## ISO 27002

### A.5 Security Policy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 5.1 Information Security Policy | | | | |
| 5.1.1 | Information security policy document | An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. |  |  |
| 5.1.2 | Review of the information security policy | The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. |  |  |

### A.6 Organization of Information Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 6.1 Internal Organization | | | | |
| 6.1.1 | Management commitment to information security | Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. |  |  |
| 6.1.2 | Information security co-ordination | Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions. |  |  |
| 6.1.3 | Allocation of information security responsibilities | All information security responsibilities should be clearly defined. |  |  |
| 6.1.4 | Authorization process for information processing facilities | A management authorization process for new information processing facilities should be defined and implemented. |  |  |
| 6.1.5 | Confidentiality agreements | Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information should be identified and regularly reviewed. |  |  |
| 6.1.6 | Contact with authorities | Appropriate contacts with relevant authorities should be maintained. |  |  |
| 6.1.7 | Contact with special interest groups | Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. |  |  |
| 6.1.8 | Independent review of information security | The organization’s approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur. |  |  |
| 6.2 External Parties | | | | |
| 6.2.1 | Identification of risks related to external parties | The risks to the organization’s information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access. |  |  |
| 6.2.2 | Addressing security when dealing with customers | All identified security requirements should be addressed before giving customers access to the organization’s information or assets. |  |  |
| 6.2.3 | Addressing security in third party agreements | Agreements with third parties involving accessing, processing, communicating or managing the organization’s information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements. |  |  |

### A.7 Asset Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 7.1 Responsibility for Assets | | | | |
| 7.1.1 | Inventory of assets | All assets should be clearly identified and an inventory of all important assets drawn up and maintained. |  |  |
| 7.1.2 | Ownership of assets | All information and assets associated with information processing facilities should be owned by a designated part of the organization. |  |  |
| 7.1.3 | Acceptable use of assets | Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented. |  |  |
| 7.2 Information Classification | | | | |
| 7.2.1 | Classification Guidelines | Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization. |  |  |
| 7.2.2 | Information labeling and handling | An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization. |  |  |

### A.8 Human Resources Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 8.1 Prior to Employment | | | | |
| 8.1.1 | Roles and Responsibilities | Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization’s information security policy. |  |  |
| 8.1.2 | Screening | Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. |  |  |
| 8.1.3 | Terms and conditions of employment | As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization’s responsibilities for information security. |  |  |
| 8.2 During Employment | | | | |
| 8.2.1 | Management responsibilities | Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. |  |  |
| 8.2.2 | Awareness, education, and training | All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. |  |  |
| 8.2.3 | Disciplinary process | There should be a formal disciplinary process for employees who have committed a security breach. |  |  |
| 8.3 Termination or change of employment | | | | |
| 8.3.1 | Termination responsibilities | Responsibilities for performing employment termination or change of employment should be clearly defined and assigned. |  |  |
| 8.3.2 | Return of assets | All employees, contractors and third party users should return all of the organization’s assets in their possession upon termination of their employment, contract or agreement. |  |  |
| 8.3.3 | Removal of access rights | The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change. |  |  |

### A.9 Physical and Environmental Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 9.1 Secure areas | | | | |
| 9.1.1 | Physical security perimeter | Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities. |  |  |
| 9.1.2 | Physical entry controls | Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. |  |  |
| 9.1.3 | Securing offices, rooms, facilities | Physical security for offices, rooms, and facilities should be designed and applied. |  |  |
| 9.1.4 | 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. |  |  |
| 9.1.5 | Working in secure areas | Physical protection and guidelines for working in secure areas should be designed and applied. |  |  |
| 9.1.6 | Public access, delivery and loading areas | 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. |  |  |
| 9.2 Equipment security | | | | |
| 9.2.1 | Equipment siting and protection | Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |  |  |
| 9.2.2 | Supporting utilities | Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. |  |  |
| 9.2.3 | Cabling security | Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. |  |  |
| 9.2.4 | Equipment maintenance | Equipment should be correctly maintained to ensure its continued availability and integrity. |  |  |
| 9.2.5 | Security of equipment off-premises | Security should be applied to off-site equipment taking into account the different risks of working outside the organization’s premises. |  |  |
| 9.2.6 | Secure disposal or reuse of equipment | All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. |  |  |
| 9.2.7 | Removal of property | Equipment, information or software should not be taken off-site without prior authorization. |  |  |

### A.10 Communications and Operations Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 10.1 Operational procedures and responsibilities | | | | |
| 10.1.1 | Documented operating procedures | Operating procedures should be documented, maintained, and made available to all users who need them. |  |  |
| 10.1.2 | Change management | Changes to information processing facilities and systems should be controlled. |  |  |
| 10.1.3 | Segregation of duties | Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets. |  |  |
| 10.1.4 | Separation of development, test and operational facilities | Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system. |  |  |
| 10.2 Service delivery | | | | |
| 10.2.1 | Service delivery | It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party. |  |  |
| 10.2.2 | Monitoring and review of third-party services | The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly. |  |  |
| 10.2.3 | Managing changes to third-party services | Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks. |  |  |
| 10.3 System planning and acceptance | | | | |
| 10.3.1 | Capacity management | The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance. |  |  |
| 10.3.2 | System acceptance | Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance. |  |  |
| 10.4 Protection against malicious and mobile code | | | | |
| 10.4.1 | Controls against malicious code | Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented. |  |  |
| 10.4.2 | Controls against mobile code | Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing. |  |  |
| 10.5 Backup | | | | |
| 10.5.1 | Information Backup | Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy. |  |  |
| 10.6 Network security management | | | | |
| 10.6.1 | Network controls | Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit. |  |  |
| 10.6.2 | Security of network services | Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced. |  |  |
| 10.7 Media handling | | | | |
| 10.7.1 | Management of removable media | There should be procedures in place for the management of removable media. |  |  |
| 10.7.2 | Disposal of media | Media should be disposed of securely and safely when no longer required, using formal procedures. |  |  |
| 10.7.3 | Information handling procedures | Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse. |  |  |
| 10.7.4 | Security of system documentation | System documentation should be protected against unauthorized access. |  |  |
| 10.8 Exchange of information | | | | |
| 10.8.1 | Information exchange policies and procedures | Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. |  |  |
| 10.8.2 | Exchange agreements | Agreements should be established for the exchange of information and software between the organization and external parties. |  |  |
| 10.8.3 | Physical media in transit | Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization’s physical boundaries. |  |  |
| 10.8.4 | Electronic messaging | Information involved in electronic messaging should be appropriately protected. |  |  |
| 10.8.5 | Business information systems | Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems. |  |  |
| 10.9 Electronic commerce services | | | | |
| 10.9.1 | Electronic commerce | Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. |  |  |
| 10.9.2 | Online transactions | Information involved in on-line transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. |  |  |
| 10.9.3 | Publicly available information | The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification. |  |  |
| 10.10 Monitoring | | | | |
| 10.10.1 | Audit logging | Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring. |  |  |
| 10.10.2 | Monitoring system use | Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly. |  |  |
| 10.10.3 | Protection of log information | Logging facilities and log information should be protected against tampering and unauthorized access. |  |  |
| 10.10.4 | Administrator and operator logs | System administrator and system operator activities should be logged. |  |  |
| 10.10.5 | Fault logging | Faults should be logged, analyzed, and appropriate action taken. |  |  |
| 10.10.6 | Clock synchronization | The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source. |  |  |

### A.11 Access Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 11.1 Business requirement for access control | | | | |
| 11.1.1 | Access control policy | An access control policy should be established, documented, and reviewed based on business and security requirements for access. |  |  |
| 11.2 User access management | | | | |
| 11.2.1 | User registration | There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. |  |  |
| 11.2.2 | Privilege management | The allocation and use of privileges should be restricted and controlled. |  |  |
| 11.2.3 | User password management | The allocation of passwords should be controlled through a formal management process. |  |  |
| 11.2.4 | Review of user access rights | Management should review users’ access rights at regular intervals using a formal process. |  |  |
| 11.3 User responsibilities | | | | |
| 11.3.1 | Password use | Users should be required to follow good security practices in the selection and use of passwords. |  |  |
| 11.3.2 | Unattended user equipment | Users should ensure that unattended equipment has appropriate protection. |  |  |
| 11.3.3 | Clear desk and clear screen policy | A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted. |  |  |
| 11.4 Network access control | | | | |
| 11.4.1 | Policy on use of network services | Users should only be provided with access to the services that they have been specifically authorized to use. |  |  |
| 11.4.2 | User authentication for external connections | Appropriate authentication methods should be used to control access by remote users. |  |  |
| 11.4.3 | Equipment identification in networks | Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment. |  |  |
| 11.4.4 | Remote diagnostic and configuration port protection | Physical and logical access to diagnostic and configuration ports should be controlled. |  |  |
| 11.4.5 | Segregation in networks | Groups of information services, users, and information systems should be segregated on networks. |  |  |
| 11.4.6 | Network connection control | For shared networks, especially those extending across the organization’s boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1). |  |  |
| 11.4.7 | Network routing control | Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. |  |  |
| 11.5 Operating system access control | | | | |
| 11.5.1 | Secure log-on procedures | Access to operating systems should be controlled by a secure log-on procedure. |  |  |
| 11.5.2 | User identification and authentication | All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user. |  |  |
| 11.5.3 | Password management system | Systems for managing passwords should be interactive and should ensure quality passwords. |  |  |
| 11.5.4 | Use of system utilities | The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. |  |  |
| 11.5.5 | Session time-out | Inactive sessions should shut down after a defined period of inactivity. |  |  |
| 11.5.6 | Limitation of connection time | Restrictions on connection times should be used to provide additional security for high-risk applications. |  |  |
| 11.6 Application and information access control | | | | |
| 11.6.1 | Information access restriction | Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy. |  |  |
| 11.6.2 | Sensitive system isolation | Sensitive systems should have a dedicated (isolated) computing environment. |  |  |
| 11.7 Mobile computing and teleworking | | | | |
| 11.7.1 | Mobile computing and communications | A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities. |  |  |
| 11.7.2 | Teleworking | A policy, operational plans and procedures should be developed and implemented for teleworking activities. |  |  |

### A.12 Information Systems Acquisition, Development and Maintenance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 12.1 Security requirements of information systems | | | | |
| 12.1.1 | Security requirements analysis and specification | Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls. |  |  |
| 12.2 Correct processing in applications | | | | |
| 12.2.1 | Input data validation | Data input to applications should be validated to ensure that this data is correct and appropriate. |  |  |
| 12.2.2 | Control of internal processing | Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. |  |  |
| 12.2.3 | Message integrity | Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented. |  |  |
| 12.2.4 | Output data validation | Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. |  |  |
| 12.3 Cryptographic controls | | | | |
| 12.3.1 | Policy on the use of cryptographic controls | A policy on the use of cryptographic controls for protection of information should be developed and implemented. |  |  |
| 12.3.2 | Key management | Key management should be in place to support the organization’s use of cryptographic techniques. |  |  |
| 12.4 Security of system files | | | | |
| 12.4.1 | Control of operational software | There should be procedures in place to control the installation of software on operational systems. |  |  |
| 12.4.2 | Protection of system test data | Test data should be selected carefully, and protected and controlled. |  |  |
| 12.4.3 | Access control to program source code | Access to program source code should be restricted. |  |  |
| 12.5 Security in development and support processes | | | | |
| 12.5.1 | Change control procedures | The implementation of changes should be controlled by the use of formal change control procedures. |  |  |
| 12.5.2 | Technical review of applications after operating system changes | When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. |  |  |
| 12.5.3 | Restrictions on changes to software packages | Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled. |  |  |
| 12.5.4 | Information leakage | Opportunities for information leakage should be prevented. |  |  |
| 12.5.5 | Outsourced software development | Outsourced software development should be supervised and monitored by the organization. |  |  |
| 12.6 Technical Vulnerability Management | | | | |
| 12.6.1 | Control of technical vulnerabilities | Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. |  |  |

### A.13 Information Security Incident Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 13.1 Reporting information security events and weaknesses | | | | |
| 13.1.1 | Reporting information security events | Information security events should be reported through appropriate management channels as quickly as possible. |  |  |
| 13.1.2 | Reporting security weaknesses | All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services. |  |  |
| 13.2 Management of information security incidents and improvements | | | | |
| 13.2.1 | Responsibilities and procedures | Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. |  |  |
| 13.2.2 | Learning from information security incidents | There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. |  |  |
| 13.2.3 | Collection of evidence | Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). |  |  |

### A.14 Business Continuity Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 14.1 Information security aspects of business continuity management | | | | |
| 14.1.1 | Including information security in the business continuity management process | A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization’s business continuity. |  |  |
| 14.1.2 | Business continuity and risk assessment | Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security. |  |  |
| 14.1.3 | Developing and implementing continuity plans including information security | Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. |  |  |
| 14.1.4 | Business continuity planning framework | A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. |  |  |
| 14.1.5 | Testing, maintaining and reassessing business continuity plans | Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective. |  |  |

### A.15 Compliance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Section | Control Name | Control Description | Control Effectiveness | Notes |
| 15.1 Compliance with legal requirements | | | | |
| 15.1.1 | Identification of applicable legislation | All relevant statutory, regulatory, and contractual requirements and the organization’s approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization. |  |  |
| 15.1.2 | Intellectual property rights (IPR) | Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. |  |  |
| 15.1.3 | Protection of organizational records | Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements. |  |  |
| 15.1.4 | Data protection and privacy of personal information | Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. |  |  |
| 15.1.5 | Prevention of misuse of information processing facilities | Users should be deterred from using information processing facilities for unauthorized purposes. |  |  |
| 15.1.6 | Regulation of cryptographic controls | Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations. |  |  |
| 15.2 Compliance with security policies and standards, and technical compliance | | | | |
| 15.2.1 | Compliance with security policies and standards | Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. |  |  |
| 15.2.2 | Technical compliance checking | Information systems should be regularly checked for compliance with security implementation standards. |  |  |
| 15.3 Information systems audit considerations | | | | |
| 15.3.1 | Information systems audit controls | Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes. |  |  |
| 15.3.2 | Protection of information systems audit tools | Access to information systems audit tools should be protected to prevent any possible misuse or compromise. |  |  |