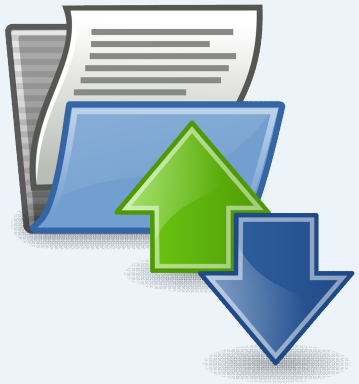
ISO/IEC 27001:2013 Information security management systems
-Information transfer-

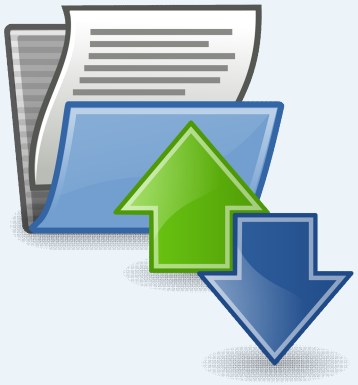
Security category – 13.2. Information transfer

Control – 13.2.1. Information transfer policies and procedures
The organization should have transfer policies, procedures and controls to protect the transfer of information for all types of communication facilities.



Exchange of information carry the risk of the information being compromised.

ISO/IEC 27001:2013 Information security management systems
-Information transfer-

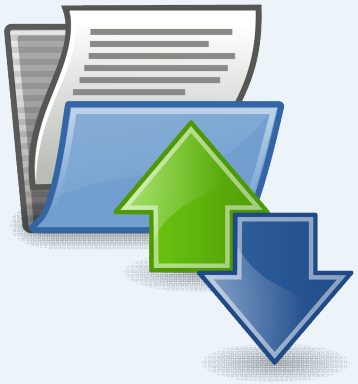


General guidelines for rules and procedures on information transfer:

- rules to protect against malware that can be transmitted through the use of electronic communications;
- rules for the acceptable use of communication facilities;
- explicit rules forbidding employees to compromise the organization (ex. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing);
- encrypt information (if needed);
- rules on the retention and disposal of business correspondence;
- not leaving messages containing confidential information on answering machines since these may be replayed by unauthorized persons;
- not leaving sensitive information in printers or fax machines;
- personnel reminded not to have confidential conversations in public places or through insecure communication channels.

Rules should be communicated to all staff.

ISO/IEC 27001:2013 Information security management systems
-Information transfer-



Control – 13.2.2. Agreements on information transfer
The organization should include in agreements with other parties the secure transfer of business information.

ISO/IEC 27002 recommends to document in the contracts the level of security expected for sensitive information passing between organizations and the controls applied.

Example elements to be included in the contracts:

- management responsibilities for controlling and notifying transmission, dispatch and receipt;
- procedures to ensure traceability and non-repudiation;
- minimum technical standards for packaging and transmission;
- escrow agreements;
- courier identification;
- responsibilities and authorities in case of security incidents;
- agreeing on a common system of labelling information between the parties.

ISO/IEC 27001:2013 Information security management systems
-Information transfer-

Control – 13.2.3. Electronic messaging
Information exchanged through electronic messaging should be appropriately protected.

Email involves many risks if used without appropriate controls.
(ex. financial fraud, infection, legal issues)

There should be some rules or procedures in place for the use of email and its essential that staff are aware of: the risks involved, the organization's requirements and the control mechanisms in place.

ISO/IEC 27001:2013 Information security management systems
-Information transfer-

Control – 13.2.4. Confidentiality or non-disclosure agreements
The organization should have suitable confidentiality and non-disclosure agreements that are in line with the needs for the protection of information.

Before giving access to confidential information - to employees or external personnel and organizations the organization should ensure that confidentiality agreements are signed.

Elements to be included in the non-disclosure agreements:
- a definition of the information to be protected (ex. confidential information);
- ownership of information and the rights to use confidential information by the signatories;
- expected duration of the agreement, including cases where confidentiality might need to be maintained indefinitely
- responsibilities and actions of the signatories to avoid information being disclosed;
- the process of notification and reporting in case of unauthorized access to confidential information;
- expected actions in case the agreement is breached