user(s).
- □ Identify the type of incident (e.g., malicious code, unauthorized access, etc.).
- □ Identify the source of the incident (e.g., internal, external, etc.).
- □ Collect evidence related to the incident (e.g., logs, screenshots, etc.).
- □ Document the findings and provide a timeline of the incident.
- □ Provide a summary of the incident and any relevant recommendations.

Escalation

- □ Identify the appropriate team or individual to escalate the incident to.
- □ Communicate the incident to the appropriate team or individual.
- □ Provide the team or individual with the appropriate information related to the incident.
- □ Ensure the team or individual is aware of the incident response procedures.
- □ Monitor and track the progress of the incident.

Communications

- □ Identify the appropriate internal and external contacts to notify of the incident.
- □ Notify the contacts of the incident and provide pertinent information.
- □ Provide the contacts with instructions on how to respond to the incident.

- □ Provide regular updates to the contacts on the progress of the incident.
- □ Ensure the contacts comply with any instructions or requests related to the incident.

5.3 Incident Scenarios

5.3.1 Scenario 1: Unauthorized Access on Windows Server 2000

ACME Corp is alerted to a breach in their Windows Server 2000 system. The unauthorized user has access to confidential information and has made attempts to alter and delete files.

Attack name/description	Unauthorized Access on Windows Server 2000
Threat/probable threat agents	Hackers, malicious actors, malware
Known or possible vulnerabilities	Unpatched vulnerabilities, weak passwords, unprotected ports/services, lack of system updates/patching, unsecured/unencrypted remote access
Precursor indicators	Unusual spike in network traffic, unauthorized logins, suspicious file/directory activities, unauthorized user accounts, etc.
Indicators of attack in progress	Malicious files/programs, data exfiltration, unauthorized remote access, altered/corrupted system settings/configurations, etc.
Information assets at risk from this attack	Confidential information, customer data, intellectual property, financial records, etc.
Damage or loss to information assets likely from this attack	Loss/theft of confidential information, financial loss, loss of credibility, reputational damage, etc.
Other assets at risk from this attack	System performance, availability, integrity, etc.
Damage or loss to other assets likely from this attack	System downtime, data corruption, system unavailability, etc.
Immediate actions indicated when this attack is under way	Isolate affected systems, identify attack source, quarantine compromised assets, assess, and mitigate risk, etc.
Follow-up actions after this attack was successfully executed	Analyze attack vectors and methods, update/patch systems, review security policies and procedures, implement additional security controls, etc.

5.3.2 Scenario 2: Malicious Code Infiltration

ACME Corp discovers malicious code infiltrating their Linux kernel 2.6 system, attempting to gain access to confidential information and wreak havoc on their system.

Attack name/description	Malicious code infiltration
Threat/probable threat agents	Malware, malicious actors
Known or possible vulnerabilities	Unpatched or unsupported software, weak passwords, poor access control
Likely precursor activities or indicators	Unfamiliar users logging in or out of the system, suspicious emails or files being sent or received, unusual network activity
Likely attack activities or indicators of attack in progress	Unauthorized access to the system, changes to system settings and files, attempts to gain access to confidential information
Information assets at risk from this attack	Confidential information, system settings and files, user credentials
Damage or loss to information assets likely from this attack	Theft or destruction of confidential information, alteration of system settings and files, unauthorized access to user credentials
Other assets at risk from this attack	Network infrastructure, physical access to the system, other systems on the network

Damage or loss to other assets likely from this attack	Downtime due to network disruption, physical damage to the system, unauthorized access to other systems on the network
Immediate actions indicated when this attack is under way	Isolate the system from the network, scan for malicious code and remove it, reset passwords, log out all users, disable all non-essential services, identify the source of the attack
Follow-up actions after this attack was successfully executed	Conduct an After-Action Review to determine root cause, update security policies and procedures, patch or upgrade vulnerable systems, monitor for any further malicious activity

5.3.3 Scenario 3: Microsoft Azure Breach

ACME Corp discovers their Microsoft Azure system has been accessed by an unauthorized user, who has attempted to modify and delete files, as well as access confidential information.

Attack name/description	Microsoft Azure Breach
Threat/probable threat agents	Malicious actors, hackers, unauthorized users
Known or possible vulnerabilities	Unpatched systems, weak passwords, insecure configurations, lack of multifactor authentication, etc.
Likely precursor activities or indicators	Suspicious login attempts, unauthorized data access attempts, malware infections, etc.
Likely attack activities or indicators of attack in progress	Unauthorized system access, modified or deleted files, attempts to access confidential information, etc.
Information assets at risk from this attack	Confidential documents, financial and customer data, source code, etc.
Damage or loss to information assets likely from this attack	Loss of data, theft of data, disruption of services, etc.
Other assets at risk from this attack	Network and system infrastructure, reputation of the company, etc.
Damage or loss to other assets likely from this attack	Damage to hardware and software, disruption of services, etc.
Immediate actions indicated when this attack is under way	Isolate affected systems, secure affected systems, monitor suspicious activity, prevent further unauthorized access, etc.
Follow-up actions after this attack was successfully executed	Perform a forensic investigation, restore systems and data, update security measures, etc.

5.3.4 Scenario 4: Unauthorized Smartphone Access

ACME Corp is alerted to a breach in their Smartphone system, in which an unauthorized user has gained access and attempted to modify and delete files.

Attack name/description	Unauthorized Smartphone Access
Threat/probable threat agents	Unauthorized user attempting to gain access to the system and/or malicious code
Known or possible vulnerabilities	Weak passwords, broken authentication, insecure data storage, insecure network transmission
Likely precursor activities or indicators	Unusual network traffic, login attempts from unrecognized IP addresses, unusual account activity
Likely attack activities or indicators of attack in progress	Unauthorized access, attempted modification or deletion of files, attempted access to confidential information
Information assets at risk from this attack	Confidential information, customer data, financial data, etc.
Damage or loss to information assets likely from this attack	Theft or destruction of confidential information, financial loss, reputational damage

Other assets at risk from this attack	Smartphone system, network infrastructure, other connected devices
Damage or loss to other assets likely from this attack	System disruption, network downtime, data corruption
Immediate actions indicated when this attack is under way	Isolate the affected system, identify affected assets, and assess the extent of damage, block access to the affected system and other connected systems, notify relevant stakeholders
Follow-up actions after this attack was successfully executed	Investigate the attack, identify the root cause, develop and implement remedial measures, ensure all affected systems are patched and up to date, monitor the system for further suspicious activity.

5.3.5 Scenario 5: Unauthorized Access of Cisco Routers And Switches

ACME Corp discovers their Cisco Routers and Switches system has been infiltrated by an unauthorized user, who has made attempts to alter, delete, and access confidential information.

Attack name/description	Unauthorized Access of Cisco Routers and Switches
Threat/probable threat agents	Hackers, malicious insiders
Known or possible vulnerabilities	Weak passwords, vulnerable system components, unpatched software
Likely precursor activities or indicators	Unusual network traffic, unauthorized access attempts, malicious emails
Likely attack activities or indicators of attack in progress	Unauthorized access, changes to system configurations, data exfiltration, malicious code downloads
Information assets at risk from this attack	Confidential information, user credentials, financial data
Damage or loss to information assets likely from this attack	Corruption or destruction of data, unauthorized access to confidential information, financial loss
Other assets at risk from this attack	Network performance, reputation, customer confidence
Damage or loss to other assets likely from this attack	Performance degradation, reputational damage, customer loss
Immediate actions indicated when this attack is under way	Isolate affected system, implement intrusion prevention systems, monitor network traffic
Follow-up actions after this attack was successfully executed	Restore data from backup, audit system logs, patch vulnerable components, update security policies.

5.4 Incident Response Form

CONTACT INFORMATION FOR THIS INCIDENT	
Name:	
Title:	
Program Office	
Work Phone:	
Mobile Phone:	
Email address:	
Fax Number:	

INCIDENT DESCRIPTION

Provide a brief description:

IMPACT/POTENTIAL IMPACT CHECK ALL THE FOLLOWING THAT APPLY TO THIS INCIDENT

☐ Loss / Compromise of Data
☐ Damage to Systems
☐ System Downtime
☐ Financial Loss
☐ Other Organizations’ Systems Affected
☐ Damage to the Integrity or Delivery of Critical Goods, Services, or Information
☐ Unknown at this time

Provide a brief description:

SENSITIVITY OF DATA/INFORMATION INVOLVED

SENSITIVITY OF DATA

CATEGORY	EXAMPLE
Public	This information has been approved for public release by department managers and does not pose any risk to ACME Corp, its customers, or its business partners. Examples of this information can include marketing brochures and material posted to ACME Corp web pages. In order for the information to be disclosed to the public, it must have this label, have the permission of the information Owner, or be a long-standing practice of public distribution.
Internal Use Only	ACME Corp and affiliated organizations such as business partners should only disclose this type of information to outsiders with advance permission from the information owner, as unauthorized disclosure of it may be against laws and regulations, or may cause problems for ACME Corp, its customers, or its business partners.
Restricted/Confidential (Privacy Violation)	This information is confidential and should only be shared with those who have a legitimate business need for access. Unauthorized disclosure of this information could be illegal or cause serious problems for the company and its stakeholders, so access should be approved by the information owner. Examples of such information include customer account information, performance evaluations, citizen data, and legal information.

Select the appropriate information category:

☐ Public
☐ Internal Use Only
☐ Restricted / Confidential (Privacy violation)
☐ Unknown / Other – please describe:

Provide a brief description of data that was compromised:

WHO ELSE HAS BEEN NOTIFIED	
Provide Person and Title:	
WHAT STEPS HAVE BEEN TAKEN SO FAR	
☐ No action taken ☐ System Disconnected from Production Network ☐ Updated virus definitions & scanned system	☐ Restored backup from ASR ☐ Log files examined (saved & secured) ☐ Other – please describe:
Provide a brief description:	
INCIDENT DETAILS	
Date and Time Incident was discovered:	
Has the incident been resolved?	
Network Location of the affected systems	
Number of Networks affected by incident:	
Approximate number of systems affected:	
Approximate number of users:	
Are non-ACME systems, such as business partners, affected by the incident? (Y or N – if yes, please describe)	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	

5.5 Personnel Contact List

ACME CORP DRP KEY PERSONNEL		
Key Personnel	**Contact Information**	
DRP Director	Work	
CEO	Home	
	Cellular	
	Email	
DRP Director – Alternate	Work	
CIO/CISO	Home	
	Cellular	
	Email	
DRP Coordinator	Work	
Security Manager 1	Home	
	Cellular	
	Email	
DRP Coordinator – Alternate	Work	
Security Manager 1	Home	

	Cellular	
	Email	
DRP Team – Team Lead	Work	
IT Manager	Home	
	Cellular	
	Email	
DRP Team – Team Members	Work	
IT Technicians	Home	
System Administrators	Cellular	
Network Administrators	Email	

5.6 Vendor Contact List

VENDOR	EMERGENCY PHONE	CONTACT NAME	RESPONSE TIME	ONSITE TIME
Microsoft Azure	1-800-642-7676	Microsoft Azure Support		
Red Hat Enterprise Linux	1-888-REDHAT-1	Red Hat Enterprise Linux Support		
Cisco	1-800-553-2447	Cisco Support		

5.7 Alternate Processing Procedures

1. **Manual Processing**: ACME Corp will develop a manual process to continue some processing of information that would normally be done by the affected system. This manual process will include the following steps:
   a. Identify the affected system and the type of information it stores.
   b. Identify the manual processes that can be used to continue processing of the information.
   c. Develop a plan for implementing the manual processes.
   d. Train personnel on the manual processes.
   e. Test the manual processes to ensure they are functioning correctly.
   f. Document the manual processes and update them as needed.
2. **Technical Processing**: ACME Corp will also develop a technical process to continue some processing of information that would normally be done by the affected system. This technical process will include the following steps:
   a. Identify the affected system and the type of information it stores.
   b. Identify the technical processes that can be used to continue processing of the information.
   c. Develop a plan for implementing the technical processes.
   d. Train personnel on the technical processes.
   e. Test the technical processes to ensure they are functioning correctly.
   f. Document the technical processes and update them as needed.
   g. Ensure the technical processes are secure and compliant with applicable laws and regulations.

3. **Queuing of Data Input**: ACME Corp will also develop a process to queue data input in the event of a system failure. This process will include the following steps:
   a. Identify the affected system and the type of data it stores.
   b. Develop a plan for queuing data input in the event of a system failure.
   c. Train personnel on the queuing process.
   d. Test the queuing process to ensure it is functioning correctly.
   e. Document the queuing process and update it as needed.
   f. Ensure the queuing process is secure and compliant with applicable laws and regulations.

5.8 System Validation Test Plan

Data Integrity Testing

PROCEDURE	EXPECTED RESULTS	ACTUAL RESULTS	SUCCESSFUL?	PERFORMED BY
Check File Integrity Check the integrity of all files on the system and compare the checksums against known values.	File integrity should match the known values.			IT Technician
Verify Data Integrity Verify that the data is accurate and up to date by comparing it to the original source. Expected Result: Data should match the original source.	Data should match the original source.			IT Manager
Perform Data Comparison Compare the data to other sources of information to ensure that the data is consistent and complete. Expected Result: Data should be consistent and complete.	Data should be consistent and complete.			Security Manager

Functionality Testing

PROCEDURE	EXPECTED RESULTS	ACTUAL RESULTS	SUCCESSFUL?	PERFORMED BY
Verify application availability Check whether the application is available to users. This can be done by checking logs, monitoring response time, and other appropriate tests.	The application is available to users and is running without any errors.			IT Manager and IT Technician
Verify access control Test whether the access control system is configured correctly. This can be done by logging in with different user accounts and ensuring that access is being granted and denied as expected.	Access is granted and denied as expected.			Security Manager and Security Technician

Verify data integrity Run checksums or other appropriate tests to ensure that the data stored in the system is not modified or corrupted.	Data is intact and not corrupted.			IT Manager and IT Technician
Verify performance Measure the performance of the system under various scenarios. This can be done by running automated scripts to perform tasks and measuring the response time.	System performance is within expected tolerances.			System Administrator and Network Administrator
Verify security features Test the security features of the system such as encryption, authentication, authorization, and audit trails.	Security features are configured correctly and operating as expected.			Security Manager and Security Technician
Verify user acceptance Test the system with actual users to ensure that the system meets their needs and expectations.	System meets user needs and expectations.			IT Manager and IT Technician
Verify system backups Verify that backups of the system are being performed as expected and that they are restorable.	Backups are being performed as expected and are restorable.			System Administrator and Network Administrator
Verify system maintenance Test that the system is being maintained and updated as expected.	System is being maintained and updated as expected.			IT Manager and IT Technician
Verify system monitoring Verify that the system is being monitored as expected and that any alerts are being responded to in a timely manner.	System is being monitored as expected and any alerts are being responded to in a timely manner.			System Administrator and Network Administrator

Security Testing

PROCEDURE	EXPECTED RESULTS	ACTUAL RESULTS	SUCCESSFUL?	PERFORMED BY
Penetration Testing Test the scope and effectiveness of the security infrastructure by attempting to breach it using common attack vectors.	No successful breaches of the security infrastructure.			Security Manager and Security Technician
Vulnerability Scanning Scan the security infrastructure to identify any potential vulnerabilities.	No vulnerabilities identified.			Security Manager and Security Technician
Security Audits Perform periodic audits of the security infrastructure to ensure it is configured correctly and up to date.	System is configured correctly and up to date.			Security Manager and Security Technician

5.9 Hardware And Software Inventory

Hardware Inventory

ITEM	MODEL	SERIAL NUMBER	LOCATION	APPLICATION
Server 1			DC	Active Directory Domain Services
Server 2			DC	Firewalls and Application Layer Proxies
Switch 1			DC	Network Switching
Switch 2			DC	Network Switching
Router 1			DC	Routing
Router 2			DC	Routing

Software Inventory

SOFTWARE	VERSION	LICENSE KEY	APPLICATION
Windows Server			User Management
Red Hat Enterprise Linux			Firewalls and Application Layer Proxies
Microsoft Azure			Data Storage and Access
Cisco IOS			Network Switching

5.10 Interconnections Table

System Name	Connection Type	Information Transferred	Contact Person
Windows 3.1	Network	User Management	CIO/CISO
Windows Server 2000	Network	User Management	CIO/CISO
Microsoft Azure	Cloud	Storing and Access of Data	CIO/CISO
Linux Kernel 2.6	Network	Firewalls and Application Layer Proxies	System Administrators
Smartphones	Network	Data Access	IT Managers
Cisco Routers and Switches	Network	Network Management	Network Administrators

5.11 Test and Maintenance Schedule

1. **Quarterly Review:**
   a. Review and update the DRP, including notification procedures, system recovery, internal and external connectivity, and reconstitution procedures.
2. **Annual Functional Test:**
   a. Conduct a full functional test of the DRP, including notification procedures, system recovery, internal and external connectivity, and reconstitution procedures.
   b. Test should be facilitated by an outside or impartial observer.
   c. Test plan and procedures should be developed prior to the functional test.
   d. Results of the test should be documented in an After-Action Report.
   e. Lessons Learned should be developed for updating information in the DRP.
3. **Annual Disaster Recovery Exercise:**
   a. Conduct a full disaster recovery exercise, including notification procedures, system recovery, internal and external connectivity, and reconstitution procedures.
   b. Exercise should be facilitated by an outside or impartial observer.

c. Exercise plan and procedures should be developed prior to the exercise.
d. Results of the exercise should be documented in an After-Action Report.
e. Lessons Learned should be developed for updating information in the DRP.

5.12 Business Restoration Checklist

Date: ____ **Yes = Complete**

No = Requires Action

Completed By: ____ **N/A = Not Applicable**

DOES YOUR PLAN HAVE PROVISIONS FOR?	YES	NO	N/A
A decision-making process for implementing business restoration actions?			
Funding for restoration activities and formalizing a review of the plan to assure that adequate monies have been allocated to sustaining operations?			
Documenting building permit and facility certification procedures?			
Obtaining building permits or zoning changes before restoration is needed or begins?			
A listing identifying critical machinery, software, materials and vendors?			
Developing and documenting a list of procedures for quick procurement of machinery, equipment, software, etc.?			
Documenting specialized production facilities and reconstruction plans?			
Reviewing considerations that may increase construction time?			
Considering options that would minimize the time needed to reach pre-disaster operational capacity?			
Outlining plans to return to pre-disaster sales and revenues?			
Identifying and preparing potential relocation sites?			
Assessing facility hazards to ensure safety of all personnel?			
Establishing security at the damaged facility?			
Securing the site: protecting undamaged property, controlling facility access, reactivating facility protection systems, etc.?			
Notifying all employees, vendors, customers, and governmental agencies regarding the restorations plans?			
Conducting employee briefings?			
Documenting the decisions made, the damage costs, and the repairs?			
Taking inventory of all damages?			
Implementing a procedure for restoring damaged equipment and processes?			

Identify corrective action for all NO responses

ACTION NEEDED	COMPLETED	DATE

5.13 Business Restoration Timetables

Critical Business Units and Return Time Objectives (RTO)

Time Period (<24 Hours)	Time Period (2-4 Days)	Time Period (1 Week)

Critical Business Function (CBF) Staff Requirements and Locations

Recovery Team or CBF	Alternate Site		Command Center	Employee Homes	Other Site
	Immediate RTO	Short Term RTO			
CBF/TEAM 1					
Function					
Function					
CBF/TEAM 2					
Function					
Function					
CBF/TEAM 3					
Function					
Function					
CBF/TEAM 4					
Function					
Function					
TOTALS	0	0	0	0	0