Insert Company Logo

# Operating Procedures for Information and Communication Technology

Document Control

| | |
|---|---|
| **Document Number:** | ISMS-PRO-007 |
| **Version Number:** | 1 |
| **Review Date:** | Insert date |
| **Next Review:** | Insert date |
| **Authorised by:** | Insert Job Title and Department |

Version History

| Version | Date | Author | Brief Description of Changes |
|---|---|---|---|
| 1 | Insert Effective Date | Insert author | Describe changes that were made to document in order to qualify changing the version. |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 1. Purpose

The purpose of this document is to ensure correct and secure functioning of information and communication technology.

## 2. Scope

This document applies to employees of Insert Company Name's unit for information and communication technology.

## 3. References

- ISO 27001:2013 Annexures A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2
- Information Security Policy
- Acceptable Use Policy
- Inventory of Assets
- Supplier Security Policy



## 4. Operating Procedures for Information and Communication Technology

### 4.1 Change management

Each change to operational or production systems must be made in the following way:

- change may be proposed by Insert position of authority and Insert position of authority by creating a record in the "Provide file of the server" on Provide location on server. A Specification of Information System Requirements should be attached to the change request record for new information requests
- An associated risk assessment entry must be created in Provide file of the server on Provide location on server.
- change must be authorized by Insert position of authority or Insert position of authority depending on who is requesting the change, who must assess its justification for business and potential negative security impacts
- changes must be implemented by Insert position of authority or Insert position of authority
- Insert position of authority or Insert position of authority is responsible for checking that the change has been implemented in accordance with the requirement
- Insert position of authority or Insert position of authority is responsible for testing and verifying the system's stability – the system must not be put into production before thorough testing has been conducted
- implementation of changes must be reported to the following persons: Insert position of authority or Insert position of authority

Change records are kept on Provide location on server in the "Provide file of the server (e.g. Operational /Production Systems Change Requests).

### 4.2 Network security management

Security Officers are responsible for managing and controlling the computer networks, for ensuring the security of information in networks, and for protecting the services connected to the networks from unauthorized access. It is therefore necessary:

- to separate the operational responsibility for networks from the responsibility for sensitive applications and other systems
- to protect sensitive data passing over the public network by ensuring applications are accessed over SSL connections
- to protect sensitive data passing over wireless networks by enabling strong encryption on the Wifi device
- to segregate traffic coming in from mobile devices, set up unique firewall policies, static routes, Virtual Local Area Networks, etc.
- to ensure the availability of network services by utilizing credible, recognized vendors in terms of internet breakout

## 5. Disposal and destruction of equipment and media

All data and licensed software stored on mobile storage media (e.g. on CD, DVD, USB flash drive, memory card, etc.; but also on paper) and on all equipment containing storage media (e.g. computers, mobile phones, etc.) must be erased or the medium destroyed before it is disposed of or reused.

The person responsible for erasing data / destroying media must inform the owner of the asset in question about erasing/destroying, and the asset owner must update the Inventory of Assets.

### 5.1 Equipment

Security Officers are responsible for authorizing, checking and erasing data from equipment. Data must be erased, but if the process is not secure enough considering the sensitivity of the data, then the storage medium must be destroyed.

### 5.2 Mobile storage media

Security Officer is responsible for delegating the erasing of data from mobile storage media. Data must be erased completely but if the erasure process is not secure enough considering the sensitivity of the data, then the storage medium must be destroyed.

### 5.3 Paper media

Employees of the organization handling individual documents are responsible for destroying paper documents. Paper documents are destroyed by using the paper shredder in the offices.

## 6. Information transfer

### 6.1 Electronic communication channels

Organization's information may be exchanged through the following electronic communication channels: e-mail, download of files from the Internet, transfer of data via Insert Company Name Cloud Room, telephones, fax machines, SMS text messages, portable media, and forums and social networks.

When sensitive data is being exchanged between Insert Company Name users and client users for purposes of support or assistance, as far as possible, the data should be secured in a password protected manner i.e. password protect zip file, excel password protect sheet etc. and the password should be provided to the respective user through a different channel than that of the channel being used to send the data i.e. data is sent as an attachment in an email, password sent in a different email or communicated telephonically.

Security Officers prescribes additional controls for each type of data and communication channel, based on risk assessment results.

### 6.2 Relations with external parties

External parties who have access to or handle any data relating to Insert Company Name or Insert Company Name's clients must sign an agreement, which is the responsibility of Security Officer, according to the Supplier Security Policy.



## 7. System monitoring

Based on the risk assessment results, the Insert position of authority decides which logs will be kept on which systems and for which systems, and how long they will be stored. Logs must be kept for all administrators and system operators on sensitive systems.

Security Officers are responsible for monitoring the logs of automatically reported faults on a daily basis, as well as to register faults reported by users, to analyze why errors occurred and to take appropriate corrective actions.

Security Officers are responsible for regularly reviewing logs in order to monitor the activities of users, administrators and system operators. The review is conducted at intervals prescribed by the Insert position of authority who determines and selects the records to be reviewed, and how the implemented review will be recorded. The Insert position of authority must be informed about the results of the review.

## 8. Validity and document management

This document is valid as of insert date.

The owner of this document is Insert position of authority, who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of incidents related to the secure functioning of ICT systems
- number of incidents due to unclear responsibilities for the functioning of ICT systems