Devin Lachman
Mock Acme LLC Primary Responsibilities for System Administrators

1. **Overview**
   This document proposes the responsibilities and duties of Acme LLC system administrators and promotes practices that create an effective system administration team that strives to achieve company goals and objectives.

2. **Purpose**
   The purpose of this document is to delineate the responsibilities of Acme LLC's System Administration Team.

3. **Scope**
   This document applies to all administrators working under Acme LLC’s System Administration Team.

4. **Policy**
   4.1.1 Each department or employee who is an Information Resource Owner must have documented procedures for approving elevated access for Acme system administrators.
   4.1.2 In the case where the system administrator’s role or responsibility changes, the Elevated access must be evaluated and, if necessary, updated or removed according to the transfer of duties.

System Administration Policy

4.2.1 Acme System Administrators must:

a. Restrict their use of elevated access for official company purposes that fall into the system administration role, responsibilities, and purpose for which the elevated access was granted.

b. Never use their elevated privilege for purposes outside of the scope of company purposes

c. Never expose disclosed information to unauthorized personnel

d. Never share their own personal login credentials

e. Follow Acme Password Configuration guidelines

f. Never give themselves or another employee access to Information Systems without formally documenting and authorizing access.

g. Take steps to ensure compliance with all hardware and software license agreements

h. Fulfill the responsibilities that accompany elevated access as well as take measures to ensure the protection, confidentiality, integrity, and availability of information resources.

Responsibilities

4.3.1 The responsibilities of Acme's system administration team include:

a. System Administrators must manage the physical and logical access control to a network. They must control users' access to a network through managing the three major elements of safe managing a network which:
   - Authentication - administrators must verify a user's credentials before granting them access to secure resources found on a network or system.
   - Authorization - the administration team must dictate what employees can and cannot do with network resources. Administrators must also dictate the authorization of an employee entering specific locations within Acme's workplace through the use of keycards.
   - Accounting - The administration team must keep an accounting system that logs users' access and activities within the network and keeps records that will be audited in the future by either an internal or external entity to ensure compliance.

   To help manage the complexity of a network's authentication, authorization, and accounting, a NAC (Network Access Control) system will be managed by system administrators. Administrators will create network policies to delineate the level and type of access granted to devices.

b. Management of network traffic including the use of a proxy network, network usage, and network space.

c. The installation, configuration, management, and disposal of system hardware and system software.

d. Manage all file servers and ensure that drives are redundant and drives are completely backed up every Friday night. Monthly backups are completed at the end of each month and held for a 12-month period.

e. Manage all camera recordings and ensure backups onto company servers every Friday night. Monthly backups are completed at the end of each and all backups are held for 6 months. In the event that camera recordings are necessary for investigative purposes, the camera footage in question will be held for as long as necessary.

f. Administer the recovery process in the event that data within the internal network must be recovered.

g. Ensure the compliance of Acme employees by performing audits of users' logs, emails, and network traffic. DigiStructure will handle all Spam emails and filter them throughout its partnership with Acme LLC.

Frequency of Responsibilities

Administration Task	Frequency
System Hardware	
● Installation/disposal of hardware	When Required
● Configuration of hardware	When Required
● Maintenance and repair of hardware	When Required

System Software	
● Installation/disposal of software	When Required
● Configuration of software and operating systems	When Required
● Maintenance and patching of software	When Required
● License management of software	When Required
System Resources	
● Monitor system performance	Daily
● Monitor network usage	Daily
● Manage storage space	Daily
Data Backups	
● Files, User Logs, Emails (Back Up)	Weekly
● Camera Recording Back-Up	Weekly
● Data Recovery	When Required

6. Policy Compliance

5.1.1 Compliance Measures

The Acme LLC's System Administration Team will verify employee compliance through various methods, including internal and external audits, network management and monitoring tools, and anonymous employee reports.

7. Related Standards, Policies and Processes

- Acceptable Use Policy
- Email Policy
- Password Protection Policy
- Incident Response Policy
- Clean Desk Policy
- Anti-Virus Guidelines.

8. Revision History

Date of Change	Responsible	Summary of Change
November 2022	DigiStructure CSO Devin Lachman	Creation of Policy

Employee Training Policy

This policy is created by DigiStructuce LLC for the use of Acme.

1. **Overview**
   For the interest of Acme and for the benefit of employees, all incoming new employees will go through mandatory training that will provide cyber security knowledge and risk management skills.

2. **Purpose**
   This policy is to outline the basic skills and rules needed for an entry position at Acme LLC. These rules are in place to protect the employees and Acme LLC, while also continuing the workflow occurring at Acme LLC office locations.

3. **Scope**
   This policy applies to all new hires at Acme LLC. However, the practices and policies mentioned must also be held by any employee under Acme LLC.

4. **Policy**
   4.1.1 All new employees at Acme LLC must review the Acceptable Use Policy, Email Policy, Password Protection Policy, Incident Response Policy, Clean Desk Policy, and the Anti-Virus Guidelines.
   4.1.2 All new employees must go through mandatory security awareness training provided by DigiStructure. This will include labs and video lectures that will take place within the first few days of employment.

5. **Policy Compliance**
   5.1.1 Compliance Measures
   The Acme LLC's System Administration Team will verify employee compliance through various methods, including internal and external audits, network management and monitoring tools, and through anonymous employee reports.

6. **Related Standards, Policies, and Processes**
   - Acceptable Use Policy
   - Email Policy
   - Password Protection Policy
   - Incident Response Policy
   - Clean Desk Policy
   - Anti-Virus Guidelines.

7. **Revision History**

Date of Change	**Responsible**	**Summary of Change**
November 2022	DigiStructure CSO Devin Lachman	Creation of Policy

Acceptable Use Policy

This policy is created by DigiStructuce LLC for the use of Acme.

1. **Overview**
   Acme is committed to protecting employees, partners, and companies from illegal or damaging actions by individuals, either knowingly or unknowingly.

2. **Purpose**
   The purpose of this policy is to outline the acceptable use of computer equipment and other electronics on company-specified property. The rules are set in place to protect employees and Acme. All property provided by Acme which includes Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, mobile devices, software, operating systems, storage media, and network accounts providing electronic mail must be used for business purposes, serving the interest of Acme. Inappropriate use of Acme devices can lead to cyber security risk which includes data breaches, viruses, and ransomware.

3. **Scope**
   This policy applies to all Acme-provided devices and all devices that conduct Acme business or devices that interact with internal networks and business systems, whether owned or leased by Acme employees. All Acme employees are required to follow these guidelines and practice good judgment regarding company information, network resources, and electronic devices, provided by Acme or interacting with Acme's internal network and business systems.

4. **Policy**
   4.1.1 Acme proprietary information whether the device is owned or leased, by Acme LLC, the employee, or a third party remains the sole property of Acme LLC. Employees must ensure that both through legal and technical means, proprietary information is in accordance with the Data Protection Standard.
   4.1.2 The sharing of Acme LLC's proprietary information may only be done as authorized and if necessary fulfills assigned job duties.
   4.1.3 All devices with Acme's network will be monitored by authorized individuals within Acme LLC for security purposes. This may include the monitoring of equipment, emails, and network traffic.
   4.1.4 All employees have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Acme LLC's proprietary information.
   4.1.5 Acme LLC reserves the right to audit networks and systems on a periodic basis to ensure compliance with the policies in place.

5. **Policy Compliance**
   5.1.1 Compliance Measures

The Acme LLC's System Administration Team will verify employee compliance through various methods, including internal and external audits, network management and monitoring tools, and anonymous employee reports.

6. Revision History

Date of Change	Responsible	Summary of Change
November 2022	DigiStructure CSO Devin Lachman	Creation of Policy

Email Policy

This policy is created by DigiStructuce LLC for the use of Acme.

1. **Overview**
   Electronic email is an integral tool for many industries and is often the primary communication and awareness method within an organization. At the same time, misuse of email can pose many legal, privacy, and security risks, thus it's important for users to understand the appropriate use of electronic communications.

2. **Purpose**
   The purpose of this email policy is to ensure the proper use of the email system and make users aware of what is an acceptable and unacceptable use of Acme's email system.

3. **Scope**
   This policy applies to all employees of Acme LLC and affiliates who fall under Acme's emailing system.

4. **Policy**
   4.1.1 Acme email accounts should primarily be used for Acme business-related purposes.
   4.1.2 Employees are prohibited from using Acme email accounts to contact third-party emailing services. Employees are prohibited from forwarding confidential information to a third-party email address.
   4.1.3 All email addresses provided by Acme LLC are identified as business records and are retained by Acme LLC.
   4.1.4 All email policies provided by Acme should have a secure password.
   4.1.5 Acme employees should have no expectation of privacy when it comes to anything stored, sent, or received on Acme's emailing system. Acme may monitor messages stored, sent, and received, without prior notice from Acme LLC,

5. **Policy Compliance**
   5.1.1 Compliance Measures
   The Acme LLC's System Administration Team will verify employee compliance through various methods, including internal and external audits, network management and monitoring tools, and anonymous employee reports.

6. **Related Standards, Policies, and Processes**
   - Acceptable Use Policy

7. **Revision History**

Date of Change	**Responsible**	**Summary of Change**

November 2022	DigiStructure CSO Devin Lachman	Creation of Policy

Clean Desk Policy

This policy is created by DigiStructuce LLC for the use of Acme.

1. **Overview**
   A clean desk policy is necessary for all employees to comply with as it is an important tool to ensure that confidential/sensitive information is not stolen. The clean desk policy is a risk mitigation tool to protect sensitive information while making employees aware of how information should be handled.

2. **Purpose**
   The purpose of this policy is to dictate the requirements for maintaining a clean desk while also enforcing the handling of sensitive information about employees or about Acme, its clients, customers, or vendors.

3. **Scope**
   The scope of this policy includes all Acme employees who are responsible for any account, device, or document provided by Acme LLC and located within Acme LLC facilities and within Acme LLC's network.

4. **Policy**
   4.1.1 Employees are required to ensure the protection of sensitive information in their workspace at the end of the work day or when leaving their desks.
   4.1.2 Employees are required to lock their workstations and turn off their monitors when leaving their desks.
   4.1.3 At the end of the day employee workstations must be turned off.
   4.1.4 Employee file cabinets must be locked by the end of the work day. When dealing with sensitive information, employees must lock sensitive documents in the filing cabinet when not in use.
   4.1.5 If sensitive Acme documents are to be disposed of, they must be shredded and disposed of.
   4.1.6 Any sensitive information written on whiteboards must be erased.
   4.1.7 Passwords must not be written on sticky notes and placed on the desk or in any other accessible location.

5. **Policy Compliance**
   5.1.1 Acme LLC's System Administration Team will monitor employee compliance with this policy through various methods which include periodic walk-throughs of office spaces, video monitoring, and anonymous employee reports.

6. **Revision History**

Date of Change	**Responsible**	**Summary of Change**
November 2022	DigiStructure CSO Devin Lachman	Creation of Policy

Password Protection Policy

This policy is created by DigiStructuce LLC for the use of Acme.

1. **Overview**
   Passwords are an integral part of mitigating risk and strengthening computer security. Weak or compromised passwords can lead to data breaches, unauthorized access to sensitive data, or exploitation of resources. All Acme employees are responsible for taking the steps to secure their passwords.

2. **Purpose**
   The purpose of the Password Protection Policy is to create a standard that Acme's employees can use to create secure passwords for the protection of all word-related devices, and documents. This policy also establishes what should be protected under a password.

3. **Scope**
   The scope of this policy includes all Acme employees who are responsible for any account, device, or document provided by Acme LLC and located within Acme LLC facilities and within Acme LLC's network.

4. **Policy**
   4.1.1 All user-level and system-level passwords must comply with Acme's Password Construction Guidelines.
   4.1.2 Employees must use separate and unique passwords for each work-related account. Employees are prohibited from replicating passwords, and from using passwords that are related to employee personal accounts.
   4.1.3 Multi-factor authentication is required for any account considered a privileged account.
   4.1.4 All employees will be required to periodically change their passwords. Passwords must be unique enough from previous passwords and employees will be prohibited from reusing passwords.
   4.1.5 Employees must not share passwords with anyone, including supervisors and coworkers.
   4.1.6 Employees must not use the "Remember Password" feature on applications like web browsers.
   4.1.7 Individuals who believe their password was compromised must report the incident to Acme's Infosec Tea, and change all relevant passwords.

5. **Policy Compliance**
   5.1.1 Compliance Measures
   The Acme LLC's System Administration Team will verify employee compliance through various methods, including internal and external audits, network management and monitoring tools, and anonymous employee reports. Acme LLC will also give

recommendations to strengthen passwords when employees are creating passwords for Acme's emailing services and other services provided by Acme.

6. Revision History

Date of Change	Responsible	Summary of Change
November 2022	DigiStructure CSO Devin Lachman	Creation of Policy

Incident Response Policy

This policy is created by DigiStructuce LLC for the use of Acme.

1. **Overview**

   Incident Response is a great tool to mitigate any additional harm from taking place within a company. An incident is an event that could lead to loss or disrupt an organization's operations. Employees should practice incident management as well as risk management.

2. **Purpose**

   The purpose of the Incident Response Policy is to make Acme employees aware of the procedures to conduct when an incident takes place. All employees are responsible for reporting incidents to Acme's System Administration Team. The goal of this policy and the goal of all Acme employees is to contain an incident and prevent it from turning into a disaster.

3. **Scope**

   The scope of this policy includes all Acme employees who are responsible for any account, device, or document provided by Acme LLC and located within Acme LLC facilities and within Acme LLC's network.

4. **Policy**

   4.1.1 In the event that an incident takes place, the individual employee must inform Acme's System Administration Team.
   4.1.2 The incident must also be documented by Acme LLC's System Administration Team using Acme LLC's Cyber Security Incident Recovery Document.
   4.1.3 The incident recovery process should also be documented for future use.
   4.1.4 The Acme System Administration Team should confirm the theft, breach, or exposure of Acme LLCs' data.
   4.1.5 If theft, breach, or exposure of Acme LLCs' data has occurred, the System Administration Team should immediately contact the authorities and Acme LLCs' legal team.

5. **Policy Compliance**

   5.1.1 Compliance Measures
   The Acme LLC's System Administration Team will verify employee compliance through various methods, including internal and external audits, network management and monitoring tools, and through anonymous employee reports.

6. **Revision History**

Date of Change	Responsible	Summary of Change
November 2022	DigiStructure CSO Devin Lachman	Creation of Policy

Termination Policy

This policy is created by DigiStructuce LLC for the use of Acme.

1. **Overview**
   The termination policy indicates the conduct which permits the termination of the employee. This policy is set in place to emphasize the importance of following the policy and the prohibited actions that lead to the termination of an individual. The policy also standardized the procedures for voluntary and involuntary dismissal from Acme LLC.

2. **Purpose**
   The purpose of the termination policy is to set the procedures for an individual's voluntary or involuntary dismissal.

3. **Scope**
   The scope of this policy includes all Acme employees who are responsible for any account, device, or document provided by Acme LLC and located within Acme LLC facilities and within Acme LLC's network.

4. **Policy**
   4.1.1 Failure to comply with Acme Policies to the degree to which Acme LLC data has been leaked or quantifiable damage has been done to the company will result in the termination of an individual or individuals.
   4.1.2 We highly suggest employees deciding to go through the voluntary termination process, whether it be through resignation or retirement, give Acme LLC. at least two weeks' notice, in order to prepare and ensure a smooth transition.
   4.1.3 Employees who voluntarily terminate their employment must hand in an Acme Termination Form
   4.1.4 In the case of involuntary termination, the administrator must audit the individual's activities that occurred during the past 7 days before termination.
   4.1.5 All involuntary terminations must include evidence explaining the termination. This evidence must be clearly documented within Acme's Termination Form. All evidence of termination must be held by Acme's HR department and used in cases where the individual pursues legal action for wrongful termination. Evidence must also be presented to the individual.

5. **Policy Compliance**
   5.1.1 Compliance Measures
   The Acme LLC's System Administration Team will verify employee compliance through various methods, including internal and external audits, network management and monitoring tools, and anonymous employee reports.

6. **Revision History**

Date of Change	Responsible	Summary of Change

November 2022	DigiStructure CSO Devin Lachman	Creation of Policy

Anti-Virus Guidelines

These guidelines are created by DigiStructuce LLC for the use of Acme.

Recommended processes to prevent virus problems for Acme employees.

- Always run the corporate standard, supported anti-virus software provided to you by Acme LLC. This software will already be available on all devices provided by Acme LLC. Acme employees are prohibited from installing any other antivirus software onto company devices. All antivirus software should be updated frequently.
- Employees should never open any files or links attached to emails from unknown, or untrustworthy partners. All untrustworthy emails should be deleted from your company-provided emailing service and then removed from your Trash.
- Employees should not use company-provided email addresses for personal use. All emails are monitored by Acme's Network Administration Team.
- Employees are prohibited from downloading any software onto Acme devices.

Password Construction Guidelines

These guidelines are created by DigiStructuce LLC for the use of Acme.

Recommended for the security of Acme-provided accounts and devices.

- At least one number (Example: 1 2 3)
- At least one uppercase letter (Example: A B C)
- At least one lowercase letter (Example: a b c)
- One of these symbols:! @ # $ % & _ -
- Between 10 and 30 characters
- Passwords may not repeat any character more than twice in a row.
- Passwords may not include first or last names.

Entry and Exit Policy

This policy is created by DigiStructuce LLC for the use of Acme.

1. **Overview**
   Physical security is one of the most important aspects when it comes to protecting data within Acme LLC. Physical security includes the use of cameras, keycards, keycard readers, and an organizational structure to prevent the leakage of information within the organization.

2. **Purpose**
   The purpose of this policy is the address the conduct of which an employee must act. In this case, employees must always have their key cards with them.

3. **Scope**
   The scope of this policy includes all Acme employees who are responsible for any account, device, or document provided by Acme LLC and located within Acme LLC facilities and within Acme LLC's network.

4. **Policy**
   4.1.1 Employees must have their company keycards on them at all times. The keycards must have the individual's photo and name on the front of the card. The picture on the key card must not be obscured or damaged.
   4.1.2 Upon entry into the office, all employees must use their keycards, and must only allow others to use the door if they are permitted into the office.
   4.1.3 Anyone who loses a key card must report it to the administration team in order for them to deactivate the card and give individual new ones.
   4.1.4 You may not give your keycard to other individuals including co-workers.

5. **Policy Compliance**
   5.1.1 Compliance Measures
   The Acme LLC's System Administration Team will verify employee compliance through various methods, including internal and external audits, network management and monitoring tools, and anonymous employee reports.

6. **Revision History**

Date of Change	Responsible	Summary of Change
November 2022	DigiStructure CSO Devin Lachman	Creation of Policy

Acme LLC Cyber Security Incident Recovery Form

Incident Name:

Name of persons performing forensics on systems:

Was the root cause identified? YES NO
Describe:

Steps performed for system recovery:

Incident Containment Form by:

Date and Time of Form: ____________________

Title:

Signature: