[organization logo]

[organization name]

**STATEMENT OF APPLICABILITY**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415649225)

[2. Reference documents 3](#_Toc415649226)

[3. Applicability of controls 3](#_Toc415649227)

[4. Acceptance of Residual Risks 21](#_Toc415649228)

[5. Validity and document management 22](#_Toc415649229)

# Purpose, scope and users

The purpose of this document is to define which controls are appropriate to be implemented in [organization name], the objectives of these controls and how they are implemented, as well as to approve residual risks and formally approve the implementation of said controls.

This document includes all controls listed in Annex A of the ISO 27001 standard. Controls are applicable to the entire Information Security Management System (ISMS) scope.

Users of this document are all employees of [organization name] who have a role in the ISMS.

# Reference documents

* ISO/IEC 27001 standard, clause 6.1.3 d)
* Information Security Policy
* Risk Assessment and Risk Treatment Methodology
* Risk Assessment and Risk Treatment Report

# Applicability of controls

The following controls from ISO 27001 Annex A are applicable:

| ID | Controls according to ISO/IEC 27001 | Appli-cability (YES/NO) | Justification for selection/ non-selection | Control objectives | Implementation method | Status |
| --- | --- | --- | --- | --- | --- | --- |
| A.5 | Information security policies |  |  |  |  |  |
| A.5.1 | Management direction for information security |  |  |  |  |  |
| A.5.1.1 | Policies for information  security |  |  |  | All policies referred to below in this column |  |
| A.5.1.2 | Review of the policies  for information  security |  |  |  | Each policy has a designated owner who has to review the document at planned interval |  |
| A.6 | Organization of information security |  |  |  |  |  |
| A.6.1 | Internal organization |  |  |  |  |  |
| A.6.1.1 | Information security  roles and responsibilities |  |  |  | Responsibilities for information security are listed in various ISMS documents. If required, [job title] defines additional responsibilities |  |
| A.6.1.2 | Segregation of duties |  |  |  | Any activity that includes sensitive information is approved by one person and implemented by another |  |
| A.6.1.3 | Contact with authorities |  |  |  | [Business Continuity Strategy], [Incident Response Plan] |  |
| A.6.1.4 | Contact with special  interest groups |  |  |  | [job title] is responsible for monitoring [list names of interest groups and security forums] |  |
| A.6.1.5 | Information security  in project management |  |  |  | Project manager is required to include applicable information security rules in every project |  |
| A.6.2 | Mobile devices and teleworking |  |  |  |  |  |
| A.6.2.1 | Mobile device policy |  |  |  | [Acceptable Use Policy] / [Mobile Device and Teleworking Policy], [Bring Your Own Device (BYOD) Policy] |  |
| A.6.2.2 | Teleworking |  |  |  | [Acceptable Use Policy] / [Mobile Device and Teleworking Policy] |  |
| A.7 | Human resource security |  |  |  |  |  |
| A.7.1 | Prior to employment |  |  |  |  |  |
| A.7.1.1 | Screening |  |  |  | [job title] checks each candidate by [describe the method for verification checks – e.g. checking the CV, contacting former employers, checking criminal records, financial status, etc.]; [Supplier Security Policy] |  |
| A.7.1.2 | Terms and conditions  of employment |  |  |  | All employees sign the [Statement of Acceptance of ISMS Documents] and [Confidentiality Statement]; [Supplier Security Policy] |  |
| A.7.2 | During employment |  |  |  |  |  |
| A.7.2.1 | Management responsibilities |  |  |  | Management actively requires that all ISMS rules be implemented by all employees, suppliers and outsourcing partners |  |
| A.7.2.2 | Information security  awareness, education  and training |  |  |  | Information Security Policy, Training and Awareness Plan, [Supplier Security Policy] |  |
| A.7.2.3 | Disciplinary process |  |  |  | [Incident Management Procedure], [Statement of Acceptance of ISMS Documents] |  |
| A.7.3 | Termination and change of employment |  |  |  |  |  |
| A.7.3.1 | Termination or change  of employment responsibilities |  |  |  | All agreements with suppliers and partners contain clauses that remain valid after the termination of employment, as well as the [Confidentiality Statements] signed with employees. |  |
| A.8 | Asset management |  |  |  |  |  |
| A.8.1 | Responsibility for assets |  |  |  |  |  |
| A.8.1.1 | Inventory of assets |  |  |  | [Inventory of Assets], [Information Classification Policy] |  |
| A.8.1.2 | Ownership of assets |  |  |  | [Inventory of Assets], [Acceptable Use Policy] |  |
| A.8.1.3 | Acceptable use of  assets |  |  |  | [Acceptable Use Policy] |  |
| A.8.1.4 | Return of assets |  |  |  | [Acceptable Use Policy]; [Supplier Security Policy] |  |
| A.8.2 | Information classification |  |  |  |  |  |
| A.8.2.1 | Classification of information |  |  |  | [Information Classification Policy] |  |
| A.8.2.2 | Labeling of information |  |  |  | [Information Classification Policy] |  |
| A.8.2.3 | Handling of assets |  |  |  | [Information Classification Policy] |  |
| A.8.3 | Media handling |  |  |  |  |  |
| A.8.3.1 | Management of removable  media |  |  |  | [Information Classification Policy] |  |
| A.8.3.2 | Disposal of media |  |  |  | [Operating Procedures for Information and Communication Technology] / [Disposal and Destruction Policy] |  |
| A.8.3.3 | Physical media transfer |  |  |  | [Information Classification Policy] |  |
| A.9 | Access control |  |  |  |  |  |
| A.9.1 | Business requirements of access control |  |  |  |  |  |
| A.9.1.1 | Access control policy |  |  |  | [Access Control Policy] |  |
| A.9.1.2 | Access to networks and network services |  |  |  | [Access Control Policy] |  |
| A.9.2 | User access management |  |  |  |  |  |
| A.9.2.1 | User registration and  de-registration |  |  |  | [Access Control Policy] / [Password Policy] |  |
| A.9.2.2 | User access provisioning |  |  |  | [Access Control Policy] / [Password Policy] |  |
| A.9.2.3 | Management of privileged  access rights |  |  |  | [Access Control Policy] |  |
| A.9.2.4 | Management of secret  authentication information  of users |  |  |  | [Access Control Policy] / [Password Policy] |  |
| A.9.2.5 | Review of user access  rights |  |  |  | [Access Control Policy] |  |
| A.9.2.6 | Removal or adjustment  of access rights |  |  |  | [Access Control Policy] |  |
| A.9.3 | User responsibilities |  |  |  |  |  |
| A.9.3.1 | Use of secret authentication  information |  |  |  | [Acceptable Use Policy], [Access Control Policy] / [Password Policy] |  |
| A.9.4 | System and application access control |  |  |  |  |  |
| A.9.4.1 | Information access  restriction |  |  |  | [Access Control Policy], [Information Classification Policy] |  |
| A.9.4.2 | Secure log-on procedures |  |  |  | A secure log-on process exists for all computers on the network |  |
| A.9.4.3 | Password management  system |  |  |  | [Access Control Policy] / [Password Policy] |  |
| A.9.4.4 | Use of privileged utility  programs |  |  |  | Only [job title] has the right to use privileged utility programs |  |
| A.9.4.5 | Access control to program  source code |  |  |  | The program source code is stored [describe technical implementation] and only [job title] has access rights |  |
| A.10 | Cryptography |  |  |  |  |  |
| A.10.1 | Cryptographic controls |  |  |  |  |  |
| A.10.1.1 | Policy on the use of  cryptographic controls |  |  |  | [Policy on the Use of Cryptographic Controls] |  |
| A.10.1.2 | Key management |  |  |  | [Policy on the Use of Cryptographic Controls] |  |
| A.11 | Physical and environmental security |  |  |  |  |  |
| A.11.1 | Secure areas |  |  |  |  |  |
| A.11.1.1 | Physical security  perimeter |  |  |  | Areas with sensitive information are protected [describe how – walls, etc.] |  |
| A.11.1.2 | Physical entry controls |  |  |  | Access to the organization's secure areas must be controlled [describe how – access cards, manned front entrance, etc.] |  |
| A.11.1.3 | Securing offices,  rooms and facilities |  |  |  | The facilities cannot be accessed from public areas, and secure areas are not noticeable to outsiders |  |
| A.11.1.4 | Protecting against  external and environmental  threats |  |  |  | An alarm system is installed and linked to the alarm monitoring center of [name of security service provider]; surveillance cameras are installed; fire protection is implemented [describe how]; flood protection is implemented [describe how] |  |
| A.11.1.5 | Working in secure  areas |  |  |  | [Procedures for working in secure areas] |  |
| A.11.1.6 | Delivery and loading  areas |  |  |  | Public access areas are controlled [describe how], and delivery and loading areas [specify which] are controlled [describe how] |  |
| A.11.2 | Equipment |  |  |  |  |  |
| A.11.2.1 | Equipment siting and protection |  |  |  | All equipment is located in a physically protected area, and highly sensitive equipment [specify which] is located in [name of secure area – e.g. server room] |  |
| A.11.2.2 | Supporting utilities |  |  |  | Devices for uninterruptible power supply [specify which – UPS, power generator, etc.] are installed for [specify for which IT and other equipment] |  |
| A.11.2.3 | Cabling security |  |  |  | Energy and data cables are installed within the secured area of the organization, and where this was not possible, they are protected [specify how] |  |
| A.11.2.4 | Equipment maintenance |  |  |  | [job title] must keep a maintenance record for all equipment in accordance with the manufacturer's instructions, and ensure adequate maintenance in a timely manner |  |
| A.11.2.5 | Removal of assets |  |  |  | [Acceptable Use Policy] |  |
| A.11.2.6 | Security of equipment  and assets off-premises |  |  |  | [Acceptable Use Policy] / [Mobile Device and Teleworking Policy] |  |
| A.11.2.7 | Secure disposal or reuse of equipment |  |  |  | [Operating Procedures for Information and Communication Technology] / [Disposal and Destruction Policy] |  |
| A.11.2.8 | Unattended user  equipment |  |  |  | [Acceptable Use Policy] / [Clear Desk and Clear Screen Policy] |  |
| A.11.2.9 | Clear desk and clear screen policy |  |  |  | [Acceptable Use Policy] / [Clear Desk and Clear Screen Policy] |  |
| A.12 | Operations security |  |  |  |  |  |
| A.12.1 | Operational procedures and responsibilities |  |  |  |  |  |
| A.12.1.1 | Documented operating  procedures |  |  |  | [Operating Procedures for Information and Communication Technology] |  |
| A.12.1.2 | Change management |  |  |  | [Operating Procedures for Information and Communication Technology] / [Change Management Policy] |  |
| A.12.1.3 | Capacity management |  |  |  | [job title] is responsible for monitoring the use of ICT assets and for planning required capacity |  |
| A.12.1.4 | Separation of development,  testing and  operational environments |  |  |  | Development, testing and operational systems are separated |  |
| A.12.2 | Protection from malware |  |  |  |  |  |
| A.12.2.1 | Controls against malware |  |  |  | The tool in use is [describe the tool that is used]; [Acceptable Use Policy] |  |
| A.12.3 | Backup |  |  |  |  |  |
| A.12.3.1 | Information backup |  |  |  | [Operating Procedures for Information and Communication Technology] / [Backup Policy], [Acceptable Use Policy] |  |
| A.12.4 | Logging and monitoring |  |  |  |  |  |
| A.12.4.1 | Event logging |  |  |  | [Operating Procedures for Information and Communication Technology] |  |
| A.12.4.2 | Protection of log information |  |  |  | Logs may not be deleted without permission granted by the authorized person |  |
| A.12.4.3 | Administrator and  operator logs |  |  |  | [Operating Procedures for Information and Communication Technology] |  |
| A.12.4.4 | Clock synchronization |  |  |  | System clocks on all computers are synchronized [describe how they are synchronized and with which accurate time source] |  |
| A.12.5 | Control of operational software |  |  |  |  |  |
| A.12.5.1 | Installation of software  on operational  systems |  |  |  | [Acceptable Use Policy] |  |
| A.12.6 | Technical vulnerability management |  |  |  |  |  |
| A.12.6.1 | Management of technical  vulnerabilities |  |  |  | [job title] is responsible for monitoring all vulnerabilities of applications and other systems, and [job title] must select actions to be taken in case new vulnerabilities are identified |  |
| A.12.6.2 | Restrictions on software  installation |  |  |  | [Acceptable Use Policy] |  |
| A.12.7 | Information systems audit considerations |  |  |  |  |  |
| A.12.7.1 | Information systems  audit controls |  |  |  | Each audit is planned and coordinated with management; audits are performed only on read-only access rights |  |
| A.13 | Communications security |  |  |  |  |  |
| A.13.1 | Network security management |  |  |  |  |  |
| A.13.1.1 | Network controls |  |  |  | [Operating Procedures for Information and Communication Technology] |  |
| A.13.1.2 | Security of network  services |  |  |  | [Operating Procedures for Information and Communication Technology] |  |
| A.13.1.3 | Segregation in networks |  |  |  | The network is segregated in the following fashion: [describe which segments of the network are segregated; describe whether the segregation is physical or logical] |  |
| A.13.2 | Information transfer |  |  |  |  |  |
| A.13.2.1 | Information transfer  policies and procedures |  |  |  | [Operating Procedures for Information and Communication Technology] / [Information Transfer Policy], [Bring Your Own Device (BYOD) Policy] |  |
| A.13.2.2 | Agreements on information  transfer |  |  |  | [Operating Procedures for Information and Communication Technology] / [Information Transfer Policy] |  |
| A.13.2.3 | Electronic messaging |  |  |  | [Information Classification Policy], [Acceptable Use Policy] |  |
| A.13.2.4 | Confidentiality or nondisclosure  agreements |  |  |  | The form of [Confidentiality Statement] is pre-defined |  |
| A.14 | System acquisition, development and maintenance |  |  |  |  |  |
| A.14.1 | Security requirements of information systems |  |  |  |  |  |
| A.14.1.1 | Information security  requirements analysis  and specification |  |  |  | When acquiring new information systems or changing existing ones, [job title] must document security requirements in the [Security Requirements Specification] |  |
| A.14.1.2 | Securing application  services on public  networks |  |  |  | [Secure Development Policy] |  |
| A.14.1.3 | Protecting application  services transactions |  |  |  | [Secure Development Policy] |  |
| A.14.2 | Security in development and support processes |  |  |  |  |  |
| A.14.2.1 | Secure development policy |  |  |  | [Secure Development Policy] |  |
| A.14.2.2 | System change control  procedures |  |  |  | [Secure Development Policy] |  |
| A.14.2.3 | Technical review of  applications after  operating platform  changes |  |  |  | [job title] is responsible for reviewing and testing all applications after operating system changes, before they are put into production |  |
| A.14.2.4 | Restrictions on  changes to software  packages |  |  |  | [Operating Procedures for Information and Communication Technology] / [Change Management Policy] |  |
| A.14.2.5 | Secure system engineering  principles |  |  |  | [Secure Development Policy] |  |
| A.14.2.6 | Secure development  environment |  |  |  | [Secure Development Policy] |  |
| A.14.2.7 | Outsourced development |  |  |  | [Supplier Security Policy], [Secure Development Policy] |  |
| A.14.2.8 | System security testing |  |  |  | [Secure Development Policy] |  |
| A.14.2.9 | System acceptance  testing |  |  |  | [Secure Development Policy] |  |
| A.14.3 | Test data |  |  |  |  |  |
| A.14.3.1 | Protection of test data |  |  |  | [Secure Development Policy] |  |
| A.15 | Supplier relationships |  |  |  |  |  |
| A.15.1 | Information security in supplier relationships |  |  |  |  |  |
| A.15.1.1 | Information security  policy for supplier  relationships |  |  |  | [Supplier Security Policy] |  |
| A.15.1.2 | Addressing security  within supplier agreements |  |  |  | [Supplier Security Policy] |  |
| A.15.1.3 | Information and communication  technology  supply chain |  |  |  | [Supplier Security Policy] |  |
| A.15.2 | Supplier service delivery management |  |  |  |  |  |
| A.15.2.1 | Monitoring and review  of supplier services |  |  |  | [Supplier Security Policy] |  |
| A.15.2.2 | Managing changes to  supplier services |  |  |  | [Supplier Security Policy] |  |
| A.16 | Information security incident management |  |  |  |  |  |
| A.16.1 | Management of information security incidents and improvements |  |  |  |  |  |
| A.16.1.1 | Responsibilities and  procedures |  |  |  | [Incident Management Procedure] |  |
| A.16.1.2 | Reporting information  security events |  |  |  | [Incident Management Procedure] |  |
| A.16.1.3 | Reporting information  security weaknesses |  |  |  | [Incident Management Procedure] |  |
| A.16.1.4 | Assessment of and  decision on information  security events |  |  |  | [Incident Management Procedure] |  |
| A.16.1.5 | Response to information  security incidents |  |  |  | [Incident Management Procedure], [Incident Response Plan] |  |
| A.16.1.6 | Learning from  information security  incidents |  |  |  | [Incident Management Procedure], [Procedure for Corrective Action] |  |
| A.16.1.7 | Collection of evidence |  |  |  | [Incident Management Procedure] |  |
| A.17 | Information security aspects of business continuity management |  |  |  |  |  |
| A.17.1 | Information security continuity |  |  |  |  |  |
| A.17.1.1 | Planning information  security continuity |  |  |  | [Procedure for Identification of Requirements], [Business Continuity Policy], [Business Impact Analysis Methodology], [Business Continuity Strategy] |  |
| A.17.1.2 | Implementing information  security continuity |  |  |  | [Business Continuity Plan] |  |
| A.17.1.3 | Verify, review and  evaluate information  security continuity |  |  |  | [BCMS Maintenance and Review Plan], [Exercising and Testing Plan], [Post-incident Review Form] |  |
| A.17.2 | Redundancies |  |  |  |  |  |
| A.17.2.1 | Availability of information  processing  facilities |  |  |  | [Recovery strategy for IT infrastructure] |  |
| A.18 | Compliance |  |  |  |  |  |
| A.18.1 | Compliance with legal and contractual requirements |  |  |  |  |  |
| A.18.1.1 | Identification of applicable  legislation and  contractual requirements |  |  |  | [List of Legal, Regulatory, Contractual and Other Requirements] |  |
| A.18.1.2 | Intellectual property  rights |  |  |  | [Acceptable Use Policy] |  |
| A.18.1.3 | Protection of records |  |  |  | [Procedure for Document and Record Control], [Secure Development Policy] |  |
| A.18.1.4 | Privacy and protection  of personally identifiable  information |  |  |  | [job title] is responsible for implementing legal requirements related to personal data protection |  |
| A.18.1.5 | Regulation of cryptographic  controls |  |  |  | [List of Legal, Regulatory, Contractual and Other Requirements], [Policy on the Use of Cryptographic Controls] |  |
| A.18.2 | Information security reviews |  |  |  |  |  |
| A.18.2.1 | Independent review of  information security |  |  |  | [Internal Audit Procedure], certification audit by [name of certification body] |  |
| A.18.2.2 | Compliance with  security policies and  standards |  |  |  | All owners of information assets, as well as the management, regularly review the implementation of security controls |  |
| A.18.2.3 | Technical compliance  review |  |  |  | [job title] is responsible for checking the technical compliance of information systems with security requirements |  |

# Acceptance of Residual Risks

Since not all risks could be reduced in the risk management process, all residual risks are hereby accepted:

1. all risks with the value 0, 1 or 2
2. risks which could not be reduced to the abovementioned levels after the application of controls, according to the following table:

[Complete the table with data on all individual risks which are not acceptable – use the Risk Treatment Table as the source.]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Name of asset** | **Asset owner** | **Threat** | **Vulnerability** | **New impact** | **New probability** | **Residual risk** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year, and immediately after risk assessment review and updates to the Risk Assessment Table and Risk Treatment Table.

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

* number of nonconformities due to unclearly defined implementation method of individual controls
* number of nonconformities due to unclearly defined control objectives
* number of controls for which the achievement of objectives cannot be measured

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]