ACME AG

Information Security Policy

VERSION: 1.7

ACME AG^{TM} 22.12.2014

Authors

Andreas Ntaflos (Nta1) e0326302

Andreas Ntaflos (Nta2) e1328682

Christoph Seidl (Sei) e0427434

Contents

1 Document Revision History

Revision	Date	Author	Status and Description
1.7	22.12.2014	Nta1	Change of the Software Installation Policy
1.6	22.11.2014	Nta1	Change of the Server Security Policy
1.5	22.10.2014	Nta2	Change of the Responibilities for Data Security
1.4	22.09.2014	Sei	Change of the Clean Desk Policy
1.3	22.08.2014	Sei	Change of the Roles
1.2	22.07.2014	Sei	Change of the Backup Policy
1.1	22.06.2014	Nta2	Change of the Clean Desk Policy
1.0	22.05.2014	Nta1	First Version of the IS Policy

2 Introduction

ACME AG has a long and proud history of being the market leader in manufacturing high end goods. The company was founded to set and redefine the standards of product quality. Every part of the company embodies the motto “Achieve greatness by building better products”. This motto does not only apply to the production of goods, but it also applies to the protection and availability of our information system.

To achieve the highest level of protection, clear standards and mechanism must be developed and executed. To fulfil this goal this document will provide security objectives and strategies and will define roles and responsibilities.

The document will contain our solutions for the core principles of information security management as defined in the ISO 27002.

3 Security goals

ACME AG is committed to protect the confidentiality, integrity and availability of all physical and electronic information assets of the company. This includes every department of the company, informations about our customers and informations about our partners. The goals for this information policy are the following [2]

- Ensure that the information security standards of the company comply with regulations, laws and guidelines
- Establish mechanism to protect the information system against abuse, theft and other forms of harm
- Motivate administrators and employees to constantly improve their knowledge about information security
- Ensure the availability and reliability of services
- Build contingency plans for continuing services after major security incidents
- Ensure that external service providers comply to international security standards

4 Roles

Building and executing an information security policy requires a strict organization of rules and responsibilities. To achieve this, roles must be defined. Each role has its own responsibilities and certain amount of rights. ACME defines following roles [2]:

4.1 Owner of the Security Policy

The CEO of the company is in charge of the information security policy. He delegates every responsibility about the information security to the Chief Information Security Officer. Changes to the information security policy must be reviewed and approved by the CEO.

4.2 Chief Information Security Officer

The Chief Information Security Officer's main responsibility is to control and adapt the information security of the company. He is in charge of executing the policy and he is also the only person that can suggests changes to the security policy.

4.3 System Owner

The System owner in cooperation with the IT department is responsible for building and maintaining the information stored on a system. He is also in charge of implementing access control to the information system. The System owner defines user roles and defines which user group has access to which part of the system.

4.4 System Administrator

System Administrators operate the information systems of the company. Each information system of the company has at least one or more administrators. They are responsible for protecting and maintaining the confidentiality and availability of the data stored in the system. They are also responsible for restoring the systems after security incidents and other type of incidents. They will also implement the security protection mechanism according to this policy.

4.5 User

Employees are required to get acquainted with ACME AG information security policy. They should follow every aspect of the information security policy and violations should be dealt with extreme prejudice. In the case of questions about the policy employees should ask the system owner or the system administrators.

4.6 Consultants and contractual partner

External partners are only allowed to access the internal information system after signing a confidentiality agreement. They are only allowed to access system parts they have clearance. For accessing other parts of the systems the approval of the system administrator or the system owner is required.

5 Risk Management

- The first step in building a information security policy is to determine the different sensitivity or critically of the data stored in the network. To build an appropriate security policy a risk assessments must be done. In this process each information must be identified and classified. Each information must be categorized after consequences and like hood of security breaches [2].
- This risk assessment must be done by each department. After this assessment the result must be reviewed by the CEO.
- Each department must identify information assets that exist in their department. After finding the assets, it must be defined who owns the assets and they must be classified according to rules defined by the CEO and the CSO.
- After classifying the assets rules for the acceptable use must be defined and documented.
- The risk assessment must be done periodically and include every department of the company.

6 Reporting

6.1 Purpose

This policy serves to protect the company against damages caused by security breaches and to restore operations after incidents. This policy should provide a clear chain of communication for reporting incidents, so that the appropriate persons are informed as soon as possible [3].

6.2 Policy

6.2.1 Users

Users must report immediately every security incidents to system administrators and system owners.

6.2.2 System Administrators

System administrators must report immediately every incidents to the system owners. According to the level of the security breach the CSO must be informed.

If the threat is a class A incident counter actions must be performed accordingly to the company policy. Also the CEO must be informed.

If the threat is a class B incident the CSO must be informed during the next department meeting. The incident must be reviewed by the system administrator and the system owner and possible scenarios must be developed to protect against the same type of attack.

If the threat is a class C incident the system administrator must inform the person that violated the information security policy about the violation.

6.3 Definition

6.3.1 Threat Level A

Highest threat level of the organization. An unauthorized attack against high value informations was detected.

6.3.2 Threat Level B

An unauthorized access attempt was detected.

6.3.3 Threat Level C

Is a small violation against the information security policy of the company.

7 Acceptable Use Policy

7.1 Purpose

The purpose of this policy is to give employees a guideline in acceptable use of company equipment. This policy should protect users and the company against possible treats like viruses, attacks on the computer networks and legal issues [1].

7.2 Scope

This policy applies to every employee, external personal and temporary worker. It applies to every type of telecommunication equipment that is connected to our services and it also applies to every computer or other device that is connected through the network of ACME AG.

7.3 Policy

- Every information that is stored on devices owned or leased by the ACME AG is property of the company. Every information should be protected with the highest standards of data security.
- Employees have to immediately report the theft or loss of devices.
- To control and to protect the network authorized personal are allowed to monitor the traffic of the devices.
- ACME AG reserves the rights to change the user rights of the device.
- All devices that are connected to the internet must fulfil the basic protection standards of the company.
- Employees must clarify when posting in forums that they are not expressing the opinion of the company.
- Password must comply with company policies regarding passwords.
- Employees must be extremely cautious about opening attachments from unknown email addresses.
- Each device must be secured with password protected screen savers.

8 Clean Desk Policy

8.1 Purpose

The purpose of this policy is to protect informations about our employees and intellectual property of ACME AG. Every important information must be locked away [1].

8.2 Scope

This policy applies to every member of this company.

8.3 Policy

- Every employee is required to ensure that every information is locked away if he or she leaves work at the end of the day or when the person leaves his or her workplace for a extended period.
- Computers must be locked during the day and shut down after work.
- Whiteboards containing informations should be cleaned.
- Information that is no longer required should be destroyed.
- Portable devices should be treated as important information and should be locked away.

9 Disaster Recovery Plan Policy

9.1 Purpose

The purpose of this policy is to define a disaster recovery plan that describes the process of restoring the services and data of the ACME AG information system [1].

9.2 Scope

This policy is directed at the system owners. They should ensure that there is contingency plan in case of disasters. This plan should be developed, tested and regularly adapted [1].

9.3 Policy

- Data Study: List every information stored in the system
- Computer Emergency Plan: Action plan for certain scenarios
- Service List: A list of services ordered by their importance.
- Data Backup and Restoration Plan: A detailed plan to restore the information system.
- Equipment Replacement Plan: A list ordered by the importance of the equipment and places to buy replacements.

10 Email Policy

10.1 Purpose

The purpose of this policy is to set a guideline about the use of the company email services. It should protect the company against unacceptable use of the email system [1].

10.2 Scope

This policy applies to every email sent by an email address of the company.

10.3 Policy

- Email accounts should be primarily used for company business.
- All data contained in the email must fulfill the data protection standards.
- Emails should only be retained if they qualify as business record.
- Employees are not allowed to contribute offensive material and should report offensive material.
- Users are not allowed to use third party email systems
- Personal emails are allowed but must be stored in different folders.
- If there is any suspicion of violation of the information security policy the company is allowed to monitor the email traffic of employees.

11 Password Protection Policy

11.1 Purpose

Purpose of the policy is to create strong password to protect the system [1].

11.2 Scope

This policy applies to every person with an manageable account.

11.3 Policy

- The password must contain at least 6 characters.
- The password must contain at least 1 number.
- The password must contain at least 1 special number.
- Users must use different passwords for different accounts.
- All passwords must be changed at least every month.
- Passwords must not be shared with anyone.
- Passwords must not be written down.
- User should not use the remember password functions.

12 Software Installation Policy

12.1 Purpose

The purpose of this policy is to create a guideline for installing software on company devices. This should help to protect the company against malware, exposure of sensitive informations [1].

12.2 Scope

This policy applies to every employees and partners of the ACME AG. It covers every device that is somehow connected to the network.

12.3 Policy

- Employees are not allowed to install software on devices owned or leased by the ACME AG.
- Software request must be approved by the system administrators and the system owners. The request must be documented.
- System administrator will obtain the licenses for the software and test the software for possible issues with the system.

Bibliography

[1] Guel et al. Information security policy templates. *SANS Policy Project*, 2014.

[2] Eilertsen Boe Hostland, Enstad. Information security practice, best practice. *Geant*, 2010.

[3] Oxford IT services. Information security incident reponse. *University of Oxford*, 2014.