

Linnaeus University

1DV700 - Computer Security

Assignment 3

Individual work

Student\_ID: rs223fx



# Introduction

## This document aims to summarise the policies of physical and environmental security (Chapter 11), operations security (Chapter 12) and communications security (Chapter 13) from ISO 27002.

1. **Physical and environmental security (Chapter 11)**

Each perimeter should have its security requirements. These should be designed to protect different assets within the facility. Control measures should be in place to prevent unauthorized access to the site or building. For example, an intruder detection system should be installed at the entrances. Workers should ensure lockage of doors and windows when exiting the facility. Access to the site should be available only for authorized individuals. Visitors should authenticate themselves and be recorded if necessary. Areas where confidential information is stored should be allowed only to authorized individuals. Access control mechanisms for such areas should be considered. Organization should have electronic audit trail where all access is to the cite is documented. All employees should be required to carry visible identifications. A specialist should also advise how to protect the facilities in case of natural disaster. Secure areas should be known by individuals by need-to-know basis and devices with recording equipment to these areas should not be allowed.

Securing assets with sensitive information from being leaked should be considered. Should be ensured correct functionality of all equipment. Power and telecommunications data cables should be checked with technical sweeps and physical inspections for unauthorized devices attached to them. Only authorized individuals should perform maintenance on equipment. These individuals should also ensure that maintained equipment is not malfunctioning. In case of maintenance performed by external organization, confidential information should be cleared from the equipment. The identity of the individuals who used this equipment should be documented. Equipment should not be left unattended while using off-site. When equipment is transferred site-off between individuals, a log including name and organization should be maintained. Sensitive data should be securely deleted from assets, and encryption should be applied to prevent it from being recovered or destroyed. All electronic equipment containing confidential information should be secured with passwords or biometric authentication mechanisms. Media with sensitive or secret content should be deleted immediately from these reproductive technologies.

1. **Operations security (Chapter 12)**

Operating procedures should be documented and accessible to all users who need them. These procedures should include installation and configuration, processing, and handling of information both automated and manual, backing up the system, accessing technical support and escalation contacts, instructions for error handling to avoid interruption at work, confidential information handling, system restart and recovery instructions, audit-trail and log instructions, monitoring procedures. Identification and recording of significant changes should be kept, and planning and the testing of them also if necessary. The influence of changes on the system and a backup plan for unsuccessful implementation should be considered. Authorised individuals should approve that requirements have been met and reported for these changes. Deletion of unnecessary data to achieve better system performance should be trained. Optimisation of system logic and restricting hungry services should also be considered for better system performance. Software testing and development environment should be separated from the operational environment. Test environments should not have access to any development tools used in the workspace if not required. Users should use different accounts, and any confidential info should be kept away from the test environments when not required.

Black and whitelist controls should be considered to prevent or detect the use of unauthorized software. Malware detection tools which can scan for harmful software should also be considered. These tools should be regularly checked and kept up to date. Control measures should be implemented for regular information collecting from the network. Having a backup copy of all critical data should be considered. These copies should be regularly checked and kept up to date in a remote location away from the cite. Event logs should be used. Audit logs should be checked regularly. Clocks should be synchronized. Only authorized individuals should install and modify code or scripts. These additions should be checked for security and suitability with the rest of the system in the test environment before implementation. In case of system failure, the system should have ability to be returned to an earlier state. In case of vulnerability identification, the organization should define responsibilities and perform a hazard analysis. If patch is available from a legitimate source risk analysis should be made, otherwise patches should be remade, or other temporary controls should be applied. Log should be kept and procedures and systems at high risk should be addressed first. Organization should have strict policies of software installation backed by monitoring if required.

1. **Communications security (Chapter 13)**

Network controls are designed to protect the confidentiality, integrity, and availability of information stored within a network. These controls should ensure prevention of unauthorised access to the network, wireless network and connected system applications. Monitoring the network should be considered to secure it from flaws. System connection to a network should be restricted and only authenticated systems should be used over the network. Responsibilities for networks and computer operations should be separated. Features such as authentication, encryption, connection controls and restriction of access to network services or applications should be considered. For large networks segregation should be considered with dividing it into separate network domains. These domains can be chosen based on appropriate trust levels and organizational units. Access between segregated networks should be controlled using gateway. Organizations should ensure having policies regarding the protection of transferred information and attachments. Policies against compromising the organization and proper usage of email should be implemented as well. Cryptographic techniques should be used to protect confidentiality, integrity, and authenticity of information. No confidential information should be transferred over insecure network. Agreements should ensure that transfers are traceable and non-repudiation. Electronic messages should be protected from attacks on the transfer process and should be transported to the correct address. Should be considered implementation of watermarks or signatures to ensure integrity. Should be considered having terms for the information when the agreement period is over and additionally in case of agreement breaches.

Questions:

1. How many access points are on point to enter the facility?
2. How currently the access points are secured?
3. How it is defined who can get access to secure areas and how they get that access?
4. How often correct functionality of the equipment is checked and by who?
5. Is there a procedure and/or policy that is on point in case of required maintenance of critical for the workflow equipment? For example, burnt hard disk of the server.
6. Does the organization have policies regarding expiry of information value after a certain time when it is published? If so, can we see the policy?
7. How does the organization currently handle new implementations to the system? Please provide detailed information.
8. Does the organization prefers storing the information remotely or on the cloud storage or on both?
9. What is currently being done with the documents when agreement period is over between the organizations?
10. Can we get statistics about how often users forget their passwords If you have one at the workplace or how often do, they forget to lock the door or log out of the applications after work? Does the human factor (human errors such as forgetting or mistyping an information piece) happens often?

Resource: Information technology — Security techniques — Code of practice for information security controls, ISO/IEC 27002, Second edition 2013-10-01, Available:   
[<https://mymoodle.lnu.se/pluginfile.php/6753796/mod_resource/content/2/ISO_IEC_27002_2013.pdf>]