Acme Corporation

123 Business Way

Retail Park

BD33 K33

Tel: 0117-01110111

Email: acmesupport@acme.com

Acme Corporation

Information Security Policy

Table of Contents

Introduction

Background

Acme corporation is a public facing company, we handle personal and pubic data. Therefore, it is important to outlay clean and concise security information to keep all employees, the business and public safe.

Target Audience

This document is intended for all employees, staff or onsite visitors to the premises named on the front page (Acme Corporation).

Scope

The aim of Acme Corporation is simple, to provide great services whilst complying with the industry's law's and standards. We aim to keep all staff informed with an ability to get the help and education they need for any security concerns.

- All staff are in scope of the policies in this document.

Availability	Information is available and will be delivered then accessible by the correct people
Integrity	Systems will be up to date and updated to the latest editions for software
Reliability	Any older systems replaced with new and all methods standardised.

Objectives

The objectives of the Acme Company's policies are to maintain and secure confidentiality with information across the whole organization, including but not limited to Servers, Computers, Phones, Networks.

- All members of staff to be trained in the latest security measures, ensuring you are accountable and fully compliant with the latest security guideline's.
- Working closely with third party security bodies to improve overall security through innovation and open networking.
- Protection information, databases and private data with higher encryption methods.
- Training and retraining staff to help them better understand the need for better security measures.
- Protecting staff whilst making them more aware of them responsibility's whilst ensure they are also aware of their role in the business.

Roles and Responsibilities

Chief Executive

All responsibility for the company resides with the Chief Executive. The responsibility is discharged through the designated roles of the Head of Security in accordance with policies already stated in the last annual security review.

Head of Security

The head of security was appointed to managed the overall security and managed training of all staff in the organization. The head of security can bestow powers of security to other trained staff members in cases of data breech or other business need.

Appointed Staff from Head of Security

Your roles will be designated at such times your services are needed. You will have previously passed the in-house new security training policies to be eligible for the role.

All Staff

All staff are responsible for personal and business security, therefor must comply and complexly understand the importance of being trained and meeting the security guidelines. In particular, related to our business, all staff are to undertake mandatory security training. It's also important to under the below core key concepts.

- How is data handled. How is data transmitted across the business?
- What procedures are in place to protect you, what tools do you have available to utilize.
- How do you report a breech or security concern with the business?
- Your understanding in when and how to reach the head of security or an appointed security offer.

Shared Responsibility	Observe and Report	Think Cyber
Be Vigilant	Be Resilient	Team Player
Work Safe	Don't Take Risk's	Be Aware

Policies

Data Security

Employees

All employees must complete the training security program and sign the acceptable usage policy agreements.

- If you find an unidentified person on the premises, to repot them straight away.
- To keep all personal devices away from work computers, including USB, mobile charging or anything that will interface with another device in the office.
- To be vigilant and safe in how you handle data.
- To change your password at least once every 2 weeks with 12 characters' long and a mix of alpha numeric character's (abcdefgABCDEFG12345…)
- Workspaces to be kept clean with minimal personal items.

Equipment

All equipment will be tested and then given an ID, DATE and SERIAL ID to mark them as currently tested to be known safe and bug free.

- All equipment used or taken of the premises to be logged and recorded.
- Any internal or external access only to be used with the in-house company VPN.
- You will be given new ID RSA tag for two-factor authentication for logging in.
- Any equipment found to be faulty must be immediately reported and logged.

Acceptable Usage

Access control

Access will be restricted to only a few individuals who will need to verify certain actions within the business moving forward.

Applications Access

Applications will need to use two-factor authentication to login to workstations and VPN. Only authorized users will have access and be allowed in.

Risk Assessment

You are to remain clean and diligent at all times, if you suspect any risk in the workplace to report it immediately

Security Incident Management

Incident management will apply to all security trained staff who have passed the in-house security exam, they will be the first point of call and respond immediately to any security incidents.

Secure incidents that include;

- Data Theft
- Data Loss
- Attacks or Attempts to gain access to internal networks
- Unwanted disruption of services
- Human error (wrong data entry etc.)
- Unauthorized access of systems
- Unauthorized access of work equipment
- Non-compliance with company security policies and procedures.
- Risk to any person's health or data

Logical Security Measures

Passwords

All passwords are to be wiped and reset with newer stronger ones.

Passwords are to meet the minimum requirements' below.

- Use a phase phrase or character's longer than 12 character's long
- The passwords MUST contain 1 upper and 1 special character [!"£!^&$%]
- All passwords will be changed every 180 days
- Old passwords may not be reused

Software

Software will be updated every Friday night unless no patches are available.

All software licenced will need to be logged in with two-factor authentication. Note: we are now operating a logging software to track all movement's and transactions across the business.

If you receive any spam email, to report it and send a copy to the Head of Security to be address and added to our internal filters.

End point

All end points or any accessible port of entry to any data in the organization is to be logged. This is largely automatic due to the newer security systems and IDS (Intrusion detection system) we have.

Any end points you find not already disclosed must be reported immediately.

Patch Management

All software within the business with be routinely updated.

Patches will happen every Friday evening by the night staff, to pick up early on any incidents and also have more time available to fix any new issue's that may arise.

Patches will only be handled by the in-house IT team and will not be accessible for staff.

Legislation references

- The Data Protection Act (2018)
- The General Data Protection Regulation
- The Copyright, Designs and Patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Freedom of Information Act (2000)
- Health & Social Care Act (2012)

Conclusion

Acme Company considers all of its staff to be a vital cog in the overall impact fullness of the business as whole. We are committed to keeping your best interest at heart whilst maintaining a publicly secure figure that can be trusted and respected.

Thank you for taking the time to read and adhere to this document.

Richard Jones

Mosse Cyber Security
User id: eoEPcxbizUSJ9yEZIWdLslF4Puj2