International Journal of Computer Applications Technology and Research
Volume 7–Issue 06, 221-224, 2018, ISSN:-2319–8656

Information System Security Policy Studies as a Form of Company Privacy Protection

Rio Jumardi
Sekolah Tinggi Teknologi Bontang
Bontang, Indonesia

Abstract: Technology that interconnects computers in the world allows to be able to exchange information and data even communicate with each other in the form of images and video. The more valuable the information is required a security standard to maintain the information. Computer security target, among others, is as protection of information. The higher the security standards provided the higher the privacy protection of the information. Protection of employee privacy within a company is one factor that must be considered in the information systems implementation. Information system security policies include: System maintenance, risk handling, access rights settings and human resources, security and control of information assets, enterprise server security policy and password policy. The policies that have been reviewed, be a form of protection of corporate information.

Keywords: Computer Security, Information Assets, Information Systems, Privacy, Policy.

1. INTRODUCTION

Currently we are in the digital era where communication and information exchange takes place in a growing network of increasingly widespread. A Technology that interconnects computers in the world allows to be able to exchange information and data even communicate with each other in the form of images and video. The more valuable the information is required a security standard to maintain the information.

The system can be accessed with a current high availability is required, openness and distributed would have become a necessity for an integrated system. Information systems security management can reduce the occurrence of irregularities of the access rights by certain parties and misuse of data and information of an organization or company [1].

Computer security objectives are, among others the protection of information. The components of the security plan include: information security policies, standards and procedures, control of human resources management for information security, and control of information security technologies [2].

The higher the security standards provided the higher the privacy protection of the information. Protection of personal confidentiality of company employees is one of the factors that must be considered in the implementation of information systems. The making of information system security policy is expected to be a control of the organization's or company's behavior on the system.

Privacy is the ability of one or a group of individuals to retain life and personal affairs from the public, or to control the flow of information about themselves [3]. Privacy is sometimes associated with anonymity even though anonymity is especially appreciated by people known to the public. Privacy can be considered as an aspect of security.

Computer Crime is an unlawful act committed using a computer as a tool or computer as an object, whether to gain profit or not, to the detriment of the other party.

Computer crimes stipulated in the Act ITE provided for in Chapter VII of the act is prohibited. These deeds are categorized into several groups ie [4].

1. Unauthorized access
2. Unauthorized interception
3. Disturbance to computer data

Crimes that are closely linked to the use of technology based on these computers and telecommunications networks in several literatures and practices are grouped in several forms, including: [5]

1. Unauthorized Access Computer Systems and Service, Crimes committed by infiltrated into a computer network system illegally, without permission or without the knowledge of the owner of the computer network system he entered.
2. Contents, It is a crime by using data or information to the internet about a thing that is untrue, unethical, and may be considered unlawful or disturbing public order.
3. Forgery data, It is a crime to forge data on important documents stored as scriptless documents over the internet.
4. Cyber Espionage, is a crime that exploits the Internet network to conduct spying on other parties, by entering the target computer network system.
5. Cyber Sabotage and Extortion, Crime is done by making interference, destruction or destruction of a data, computer program or computer network system connected to the internet.
6. Offense Against Intellectual Property, This Crime is directed against intellectual property rights owned by others on the internet. For example, imitating the display on the web page of someone else's site illegally, broadcasting an information on the internet that turned out to be other people's trade secret information and so on.

The core of computer security is to protect computers and networks with the aim of securing the information in it. Computer security itself includes several aspects, among others: [6]

1. Authentication, the recipient of the information can ensure the authenticity of the message, that the message came from the person being asked for information. In other words, the information actually comes from the desired person.
2. Integrity, authenticity of messages sent over the network and it is certain that the information sent is not modified by unauthorized persons.

3. Non-repudiation, is related to the sender. The sender can not deny that it was he who sent the information.
4. Authority, the information residing on the network system can not be modified by unauthorized parties to access it.
5. Confidentiality, is an attempt to keep information from unauthorized persons. This secrecy usually relates to information provided to other parties.
6. Privacy, more towards personal data.
7. Availability, availability aspect relates to the availability of information when needed. Information systems that are attacked or uprooted can inhibit or eliminate access to information.
8. Access Control, this aspect relates to the way access to information is arranged. This is usually related to authentication and privacy issues. Access control is often done using a combination of user id and password or with other mechanisms.

Computer security provides requirements for computers that differ from most system requirements because they often take the form of restrictions on what computers should not do. This makes computer security is becoming more challenging because it is quite difficult to create a computer program to do everything what is designed to be done properly. Negative requirements are also difficult to meet and require in-depth testing for verification, which is impractical for most computer programs. Computer security provides a technical strategy for turning negative requirements into positive rules that can be enforced.

The main principle of information system security consists of confidentiality, integrity and availability or often called the CIA [7].

The general approach taken to improve computer security, among others, is to restrict physical access to the computer, implementing a mechanism on the hardware and operating system for computer security, as well as make your programming strategies to generate a reliable computer program.

ISO is one of the world's bodies that make standardization used by users or producers in a particular field. ISO 17799: 27002 is a standard that contains information security system settings[8].

Security clauses in ISO are [8]: Risk assessment and treatment, security policy, organization of information security, asset management, human resources security, physical and environmental security, communication and operation management, access control, information system acquisition, development and maintenance.

Information security aspects include the following ten aspects: security policy, security organization, classification and control assets, personnel security, physical and environmental security, communication and operations management, access control, system development and maintenance, business continuity management, harmonization.

2. RESEARCH METHODS

The research method used is a descriptive qualitative method that is the result of research presented in the form of narrative description. Qualitative approach done in this research is by detailing information security policy of the company information system with existing standards at ISO 17799:27002.

Data collection is done by direct observation in the field and direct interview with end users system and system manager in this case people who are competent in the field of information technology.

The Information Security Policy is defined as: An action plan for addressing information security issues, or a set of rules for maintaining certain information conditions or security levels [10].

Policy-making is based on a hierarchy of policies, standards, guidelines, procedures and practices.

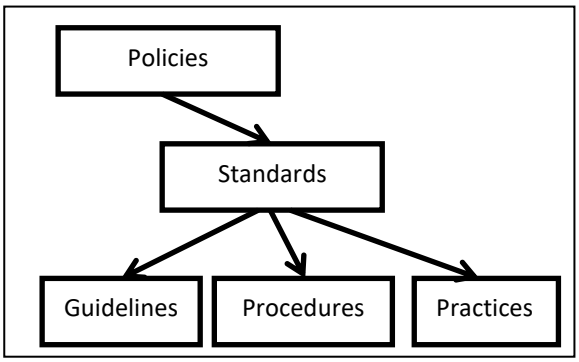

Figure 1. Policy-making Hierarchy [10]

The information security policy covers three general categories including Enterprise Information Security Policy (EISP), Issue Specific Security Policy (ISSP) and System Specific Policy (SSP) [10].

This research will discuss about EISP which includes system maintenance, risk handling, policy of access rights and human resources and security policy and control of information asset in the company and discuss about ISSP covering server security policy and password policy.

3. RESULTS AND DISCUSSION

From the introduction above, a study that discusses the information systems security policy will be one of the forms of privacy information company protection. Among the policies to be made are based on the ISO 17799: 27002 standard and also the standards issued by ID SIRTII include EISP, ISSP and SSP.

3.1 System Maintenance Policy

System maintenance policy is required to maximize maintenance of the running system, Company's system maintenance policy includes:

1. Objective: to ensure that the information system being implemented runs well.
2. Standard: used is the standard of ISO 17799: 27002 and Index KAMI as an evaluation tool.
3. Coverage: the implementation of this policy is directed to stakeholders and concerned employees in the Information Technology section as well as third parties who become vendors.
4. Guidelines for care: system maintenance should be in accordance with applicable guidelines.
5. Procedure: establish procedures related to system maintenance that include corrective care, adoptive care, preventive care and preventive care.
6. Monitoring: monitoring is required to monitor all activities related to the maintenance of the Company's systems.

3.2 Risk Management Policy

Risk management policies are required to address the risks that may arise during system implementation. The Company's risk management policy includes:

1. Objectives: identify and analyze possible risks that exist in the implementation of information systems in the company.
2. Standard: used is the standard of ISO 17799: 27002, ISO / IEC 27005, Octave Allegro Method.
3. Coverage: the implementation of this policy is intended for all employees in the corporate environment related to information assets.
4. Risk mitigation guidelines: risk handlers of the information systems and assets should be in compliance with applicable guidelines.
5. Procedures: establish procedures for risk management that include developing risk assessment criteria, developing an information asset profile, identifying containers from information assets, identifying problem areas, identifying threat scenarios, identifying risks, analyzing risks, and choosing a risk selection election approach.
6. Monitoring: monitoring is required to monitor all activities related to the Company's risk management.

3.3 Human Resource Policy

Human resource and access rights arrangements, policies are required to regulate the constraints of users of information systems within the Company. Human resource policies and corporate permissions settings include:

1. Objective: controlling user access of information systems by setting user permissions. Another purpose is to reduce risk for misuse of function or authority due to human error.
2. Standard: used is the standard of ISO 27002 and Information Technology Infrastructure Library (ITIL) V3.
3. Coverage: the implementation of this policy is directed to stakeholders and corporate leaders to determine or manage the determination of human resources by regulating access rights to the system.
4. Guidance: the determination of the right of access to the system shall be in accordance with the guidelines and rules applicable within the Company. Adjusted also with the ability of information systems to manage access rights.
5. Procedure: Establish procedures relating to the arrangement of access rights that include access requests, access grants, user identity monitoring, employee performance appraisal, employee job behavior, access restrictions, removal of access, access problems and access logging.
6. Monitoring: monitoring is required to monitor all activities related to human resource management and regulation of the access rights of information systems in the Company.

3.4 Security and Asset Control Policy

Security and asset control policies are required to manage the company's information assets. The company's information security and control policy include:

1. Objective: to provide protection for the company's assets based on the level of protection provided.
2. Standard: used is the standard of ISO 17799: 27002.
3. Coverage: the implementation of this policy is intended for stakeholders and corporate leaders and employees to the security of information assets in the use of information systems.
4. Guidelines: The guidelines for the security and control of information assets within a company's environment must be in accordance with the rules applicable to both the rules of the information system and the rules of the company.
5. Procedure: make procedures related to asset security and control of information assets include information classification and information responsibilities.
6. Monitoring: monitoring is required to monitor all activities related to the control of information assets in the Company.

3.5 Enterprise Server Security Policy

Another policy that must be considered by the company is the server security policy. This policy is necessary to maximize the security of data servers which will also directly maintain the confidentiality of Company data and employee privacy data against computer crimes that will harm the Company.

The Enterprise Server Security Policy includes:

1. Objective: maximize the security of the Company's information system from the server in use.
2. Standard: used is the standard of ISO 17799: 27002 and KAMI Index for evaluation tool.
3. Coverage: the implementation of this policy is directed to stakeholders and employees concerned in the Information Technology section
4. Guidance: The server configuration must be in accordance with applicable guidelines.
5. Procedure: make procedures related to server security that includes own server creation procedures, server storade procedures, server room security procedures, employees who served server room, and use of the server.
6. Monitoring: monitoring is required to monitor all activities related to the security of the Company's servers.

3.6 Password Policy

Password setting policy is required to set the password creation procedure and forget the password that is directly related to the security of the information system. The password setting policy includes:

1. Objective: maximize the security of corporate information systems through the use of secure passwords.
2. Standard: used is ISO 17799: 27002 standard.
3. Coverage: the implementation of this policy is directed to all company employees and system administrator sections
4. Guidance: Password settings must be in accordance with applicable guidelines.
5. Procedure: make procedures related to password setting that includes a procedure of making password, forgot password procedure, password reset procedure, captcha usage procedure, password active procedure and password combination rule.
6. Monitoring: monitoring is required to monitor all activities related to corporate information system's password setting activities.

4. CONCLUSION

Implementation of policies relating to the security of information systems is essential as a form of protection of corporate information.

The required policies include: System maintenance, risk handling, access control arrangement and human resources policies, security and control of information assets, server security policies and password policy. The protection provided not only for the Company's information, but also to the protection of the Company's personal privacy.

A Suggestion related to this research is a company can evaluate an information security policy using existing methods like KAMI Index, ITIL and other methods.

5. REFERENCES

[1] Wildan Radista Wicaksana, Anisah Herdiyanti , and Tony Dwi Susanto, "Pembuatan Standar Operasional Prosedur (SOP) Manajemen Akses Untuk Aplikasi E-Performance Bina Program Kota Surabaya Berdasarkan Kerangka Kerja ITIL V3 Dan ISO 27002," *Jurnal Sisfo*, vol. 06, no. 01, pp. 105-120, September 2016.

[2] Aan AlBOne, "Pembuatan Rencana Keamana Informasi Berdasarkan Analisis dan Mitigasi Risiko Teknologi Informasi," *Jurnal Informatika*, vol. 10, pp. 44-52, Mei 2009.

[3] "http://id.wikipedia.org/wiki/Kerahasiaan_pribadi," 2013.

[4] Ana Maria F. Pasaribu, "Kejahatan Siber Sebagai Dampak Negatif dari Perkembangan Teknologi dan Internet di Indonesia Berdasarkan Undang-undang No. 19 Tahun 2016 Perubahan atas Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Perspektif Hukum Pidana," Universitas Sumatera Utara, Medan, Thesis 2017.

[5] Dodo Zaenal Abidin, "Kejahatan dalam Teknologi Informasi dan Komunikasi," *Jurnal Ilmiah Media Processor*, vol. 10, no. 2, pp. 509-516, Oktober 2015.

[6] Muhammad Siddik Hasibuan, "Keylogger Pada Aspek Keamanan Komputer," *Jurnal Teknovasi*, vol. 03, no. 1, pp. 8-15, 2016.

[7] Deni Ahmad Jakaria, R. Teduh Dirgahayu, and Hendrik, "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro," in *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, Yogyakarta, 2013, pp. E- 37-42.

[8] Deris Stiawan, "Kebijakan Sistem Informasi Manajemen Keamanan IT (Information Security Management Policy) Standard ISO 17799 : 27002," Universitas Sriwijaya, Palembang, 2009.

[9] Prof. Richardus Eko Indrajit, "ISO17799. Kerangka Standar Keamanan Infromasi," id-SIRTII, Jakarta, 2018.

[10] Iwan Sumantri. (2018, Mei) ID SIRTII. [Online]. http://cdn.woto.com/dsfile/49ba65ea-0804-46c3-aa21-86d156d167f9