Enterprise Security Policy

1. Acceptable Use policy

1.1 purpose

The purpose of this strategy is to outline the acceptable usage of computer equipment in the company. The quasi-abiding rules will protect employees and the company. Improper use will bring risks and legal problems to the company.

1.2 policy

1.2.1 Company proprietary information stored in electronic and computer equipment is the exclusive property of Company. You must ensure that proprietary information is protected by data protection standards through legal or technical means.

1.2.2 You are responsible for promptly reporting the theft, loss or unauthorized disclosure of company proprietary information.

1.2.3 You can only access the areas where you are authorized

1.2.4 For security and network maintenance purposes, authorized personnel in the company can monitor devices, systems, and network traffic at any time according to Infosec's audit policy.

1.2.5 The company reserves the right to regularly review the network and systems to ensure compliance with this policy.

1.2.6 The employees of the company have no right to engage in any illegal activities with the resources owned by the company under any circumstances.

1.2.7 Employees of the company are strictly prohibited from infringing the rights of any individual or company protected by copyright, trade secrets, patents or other intellectual property rights or similar laws or regulations.

1.2.8 Company employees are strictly prohibited from accessing data, servers or accounts for any purpose other than company business, even if you have authorized access.

1.2.9 If an employee expresses his or her beliefs and / or opinions in a blog, the employee must not expressly or implicitly represent himself as an employee or a company representative. Employees bear all risks related to blogging.

1.2.10 Employees are prohibited from disclosing any company confidential or proprietary information, business secrets or any other materials covered by the company 's confidential information policy when blogging.

1.2.11 Any exception to the policy must be approved by the Infosec team in advance.

1.2.12 An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

1.3 Definitions

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Blogging

1.4 Associated Standard

- Data Classification Policy
- Data Protection Standard
- Social Media Policy

2. System Access Control policy

2.1 purpose

The purpose of this strategy is to establish standards for the basic configuration of internal systems owned and / or operated by the company. Effective implementation of this strategy will minimize unauthorized access to company proprietary information and technology.

2.2 Policy

2.2.1 All internal servers deployed in the company must be owned by the operations team responsible for system management. Each operation team must establish and maintain approved server configuration guidelines based on business needs and obtain InfoSec approval. The operations team should monitor configuration compliance and implement exception policies for their environment. The following regulations must be met:

- The server must have server contacts and location, alternate contacts, hardware and operating system / version and other information and must be registered in the enterprise management system.
- The information in the company's corporate management system must be kept up to date.
- Production server configuration changes must follow appropriate change management procedures.

2.2.2 Authorized personnel can monitor and audit equipment, systems, processes and network traffic according to the audit policy.

2.2.3 The operating system configuration should comply with the approved InfoSec guidelines.

2.2.4 The latest security patches must be installed on the system as soon as possible, the only exception is when immediate application will interfere with business requirements.

2.2.5 Always use standard security principles that require the least access to perform functions. When non-privileged accounts can use root, do not use root.

2.2.6 The server is specifically prohibited from operating in uncontrolled small cubicle areas.

2.2.7 The server should be physically located in an access control environment.

2.2.8 Any exception to the policy must be approved by the Infosec team in advance.

2.2.9 An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2.2.10 All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by Cisco or registered under a Cisco-owned internal network domain. This policy specifies requirements for equipment on the internal Cisco network. For secure configuration of equipment external to Cisco on the DMZ, see the Internet DMZ Equipment Policy.

2.3 Definitions

The following definition and terms can be found in the SANS Glossary located at:

https://www.sans.org/security-resources/glossary-of-terms/

- De-militarized zone (DMZ)

2.4 Associated Standard

- DMZ Equipment Policy

3. Incident handling Policy

3.1 purpose

The purpose of this strategy is to establish goals and vision for the incident handling process. The policy will clearly define who is applicable and under what circumstances, and will include definitions of violations, employee roles and responsibilities, standards and indicators (eg, prioritization of incidents), and reporting, remediation, and feedback mechanisms. This policy should be fully publicized and easy to use by all those responsible for data privacy and security protection.

3.2 Policy

3.2.1 Once the theft, leakage or exposure of company-protected data or company-sensitive data is identified, the process of deleting all access to the resource will begin.

3.2.2 The Executive Director will chair an incident response team to handle the breach or exposure. Team members include IT Infrastructure, IT Applications, legal, communications, member services, human resources, affected units or departments that use related systems or outputs or whose data may have been destroyed or exposed

- Increase the department according to the type of data involved

3.2.3 Theft, sabotage or exposure will be notified to the executive director. IT and the designated forensic team will analyze the violation or exposure to determine the root cause.

3.2.3 According to the company's network insurance regulations, insurance companies will need to provide access to forensic investigators and experts to determine how violations or exposures occur; the type of data involved; the number of affected internal / external individuals and / or organizations; and Analyze violations or exposures to determine the root cause.

3.2.4 Cooperate with the company's communications, legal and human resources departments to decide how to inform the following personnel of the violation: a) internal employees, b) the public and c) directly affected people

3.3 Definitions

- Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;
- Plain text – Unencrypted data.
- Protected Health Information (PHI)-Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.
- Personally Identifiable Information (PII)-Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered
- Protected data-See PII and PHI
- Sensitive data-Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

3.4 Associated Standard

None.

Reference:

SANS Institute: Information Security Policy Templates. (n.d.). Retrieved from https://www.sans.org/security-resources/policies/

SANS Institute. (n.d.). Retrieved from https://www.sans.org/security-resources/glossary-of-terms/