Assignment #4

Security Policy

- ISO27001

20 March, 2016

Authors:
Sarpreet Singh Buttar
Philip Lunyov
Aya Kathem
Felix Rhodin
Guillaume Fumeaux

Contents

1 Introduction **1**

2 Scope **2**

3 Risk assessment and treatment **2**

4 Security policy **2**

5 Organizing information security **2**

5.1 Internal organization 2

5.2 Independent review of information security 2

5.3 Information security co-ordination 3

5.4 Authorization process for information processing facilities 3

6 Human Resources Security **4**

6.1 Management Responsibilities 4

6.2 Information security awareness, education, and training 4

6.3 Removal of access rights 4

7 Physical and environmental security **5**

7.1 Physical access controls 5

7.2 Protecting against external and environmental threats 5

7.3 Delivery and Loading Areas 5

7.4 Supporting Utilities 6

8 Communications and Operations Management. **7**

8.1 Operational Procedures and Responsibilities 7

8.1.1 Documented operating procedures 7

8.1.2 Change Management 7

8.1.3 Third party service delivery management 7

8.1.4 System planning and acceptance 8

8.1.5 Protection against malicious and mobile code 8

8.1.6 Back-up 8

8.1.7 Network security management 8

8.1.8 Media handling 8

8.1.9 Exchange of information 8

8.1.10 Electronic commerce services 8

8.1.11 Monitoring 8

9 Access control **10**

9.1 User access management 10

9.2 Network access control 10

9.3 Operating system access control 10

9.4 Application and information access control 11

10 Information Security Events and Weaknesses **12**

10.1 Reporting Information Security and Events Management 12

10.1.1 Company's Situation 12

10.1.2 Problems 12

10.1.3 Solutions 12
10.2 Management of Information Security Incidents and Improvements 13
10.2.1 Company's Situation 13
10.2.2 Problems 13
10.2.3 Solutions 13

11 Business Continuity Management 14
11.1 Information Security Aspects of Business Continuity Management 14
11.1.1 Company's Situation 14
11.1.2 Problems 14
11.1.3 Solutions 14

12 Compliance 15
12.1 Compliance with Legal Requirements 15
12.1.1 Company's Situation 15
12.1.2 Problems 15
12.1.3 Solution 15
12.2 Compliance with Security Policies and Standards and Technical Compliance 15
12.2.1 Company's Situation 15
12.2.2 Problems 15
12.2.3 Solutions 16

1 Introduction

This document will present the different security controls that the company should apply to meet the standard of ISO 27001. Each control has been selected in regards with the actual situation of the company, and the information gathered from the meeting with the CTO of the company. They are separately presented and explained in accordance to the requirements in the ISO 27001 document.

2 Scope

This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management.

3 Risk assessment and treatment

IT administrator of the company must review systematically company's infrastructure to complete the risk analysis management and define possible risk vector. IT administrator must perform any actions to treat assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur in the infrastructure and document it to use this kind of documents in future development.

4 Security policy

After expanding your office, people who are responsible for IT infrastructure (IT administrator and CTO) should review their security policy once again to cover all added machines and procedures, and to redefine security standards within company. Before redefining security policy, IT staff should cooperate with company's employees, look at previous reports and security policy, previous management, to create useful, understandable and approachable security policy, which covers new aspects of IT security in the office.

5 Organizing information security

5.1 Internal organization

Security management must perform a security seminar to help employees to understand privacy considerations and security policy within company and outside. Employees must understand their role in company's development, know their responsibilities outside workspace and know what sort of damage can cause every worker by leaking information about IT structure outside the office.

5.2 Independent review of information security

Security management of your company should hire a security specialist to have a review of overall IT structure. Specialist should provide an independent review, based on your real-time structure and previous structure, provide suggestions to improve your IT security and provide practical advices how to maintain your security policy. Based on the information provided by independent IT security specialist, company should update their policy, its implementation and standards, also inform staff about significant changes in their work, which is related to the security.

5.3 Information security co-ordination

Information security co-ordination should involve the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialist skills in areas such as insurance, legal issues, human resources, IT or risk management.

1 Ensure that security activities are executed in compliance with the information security policy;

2 Identify how to handle non-compliances;

3 Approve methodologies and processes for information security, e.g. risk assessment, information classification;

4 Identify significant threat changes and exposure of information and information processing facilities to threats;

5 Assess the adequacy and co-ordinate the implementation of information security controls;

6 Effectively promote information security education, training and awareness throughout the organization;

7 Evaluate information received from the monitoring and reviewing of information security incidents, and recommend appropriate actions in response to identified information security incidents.

5.4 Authorization process for information processing facilities

A management authorization process for new information processing facilities should be defined and implemented. Local server which contains important data must have an additional security level and strong access control. One person should take a responsibility for managing server with important data and control its workflow.

Facilities (like server room) should have appropriate user management authorization, authorizing their purpose and use. Authorization should also be obtained from the manager (IT administrator or CTO) responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met.

The use of personal or privately owned information processing facilities, e.g. laptops, home-computers or hand-held devices, for processing business information, may introduce new vulnerabilities and necessary controls should be documented and introduced to the working groups.

6 Human Resources Security

6.1 Management Responsibilities

Management should ensure that all forms of employees applies security in accordance with established policies and procedures of the organization. In order to do so the following steps should be implemented.

1. The management ensures that all employees are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems

2. All employees are provided with guidelines to state security expectations of their role within the organization.

3. The management makes sure that all employees are motivated to fulfil the security policies of the organization

6.2 Information security awareness, education, and training

All employees of the organization should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. In addition to the one week training these steps should be implemented.

1. The training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities.

2. All employees should be regularly updated in organizational policies and procedures.

6.3 Removal of access rights

access rights of all employees to information and information processing facilities should be removed upon termination of their employment, contract or agreement. Instead of a month access after the termination the access rights should be revoked at the same time as the termination.

1. The access rights that should be removed or adapted include physical and logical access, keys, identification cards, information processing facilities, subscriptions, and removal from any documentation that identifies them as a current member of the organization

2. If a departing employee has known passwords for accounts remaining active, these should be changed.

7 Physical and environmental security

7.1 Physical access controls

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

1. In addition to electronic key card there should also be a pin code attached so that even if the card is stolen they dont have access.
2. Alarms and cameras should be set up so that noone can breach the perimeter without getting detected and identified.
3. The area were the company store sensitive information should only be accessible to employees with access and there should be another access control to prevent unauthorized personnel from gaining acces to the secure area.

7.2 Protecting against external and environmental threats

Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

1. Hazardous or combustible materials should be stored at a safe distance from a secure area. Bulk supplies such as stationery should not be stored within a secure area.
2. Fallback equipment and back-up media should besited at a safe distance to avoid damage from a disaster affecting the main site.
3. Lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines.
4. Guidelines for eating, drinking, and smoking in proximity to information processing facilities should be established.

7.3 Delivery and Loading Areas

A delivery and loading area should be set up. Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

1. the delivery and loading area should be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building
2. incoming material should be inspected for potential threats before this material is moved from the delivery and loading area to the point of use.

7.4 Supporting Utilities

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. Support utilities should be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure

1. Power contingency plans should cover the action to be taken on failure of the UPS.
2. A back-up generator should be considered if processing is required to continue in case of a prolonged power failure.
3. An adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period.
4. UPS equipment and generators should be regularly checked to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations.
5. Emergency power off switches should be located near emergency exits to facilitate rapid power down in case of an emergency.
6. Telecommunications equipment should be connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services.

8 Communications and Operations Management.

8.1 Operational Procedures and Responsibilities

8.1.1 Documented operating procedures

Operating procedures should be documented, maintained, and made available to all users who need them. Documented procedures should be prepared for system activities associated with information processing and communication facilities.The procedures should contain the following.

1. Processing and handling of information.
2. Support contacts in the event of unexpected operational or technical difficulties.
3. special output and media handling instructions, such management of confidential output including procedures for secure disposal of output from failed jobs.
4. system restart and recovery procedures for use in the event of system failure.

8.1.2 Change Management

Changes to information processing facilities and systems should be controlled. Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. These controls should be applied.

1. identification and recording of significant changes.
2. planning and testing of changes.
3. assessment of the potential impacts, including security impacts, of such changes.
4. communication of change details to all relevant persons.
5. fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

8.1.3 Third party service delivery management

The company works with Dropbox so that they can access to their information from anywhere, on any device.

Dropbox in its role protects their information from any unauthorized access. The Dropbox have a clear policies and agreement show how they work, how they make the information secure, what role they have and even what their customer allow to do with instruction.

8.1.4 System planning and acceptance

The company use paper and pen to do contingency plan so if there any error may be happen.

The company do not identify for each new ongoing activity, capacity requirements.

8.1.5 Protection against malicious and mobile code

The company use anti-viruses to protect their software against viruses, malicious and mobile code. The company employer all of them is knowledgeable in computer security and know how to avoid any viruses.

8.1.6 Back-up

The company use a Back-up to have another copy of the information to help them when they need it. The company make sure that just the authorized persons access to the information by using password.

8.1.7 Network security management

The company use a firewall to protect their network and I think that is enough to their company.

8.1.8 Media handling

The company take care before they get rid of any sensitive information, for example if they want to take rid of disk they remove all information before they get rid of it.

The company handling the sensitive information by using a password to allow the authorized person to access to the data.

8.1.9 Exchange of information

The company do not work with any other companies and do not exchange the information. The policy in this section is not related to them.

8.1.10 Electronic commerce services

The company does not work with electronic commerce. The policy in this section is not related to them.

8.1.11 Monitoring

Not only the firewall, files and ad should be monitored. Every systems should be monitored and information security be saved. Some enhancement have to be made.

Information logging

The different information that should appear in the files log when relevant are listed chapter 10.10.1 Audit logging. You need to be able to say who accessed what, when and how. Make sure that all the information needed are already saved in the logs files or make the necessary modification. The IT-administrator should not be able to deactivate/erase its own logs. His activities should be logged, and reviewed by someone else or an intrusion detection system managed outside of its controls could be implemented to monitor its activities. If any intrusive or confidential personal data are contained in the logs, an appropriate privacy protection measures should be applied on them.

System monitoring

When talking about monitoring system use, a risk assessment have to be realized to determine the level of monitoring required for individual facilities. Authorized access, all privileged operations, unauthorized access attempts, system alerts should be monitored. Nagios, Microsoft SCMM are different option available to implement this monitoring. They are infrastructure monitoring software. The review periodicity should depend on the risks involved. Even if nothing happened, the logs have to be reviewed as not all treats can be noticed without looking at the logs. The IT-administrator should be able to understand the different treats possible to review the logs correctly

Other information

The logging facilities and log information have to be protected against tampering and unauthorized access to guarantee their integrity. All the logs have to be based on the same correct clock to ensure their validity for investigations or as evidence in legal or disciplinary cases. All relevant legal requirement applicable to the monitoring and logging activities have to be complied.

9 Access control

A certain level of security is already in place for access control, as policy, VPN when connecting from outside the company, user education etc. However, some improvement on the Wi-Fi, server, personal devices and computer have to be made.

9.1 User access management

The users should not be administrator of their station. They should have only the least privileges they need for their functional role and allocated on an event-by-event basis. A process and a record of all privileges allocated should be maintained. The user get of the privilege only when the process is complete. The need to grant privileges to users should be avoided as often as possible. Microsoft GPO and AGDLP strategy can be used to enforce it.

The users' access rights should be reviewed at regular intervals. Usually when a user change his position in the company, and a 6 months basis or 3 months for special privileged access rights. The review permits to find out if a user would have obtained unauthorized privileges.

9.2 Network access control

The wireless network requires additional authentication controls. A server service as RADIUS have to be considered to authenticate users and only authorize users identified to access the wireless network.

Equipment identification in networks should require that every devices that want to connect to the wireless network has to be registered and so only they could connect by being identified. Those controls can complement each other. The capability of users to connect to the network should be restricted, especially for the networks extending across the organization's boundaries. The users should have access only to what they need for their functional role.

The monitoring system should record and help to find out about all unauthorized attempts to connect to the company wired and wireless network.

9.3 Operating system access control

Operating systems should be controlled by a secure log-on procedure. When the user wants to log in, the less possible information should be shown that could help an unauthorized user. All the unsuccessful attempts have to be logged by the monitoring system.

The users have to use strong passwords. A password management system should ensure the quality of passwords. Users could be identified by biometric authentication, tokens and smart cards. A combination of technologies and mechanisms make a stronger authentication. The strength level of the identification should be accorded to the sensitivity of the information accessed.

The operation systems should shut down inactive sessions automatically after a defined time. GPO can be used to enforce this controls, and there is multiples solution for 2 ways authentication even if the computers cannot be changed, there is some USB token solutions available.

9.4 Application and information access control

There is a good base for application and information access control with personal folder and sensitive data encrypted.

However, applications need to be protected as well because usually sensitive data are in applications.

Users should only access to applications based on individual business requirements. Applications that are able to overwrite OS rights should be avoided or monitored when essential. The access rights between applications should be controlled too.

GPO on Windows server can be used to restrict rights on applications. Sensitive applications should be isolated by having their dedicated computing environment. If the isolation is not possible, all risks should be identified and accepted by the owner of the sensitive application.

10 Information Security Events and Weaknesses

10.1 Reporting Information Security and Events Management

Objective: To handle the information security events and weaknesses related with information security in an effective way.

10.1.1 Company's Situation

I found that the company have no incident management and report point. In addition, if incidents occurs employees, contractors and third party users have no deadline to report those incidents because there is no procedure of reporting incidents. Moreover, company do not have any duress alarm in the high security area. Company do not make record of the previous incidents occurrence. There is no user awareness training about the incident which were occurred before.

10.1.2 Problems

This is not a good strategy because no one have any responsibility towards the security such as they can report the incident whenever they have time, not immediately. Incident management is missing and it leads to fixing the problems again and again because company do not record the incident occurrence which reduce the awareness to respond to such events in an effective e way to avoid them in future.

10.1.3 Solutions

Control: All the incidents related to the information security should be reported to the incident management as fast as possible.

Implementation Guidance: A complete formal procedure about reporting incidents should be established which must include the procedure about taking actions against the reported incidents. A well know office or point of contact is required where everyone can easily access and report the incidents. The point of contact must be always available and it should provide appropriate feedback to those who reported the incidents after it has been fixed. The event reporting forms are required and must be carefully designed in order to get all the necessary information such as type of non-compliance or breach and messages on the screen. The employees, contractors and third party users must know their responsibilities towards security incidents such as they must immediately report the incident rather than fixing it by themselves. A duress alarm is needed in the high risk area in order to reflect the high risk situation.

10.2 Management of Information Security Incidents and Improvements

Objective: To deal with the information security incidents in an adequate and logical way.

10.2.1 Company's Situation

As I mentioned before that company do not have any incident management, therefore it results in to lack of effective approach to handle the incidents. Moreover, when incident is detected company do no try to collect the legal evidence against the person or organisation who is responsible for it. However, company have one lawyer who handles all the legal issues if it they go beyond the limits of company's IT administrator. In addition, company is only using a firewall to identify information security incidents.

10.2.2 Problems

This strategy does not provide effective approach to handle the incidents because company have only one person (IT administrator) who have responsibility to fix all the incidents. In addition, this strategy also leads to lack of continual improvement in the form of monitoring and evaluating the incidents. Company is also compromising with the legal requirements such as not collecting evidence or taking action against the breacher.

10.2.3 Solutions

Control: In order to response fast and effective against security incidents; procedures and management responsibilities should be developed.

Implementation Guidance: Along with the development of incident management, detecting devices are required to identify the incidents such as monitoring of systems, alert and vulnerabilities. There should be the procedures which can handle and identify different types of incidents such as malicious code, system failure, loss of service, breaches of integrity and errors. In addition, analysis and identification of the cause, planning and implementation of corrective data to reduce recurrence of incidents and reporting the activity to higher authority are the other factors which must be included in the procedure. All the information gained after performing the evaluation must be recorded in order to use it to identify the occurrence of incident. It is recommended to collect the evidence and inform the lawyer or police at the early stage if incident is detected for taking legal action because may be the seriousness of the incident will not show up in the beginning and later when it shows company do not have or destroyed the evidence.

11 Business Continuity Management

11.1 Information Security Aspects of Business Continuity Management

Objective: To act against any breach such as system failure and natural disaster and establish their timely reformation in order to protect business movements and processes.

11.1.1 Company's Situation

Company have no effective business continuity plans *(using paper and pen is not effective)* to deal with natural disasters, accidents and equipment failures. In addition, there is no continuity management that can address the security needs for the company.

11.1.2 Problems

Due to lack of business continuity plans, company can face huge loss. Using pen and paper can be costly and reduce the speed of work tasks.

11.1.3 Solutions

Control: Develop the business continuity plans and continuity management process to limit the occurrence and consequences of the incidents.

Implementation Guidance: Events that cause disruption must be identified. In your company case, there is no such management that can do risk assessment. Without risk assessment, it is not possible to develop business continuity strategy. Once the company established the business continuity management then a continuity plan should be developed on the basis of the result of risk assessment. This plan will help to maintain the availability of company resources at a required level in the case of emergency, failure and interruption. The business continuity plans must focus on the business objectives such as if failure occurs how should company react and how will company continue the work during the recovery of the indents. In other words, company need some extra equipments which can be used during the occurrence of incidents. These equipment may include arrangements with other parties such as third parties in the shape of reciprocal agreement. Business continuity plans should also include temporary location during emergency and the level of security controls must be at same level as at the main site.

Control: The business continuity plans should be tested and updated on regular basis in order to make sure that these plans are up to date and effective.

Implementation Guidance: Develop the test schedule and procedure which clearly describes how and when each plan should be tested. It is recommended to test each of them frequently and number of times. IT staff and other relevant people *(Only 1 IT administrator is not enough)* must aware with their responsibilities and roles when a plan is carried out. There are various techniques that can be used for testing such as create an incident scenario and discuss the recovery arrangements related to it, technical recovery testing and testing plan at an alternative site such as temporary position which should be used during any disaster.

12 Compliance

12.1 Compliance with Legal Requirements

Objective: To stop any breach related to law, regulatory obligations and security requirements.

12.1.1 Company's Situation

Company have one legal advisor who handle all the problems related to the law. In addition, company protect its important data according to law and business requirements but company do not use cryptographic controls on saving the important data. However, company do have disclosure agreement with their employees during the time of employment.

12.1.2 Problems

Disclosure agreement is not completely reliable for meeting the standard of ISO27001. Company must perform encryption on the confidential data before uploading it on cloud based service.

12.1.3 Solution

Control: Cryptographic controls should be implemented for saving confidential data.

Implementation Guidance: Encrypt the data before uploading/saving it in order to decrease the threat of information breach.

12.2 Compliance with Security Policies and Standards and Technical Compliance

Objective: To develop observance of systems including supervising security policies and standards.

12.2.1 Company's Situation

Company do not perform regular reviewing of information system. The IT administrator reviews the system once a year. Company do not make a record of reviews and also have lack of technical reports about the system.

12.2.2 Problems

Due to lack of supervision and regular reviews, company's IT administrator might not have clear knowledge whether hardware and software are implemented correctly. There is a high risk of breach because company's strategy is to solve the incidents not prevent the incidents.

12.2.3 Solutions

Control: Divide responsibility among the people within their site. Perform Regular check up.

Implementation Guidance: Assign different people in different areas rather than having 1 IT administrator. They must be aware of their responsibilities and carry out regular check up with their area of responsibility. During the regular review if they found any non-compliance they must find the cause of it, take appropriate actions and evaluate it as well as prevent the recurrence. Once they evaluated the incident they must record it and the record should be well maintained. Furthermore, test the system regularly. For testing, appropriate tools or softwares must be used which produce a technical report of the system. These test should only be perform by authorised persons or under their supervision. Monitoring the system on regular is best practise of testing.