

ISO/IEC 27001 - Structure of Controls

5. Security Policy

5.1 Information Security Policy

- 5.1.1 Information security policy document
- 5.1.2 Review of information security policy document

6. Organization of information security

6.1 Internal Organization

- 6.1.1. Management commitment to information security
- 6.1.2. Information security coordination
- 6.1.3. Allocation of information security responsibilities
- 6.1.4. Authorization process for information processing facilities
- 6.1.5. Confidentiality agreements
- 6.1.6. Contact with authorities
- 6.1.7. Contact with special interest groups
- 6.1.8. Independent review of information security

6.2 External parties

- 6.2.1. Identification of risks related to external parties
- 6.2.2. Addressing security when dealing with customers.
- 6.2.3. Addressing security in third party agreements

7. Asset management

7.1 Responsibility for assets

- 7.1.1 Inventory of assets
- 7.1.2 Ownership of assets
- 7.1.3 Acceptable use of assets

7.2 Information Classification

- 7.2.1 Classification guidelines
- 7.2.2 Information labeling and handling

8. Human resources security

8.1 Prior to employment

- 8.1.1 Roles and responsibilities
- 8.1.2 Screening
- 8.1.3 Terms and conditions of employment

8.2 During employment

- 8.2.1 Management responsibilities
- 8.2.2 Information security awareness, education and training
- 8.2.3 Disciplinary process

8.3 Termination or change of employment

-
- 8.3.1 Termination responsibilities
 - 8.3.2 Return of assets
 - 8.3.3 Removal of access rights

9. Physical and environmental security

9.1 Secure areas

- 9.1.1 Physical security perimeter
- 9.1.2 Physical entry controls
- 9.1.3 Security offices, rooms and facilities
- 9.1.4 Protecting against external and environmental threats
- 9.1.5 Working in secure areas
- 9.1.6 Public access, delivery and loading areas

9.2 Equipment security

- 9.2.1 Equipment siting and protection
- 9.2.2 Supporting utilities
- 9.2.3 Cabling security
- 9.2.4 Equipment maintenance
- 9.2.5 Security of equipment off-premises
- 9.2.6 Secure disposal or re-use of equipment
- 9.2.7 Removal of property

10 Communications and operations management

10.1 Operational procedures and responsibilities

- 10.1.1 Documented operating procedures
- 10.1.2 Change Management
- 10.1.3 Segregation of duties
- 10.1.4 Separation of development, test and operational facilities

10.2 Third party service delivery management

- 10.2.1 Service delivery
- 10.2.2 Monitoring and review of third party services
- 10.2.3 Managing changes to third party services

10.3 System planning and acceptance

- 10.3.1 Capacity management
- 10.3.2 System acceptance

10.4 Protection against malicious and mobile code

- 10.4.1 Controls against malicious code
- 10.4.2 Controls against mobile code

10.5 Backup

- 10.5.1 Information back-up

10.6 Network security management

- 10.6.1 Network controls
- 10.6.2 Security of network services

10.7 Media handling

- 10.7.1 Management of removable media
- 10.7.2 Disposal of media
- 10.7.3 Information handling procedures
- 10.7.4 Security of system documentation

10.8 Exchange of information

- 10.8.1 Information exchange policies and procedures
- 10.8.2 Exchange agreements
- 10.8.3 Physical media in transit
- 10.8.4 Electronic messaging
- 10.8.5 Business information systems

10.9 Electronic commerce services

- 10.9.1 Electronic commerce
- 10.9.2 On-line transactions
- 10.9.3 Publicly available information

10.10 Monitoring

- 10.10.1 Audit logging
- 10.10.2 Monitoring system use
- 10.10.3 Protection of log information
- 10.10.4 Administrator and operator logs
- 10.10.5 Fault logging
- 10.10.6 Clock synchronisation

11 Access control

11.1 Business requirement for access control

- 11.1.1 Access control policy

11.2 User access management

- 11.2.1 User registration
- 11.2.2 Privilege management
- 11.2.3 User password management
- 11.2.4 Review of access rights

11.3 User responsibilities

- 11.3.1 Password use
- 11.3.2 Unattended user equipment
- 11.3.3 Clear desk and clear screen policy

11.4 Network access control

- 11.4.1 Policy on use of network services
- 11.4.2 User authentication for external connections
- 11.4.3 Equipment identification in networks
- 11.4.4 Remote diagnostic and configuration port protection
- 11.4.5 Segregation in networks

11.4.6 Network connection control

11.4.7 Network routing control

11.5 Operation system access control

11.5.1 Secure log-on procedures

11.5.2 User identification and authentication

11.5.3 Password management system

11.5.4 Use of system utilities

11.5.5 Session time-out

11.5.6 Limitation of connection time

11.6 Application and information access control

11.6.1 Information access restriction

11.6.2 Sensitive system isolation

11.7 Mobile computing and teleworking

11.7.1 Mobile computing and communications

11.7.2 Teleworking

12 Information systems acquisition, development and maintenance

12.1 Security requirements of information systems

12.1.1 Security requirements analysis and specification

12.2 Correct processing in applications

12.2.1 Input data validation

12.2.2 Control of internal processing

12.2.3 Message integrity

12.2.4 Output data validation

12.3 Cryptographic controls

12.3.1 Policy on the use of cryptographic controls

12.3.2 Key management

12.4 Security of system files

12.4.1 Control of operational software

12.4.2 Protection of system test data

12.4.3 Access control to program source code

12.5 Security in development and support processes

12.5.1 Change control procedures

12.5.2 Technical review of applications after operating system changes

12.5.3 Restrictions on changes to software packages

12.5.4 Information leakage

12.5.5 Outsourced software development

12.6 Technical Vulnerability Management

12.6.1 Control of technical vulnerabilities

13 Information security incident management

13.1 Reporting information security events and weaknesses

13.1.1 Reporting information security events

13.1.2 Reporting information security weaknesses

13.2 Management of information security incidents and improvements

13.2.1 Responsibilities and procedures

13.2.2 Learning from security incidents

13.2.3 Collection of evidence

14 Business Continuity Management

14.1 Information security aspects of business continuity management

14.1.1 Including information security in the business continuity management process

14.1.2 Business continuity and risk assessment

14.1.3 Developing and implementing continuity plans including information security

14.1.4 Business continuity planning framework

14.1.5 Testing, maintaining and re-assessing business continuity plans

15 Compliance

15.1 Compliance with legal requirements

15.1.1 Identification of applicable legislation

15.1.2 Intellectual property rights (IPR)

15.1.3 Protection of organizational records

15.1.4 Data protection and privacy of personal information

15.1.5 Prevention of misuse of information processing facilities

15.1.6 Regulation of cryptographic controls

15.2 Compliance with security policies and standards, and technical compliance

15.2.1 Compliance with security policies and standards

15.2.2 Technical compliance checking

15.3 Information systems audit considerations

15.3.1 Information systems audit controls

15.3.2 Protection of information systems audit tools