ISO 27001 CONTROLS

MAPPED T0

INFOSEC DOMAINS

PREPARED BY :

MINISTRY OF
MOS
SECURITY

ISO 27001:2022 Controls Mapping to Information Security Control Domains

GOVERNANCE, COMPLIANCE & AUDIT

Control No	Control Name	Purpose/Objective	Implementation Guidance
5.1	Policies for information security	To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements	• Create Information Security Policy aligned with business objectives and requirements • Develop topic-specific policies for key areas (access control, password management, etc.) • Ensure policies include clear objectives, scope, roles and responsibilities • Establish policy management processes including regular reviews • Document and maintain policy acknowledgments and changes • Communicate policies effectively using clear language and awareness sessions
5.2	Information security roles and responsibilities	To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization.	• Create security organization structure (CISO, Security Managers, Operations teams) • Define responsibilities for each role (decisions, access rights, reporting lines) • Document and communicate through job descriptions and policies • Provide role-specific training and verify competency • Review roles annually and update as needed
5.3	Segregation of duties	To reduce the risk of fraud, error and bypassing of information security controls.	• Identify critical activities needing separation (financial, admin, security tasks) • Define who can request, approve, and implement changes • Document segregation rules and workflows • Implement role-based access controls • Monitor compliance and review effectiveness

ISO 27001:2022 Controls Mapping to Information Security Control Domains

5.4	Management responsibilities	To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.	• Define management's security oversight responsibilities • Ensure staff security briefing and training • Enforce policy compliance and handle violations • Provide resources for security implementation • Review security performance regularly
5.5	Contact with authorities	To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities	• Identify and document relevant authority contacts • Establish incident reporting procedures • Define scenarios requiring authority contact • Maintain current contact information • Test communication channels periodically
5.6	Contact with special interest groups	To ensure appropriate flow of information takes place with respect to information security.	• Join relevant security forums and groups Participate in information sharing platforms • Maintain active membership and engagement • Document and share received information • Review value of memberships annually
5.8	Information security in project management	Information security should be integrated into project management.	• Include security requirements in project planning • Conduct security risk assessments • Assign security expertise to projects • Review security at project milestones • Document security implementation decisions
5.31	Legal, statutory, regulatory and contractual requirements	To ensure compliance with legal, statutory, regulatory and contractual requirements related	• Identify applicable requirements • Document compliance obligations • Track regulatory changes • Implement compliance controls

		to information security	• Conduct regular compliance reviews • Maintain compliance records • Train staff on requirements • Update procedures as needed
5.32	Intellectual property rights	To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.	• Document all intellectual property assets • Track software licenses and usage • Establish copyright compliance procedures • Monitor unauthorized software use • Train staff on IP rights • Maintain license inventory • Review compliance regularly • Handle violations appropriately
5.34	Privacy and protection of personal identifiable information (PII)	To ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII.	• Identify all PII handled • Create privacy protection policies • Implement data protection controls • Train staff on privacy requirements • Monitor PII handling • Respond to privacy requests • Document PII processing • Regular privacy reviews
5.35	Independent review of information security	To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security	• Schedule regular security reviews • Define review scope Select independent reviewers • Document review findings • Create improvement plans • Track implementation • Report results to management • Follow up on recommendations
5.36	Compliance with policies, rules and standards for information security	To ensure that information security is implemented and operated in accordance with the organization's information security	• Regular compliance checks • Monitor policy adherence • Document compliance status • Address non-compliance • Update policies as needed

		policy, topic-specific policies, rules and standards.	• Train on policy changes • Maintain compliance records • Review effectiveness
5.37	Documented operating procedures	To ensure the correct and secure operation of information processing facilities.	• Document key procedures • Make procedures accessible • Train staff on procedures Update when changes occur • Review regularly • Maintain version control • Get management approval • Monitor procedure effectiveness
8.34	Protection of information systems during audit testing	To minimize the impact of audit and other assurance activities on operational systems and business processes	• Plan audit activities • Control audit access • Monitor audit impact • Protect live systems • Schedule testing properly • Document audit activities • Review audit effects • Maintain operations
ASSET MANAGEMENT			
Control No	**Control Name**	**Purpose/Objective**	**Implementation Guidance**
5.9	Inventory of information and other associated assets	To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership	• Create and maintain asset inventory • Assign ownership for each asset • Classify assets by importance/sensitivity • Update inventory regularly • Track asset location and status
5.10	Acceptable use of information and other associated assets	To ensure information and other associated assets are appropriately protected, used and handled.	• Create acceptable use policy • Define allowed and prohibited activities • Communicate guidelines clearly • Monitor usage compliance • Review and update guidelines periodically
5.11	Return of assets	To protect the organization's assets as part of the process of changing or terminating employment,	• Create asset return checklist for exits • Document all assigned assets per employee • Establish formal return procedures • Verify returned assets condition

		contract or agreement.	• Update asset inventory after returns
5.12	Classification of information	To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.	• Establish classification levels (e.g., Public, Internal, Confidential) • Define criteria for each level Train staff on classification process • Review and update classifications regularly • Document classification decisions
5.13	Labelling of information	To facilitate the communication of classification of information and support automation of information processing and management.	• Create standardized labelling system • Define labelling methods for different formats • Implement automated labelling where possible • Train users on labelling requirements • Audit labelling compliance
7.1	Storage media	To ensure only authorized disclosure, modification, removal or destruction of information on storage media.	• Define security perimeters clearly • Implement physical barriers • Install appropriate entry controls • Secure all access points • Monitor perimeter breaches • Regular perimeter inspections • Document security measures • Review effectiveness regularly
7.13	Equipment maintenance	To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance.	• Create maintenance schedules • Authorize maintenance personnel • Document all maintenance • Check equipment after service • Keep maintenance logs • Monitor equipment performance • Update maintenance plans • Review service effectiveness

7.14	Secure disposal or re-use of equipment	To prevent leakage of information from equipment to be disposed or re-used.	• Define disposal procedures • Verify data removal • Document disposal actions • Control disposal process • Train disposal staff • Check cleared equipment • Maintain disposal records • Review disposal methods
ACCESS MANAGEMENT			
Control No	**Control Name**	**Purpose/Objective**	**Implementation Guidance**
5.15	Access control	To ensure authorized access and to prevent unauthorized access to information and other associated assets.	• Create access control policy • Implement role-based access • Document access approval process • Regular access reviews • Monitor access patterns
5.16	Identity management	To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.	• Establish unique identifier system • Define identity verification process • Maintain identity lifecycle • Handle shared accounts securely • Regular identity reviews
5.17	Authentication information	To ensure proper entity authentication and prevent failures of authentication processes.	• Define strong authentication requirements • Secure credential distribution process • Implement password management systems • Handle reset procedures securely • Regular authentication review
5.18	Access rights	To ensure access to information and other associated assets is defined and authorized according to the business requirements.	• Document access rights process • Link rights to job roles • Regular rights review • Handle role changes • Maintain access records
8.2	Privileged access rights	To ensure only authorized users,	• Identify privileged access needs

		software components and services are provided with privileged access rights.	Document approval process Limit privileged accounts Monitor privileged activities Regular access reviews Log special access usage Revoke unused privileges Audit privilege changes
8.3	Information access restriction	To ensure only authorized access and to prevent unauthorized access to information and other associated assets.	Define access rules Implement access controls Document access rights Review access regularly Monitor information usage Handle access violations Update access rules Maintain access logs
8.4	Access to source code	To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property	Secure code repositories Control developer access Track code changes Review code modifications Backup source code Monitor code access Document code versions Audit code controls
8.5	Secure authentication	To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.	Define authentication requirements Implement strong verification Manage authentication methods Monitor login attempts Handle failed attempts Train users on security Review authentication effectiveness Update security measures

VENDORS & SUPPLIER MANAGEMENT

Control No	Control Name	Purpose/Objective	Implementation Guidance
5.19	Information security in supplier relationships	To maintain an agreed level of information security in supplier relationships.	Define supplier security requirements Assess supplier security capabilities Include security in contracts Monitor supplier compliance Regular security reviews

5.2	Addressing information security within supplier agreements	To maintain an agreed level of information security in supplier relationships.	- Document security requirements - Include incident reporting procedures - Define security responsibilities - Specify compliance requirements - Include right to audit
5.21	Managing information security in the information and communication technology (ICT) supply chain	To maintain an agreed level of information security in supplier relationships.	- Map complete ICT supply chain - Define security requirements for suppliers - Regular security assessments - Monitor component security - Implement vulnerability management
5.22	Monitoring, review and change management of supplier services	To maintain an agreed level of information security and service delivery in line with supplier agreements.	- Establish clear monitoring metrics and reporting schedules - Conduct regular supplier security assessments and compliance checks - Create and maintain change management procedures for supplier services - Document and track all security incidents and resolutions - Hold regular performance review meetings with key suppliers - Maintain updated inventory of all supplier services and their security requirements - Develop escalation procedures for security issues - Review supplier access rights and permissions regularly

5.23	Information security for use of cloud services	To specify and manage information security for the use of cloud services.	• Assess security capabilities of cloud providers • Define data protection requirements for cloud services • Implement access controls and monitoring • Establish backup and recovery procedures • Create cloud service exit strategy • Monitor cloud service security performance • Document cloud security responsibilities • Train users on secure cloud usage
INCIDENT MANAGEMENT			
Control No	**Control Name**	**Purpose/Objective**	**Implementation Guidance**
6.8	Information Security event reporting	To support timely, consistent and effective reporting of information security events that can be identified by personnel.	• Establish reporting procedures • Create reporting channels • Define incident categories • Train staff on reporting • Track reported events • Provide feedback mechanisms • Review reporting effectiveness • Document all reports
5.24	Information security incident management planning and preparation	To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events	• Create incident response plan and procedures • Define incident response team and roles • Establish incident reporting mechanisms • Develop incident classification system • Set up communication procedures • Create incident documentation templates

			• Conduct regular incident response training • Test incident response procedures regularly
5.25	Assessment and decision on information security events	To ensure effective categorization and prioritization of information security events.	• Create event assessment criteria and severity levels • Define decision-making authority for different severity levels • Establish response procedures for each severity level • Document assessment methods and decisions • Monitor patterns in security events • Review and update assessment criteria regularly • Train staff on incident assessment procedures • Maintain incident assessment records
5.26	Response to information security incidents	To ensure efficient and effective response to information security incidents.	• Develop incident response procedures • Define containment strategies • Establish investigation processes • Create recovery procedures Set up communication protocols • Define escalation procedures • Document incident handling steps • Review and update response plans
5.27	Learning from information security incident	To reduce the likelihood or consequences of future incidents.	• Document detailed incident analysis • Identify root causes and patterns • Develop improvement recommendations • Update security controls based on lessons

			- Share lessons learned with relevant teams - Track implementation of improvements - Measure effectiveness of changes - Review incident trends periodically
5.28	Collection of evidence	To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions	- Establish evidence collection procedures - Define chain of custody process - Train staff on evidence handling - Set up secure evidence storage - Document evidence collection steps - Maintain evidence inventory - Define evidence retention periods - Create evidence disposal procedures

BUSINESS CONTINUITY & DISASTER RECOVERY MANAGEMENT

Control No	**Control Name**	**Purpose/Objective**	**Implementation Guidance**
5.29	Information security during disruption	To protect information and other associated assets during disruption.	- Identify critical security controls - Create disruption response procedures - Establish minimum security requirements - Define emergency access procedures - Test security measures during disruptions - Document emergency procedures - Train staff on emergency protocols - Review and update plans regularly
5.3	ICT readiness for business continuity	To ensure the availability of the organization's information and other associated	- Identify critical ICT services - Set recovery time objectives

		assets during disruption.	• Implement backup systems • Establish alternate processing sites • Create recovery procedures • Test continuity plans • Maintain backup equipment • Document recovery steps

INFRASTRUCTURE & DATA SECURITY

Control No	**Control Name**	**Purpose/Objective**	**Implementation Guidance**
5.14	Information transfer	To maintain the security of information transferred within an organization and with any external interested party.	• Define secure transfer methods • Establish transfer agreements • Implement encryption for sensitive transfers • Document chain of custody • Monitor transfer compliance
5.33	Protection of records	To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records.	• Identify critical records • Define retention periods • Implement protection controls • Establish storage procedures • Create access controls • Monitor record handling • Set disposal procedures • Document record locations
8.1	User end point devices	To protect information against the risks introduced by using user endpoint devices.	• Create device usage policies • Implement security controls • Configure device protection • Monitor device usage • Manage device updates • Control data access • Document issued device • Regular security reviews
8.6	Capacity management	The use of resources should be monitored	• Monitor resource usage • Plan capacity needs

		and adjusted in line with current and expected capacity requirements	- Set performance alerts - Regular capacity reviews - Handle resource issues - Document capacity plans - Forecast future needs - Update resources timely
8.7	Protection against malware	To ensure information and other associated assets are protected against malware.	- Install protection software - Keep definitions updated - Scan systems regularly - Monitor system behaviour - Respond to alerts - Train users on threats - Document incidents - Review protection effectiveness
8.9	Configuration management	To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.	- Define secure configurations - Document standard settings - Control configuration changes - Regular configuration checks - Track system settings - Update standards - Monitor compliance - Maintain configuration records
8.10	Information deletion	To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.	- Create deletion procedures - Use secure deletion methods - Verify data removal - Track deletion activities - Handle storage media - Document data removal - Train staff on procedures - Audit deletion process
8.11	Data masking	To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.	- Identify sensitive data - Define masking rules - Implement masking tools - Test masked data

			• Control access to original data • Monitor masking effectiveness • Document procedures • Review masking methods
8.12	Data leakage prevention	To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.	• Identify sensitive data flows • Implement monitoring tools • Set prevention rules • Monitor data movement • Handle violations • Train users on policies • Document incidents • Review effectiveness
8.18	Use of privileged utility programs	To ensure the use of utility programs does not harm system and application controls for information security	• Identify powerful utilities • Restrict access rights • Monitor utility usage • Document approved users • Control installation • Log all usage • Regular access review • Remove unnecessary tools
8.19	Installation of software on operational systems	To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.	• Create installation policy • Define approved software • Control installation rights • Test before installation • Document all changes • Monitor compliance • Remove unauthorized software • Regular software audits
8.24	Use of cryptography	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security	• Define encryption needs • Select encryption methods • Manage encryption keys • Train users appropriately • Monitor encryption use • Regular key updates • Document procedures • Review effectiveness

		requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.	
8.32	Change management	To preserve information security when executing changes.	• Create change procedures • Document change requests • Test proposed changes • Get proper approvals • Plan implementations • Monitor change impacts • Keep change records • Review effectiveness
INFORMATION BACKUP MANAGEMENT			
Control No	**Control Name**	**Purpose/Objective**	**Implementation Guidance**
8.13	Information backup	To enable recovery from loss of data or systems.	• Define backup requirements • Implement backup systems • Test recovery process • Secure backup storage • Monitor backup success • Document backup schedule • Regular recovery tests • Review backup strategy
8.14	Redundancy of information processing facilities	To ensure the continuous operation of information processing facilities.	• Identify critical systems • Create redundant setups • Test failover process • Maintain backup systems • Monitor system health • Document procedures • Regular testing • Review effectiveness
LOGGING & MONITORING			
Control No	**Control Name**	**Purpose/Objective**	**Implementation Guidance**
8.15	Logging	To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access,	• Define logging requirements • Configure system logs • Protect log information • Regular log reviews • Set retention periods

		identify information security events that can lead to an information security incident and to support investigations.	• Monitor log storage • Handle log alerts • Document findings
8.16	Monitoring activities	To detect anomalous behaviour and potential information security incidents.	• Set monitoring scope • Deploy monitoring tools • Define alert thresholds • Train monitoring staff • Handle security alerts • Document incidents • Regular reviews • Update monitoring rules
8.17	Clock synchronization	To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents.	• Set time source standards • Configure system clocks • Monitor synchronization • Handle time drift • Document time zones • Regular checks • Maintain accuracy • Review effectiveness

NETWORK SECURITY

Control No	Control Name	Purpose/Objective	Implementation Guidance
8.20	Networks security	To protect information in networks and its supporting information processing facilities from compromise via the network.	• Design secure networks • Implement protection tools • Monitor network traffic • Control network access • Regular security updates • Document network layout • Test security controls • Review effectiveness
8.21	Security of network services	To ensure security in the use of network services.	• Define service requirements • Implement security controls • Monitor service levels • Manage service providers • Document agreements • Regular service reviews • Handle service issues

			• Update security measures
8.22	Segregation of networks	To split the network in security boundaries and to control traffic between them based on business needs.	• Identify network types • Plan network separation • Implement segregation • Control traffic flow • Monitor segments • Document network design • Regular reviews • Test separation
8.23	Web filtering	To protect systems from being compromised by malware and to prevent access to unauthorized web resources.	• Define filtering rules • Implement web filters • Create allowed/blocked lists • Monitor web access • Handle filter alerts • Update filter rules • Document exceptions • Review effectiveness

VULNERABILITY & PATCH MANAGEMENT

Control No	**Control Name**	**Purpose/Objective**	**Implementation Guidance**
5.7	Threat intelligence	To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.	• Set up threat intelligence collection process • Subscribe to trusted intelligence sources • Analyze and validate gathered intelligence • Share actionable intelligence internally • Implement protective measures based on threats
8.8	Management of technical vulnerabilities	To prevent exploitation of technical vulnerabilities.	• Regular vulnerability scans • Prioritize identified issues • Apply security patches • Test system updates • Monitor fix effectiveness • Track vulnerable assets • Document remediation • Review scanning process

SECURE DEVELOPMENT & ENIGINEERING PRACTICE

ISO 27001:2022 Controls Mapping to Information Security Control Domains

Control No	Control Name	Purpose/Objective	Implementation Guidance
8.25	Secure development life cycle	To ensure information security is designed and implemented within the secure development life cycle of software and systems.	• Define security requirements • Include security in design • Secure coding practices • Regular security testing • Document development • Review security measures • Manage changes securely • Monitor compliance
8.26	Application security requirements	To ensure all information security requirements are identified and addressed when developing or acquiring applications.	• Document security needs • Define access requirements • Specify data protection • Set validation rules • Include audit features • Plan error handling • Review requirements • Update as needed
8.27	Secure system architecture and engineering principles	To ensure information systems are securely designed, implemented and operated within the development life cycle.	• Define security principles • Design secure architecture • Document design decisions • Review security plans • Test design effectiveness • Update architecture • Monitor compliance • Regular reviews
8.28	Secure coding	To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.	• Establish coding standards • Train developers properly • Implement code reviews • Use secure components • Test code security • Document practices • Monitor compliance • Update standards regularly
8.29	Security testing in development	To validate if information security	• Define testing requirements

	and acceptance	requirements are met when applications or code are deployed to the production environment.	- Create test scenarios - Conduct security testing - Document test results - Fix identified issues - Verify fixes work - Maintain test records - Review test process
8.30	Outsourced development	To ensure information security measures required by the organization are implemented in outsourced system development.	- Define security requirements - Include security in contracts - Monitor development work - Review code quality - Test delivered systems - Control source code - Document arrangements - Verify compliance
8.31	Separation of development, test and production environments	To protect the production environment and data from compromise by development and test activities.	- Create separate environments - Control access to each - Protect production data - Manage data transfers - Document separation - Monitor environment usage - Regular environment reviews - Maintain separation
8.33	Test information	To ensure relevance of testing and protection of operational information used for testing.	- Create test data policy - Generate safe test data - Protect test environments - Control test access - Monitor test usage - Delete after testing - Document procedures - Regular reviews

PHYSICAL & ENVIRONMENTAL SECURITY

Control No	**Control Name**	**Purpose/Objective**	**Implementation Guidance**
7.1	Physical security perimeters	To prevent unauthorized physical access, damage and interference to the organization's information and	- Define security perimeters clearly - Implement physical barriers - Install appropriate entry controls - Secure all access points

		other associated assets.	• Monitor perimeter breaches • Regular perimeter inspections • Document security measures • Review effectiveness regularly
7.2	Physical entry	To ensure only authorized physical access to the organization's information and other associated assets occurs	• Establish entry control procedures • Implement visitor management • Create access authorization process • Maintain access logs • Monitor entry points • Regular access reviews • Train security personnel • Document unauthorized attempts
7.3	Securing offices, rooms and facilities	To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.	• Identify sensitive areas • Implement appropriate security • Control access permissions • Monitor secured areas • Maintain security records • Regular security checks • Document security measures • Review protection levels
7.4	Physical security monitoring	To detect and deter unauthorized physical access.	• Install appropriate monitoring systems • Define monitoring schedules and procedures • Train security personnel on monitoring • Maintain monitoring logs and reports • Regular system maintenance • Document and investigate alerts • Review monitoring effectiveness • Update systems as needed

7.5	Protecting against physical and environmental threats	To prevent or reduce the consequences of events originating from physical and environmental threats.	• Identify potential threats • Install protective measures • Create emergency procedures • Regular equipment maintenance • Test protection systems • Train staff on procedures • Document incidents and responses • Review protection effectiveness
7.6	Working in secure areas	To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.	• Define secure work procedures • Establish supervision requirements • Control contractor access • Document all work activities • Monitor secure area activities • Train supervisory staff • Regular procedure reviews • Maintain work records
7.7	Clear desk and clear screen	To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.	• Create clear desk policy • Set screen locking requirements • Provide secure storage options • Regular compliance checks • Train staff on procedures • Monitor policy adherence • Document violations • Review effectiveness
7.8	Equipment siting and protection	To reduce the risks from physical and environmental threats, and from unauthorized access and damage.	• Assess equipment placement needs • Implement protection measures • Control environmental conditions • Regular equipment checks • Document protection measures

			• Monitor equipment status • Update protection as needed • Maintain protection records
7.9	Security of assets off-premises	To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.	• Create off-site asset policy • Track asset movement • Define protection requirements • Train users on security • Regular asset checks • Document asset location • Monitor asset usage • Review security measures
7.11	Supporting utilities	To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.	• Identify critical utilities • Install backup systems • Regular maintenance checks • Test backup systems • Monitor utility performance • Document failures • Update support systems • Review effectiveness
7.12	Cabling security	To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.	• Plan cable installations • Protect cable routes • Label cables clearly • Separate power and data cables • Regular cable inspection • Document cable layouts • Control access to cable areas • Maintain cable records
HUMAN RESOURCE MANAGEMENT			
Control No	**Control Name**	**Purpose/Objective**	**Implementation Guidance**
6.1	Screening	To ensure all personnel are eligible and suitable for the roles for which they are considered and	• Create screening policy and procedures • Define verification requirements by role

		remain eligible and suitable during their employment	• Conduct background checks • Verify professional qualifications • Check employment history • Document screening results • Handle screening failures • Regular screening reviews
6.2	Terms and conditions of employment	To ensure personnel understand their information security responsibilities for the roles for which they are considered.	• Define security responsibilities • Include in employment contracts • Explain security obligations • Get signed acknowledgment • Maintain documentation • Update terms when needed • Review compliance regularly • Handle violations appropriately
6.3	Information security awareness, education and training	To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.	• Create security awareness program • Develop training materials • Conduct regular sessions • Track participation • Test understanding • Update training content • Measure effectiveness • Document completion
6.4	Disciplinary process	To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and	• Establish disciplinary procedures • Define violation categories • Document consequences • Ensure fair process • Maintain violation records

		other relevant interested parties who committed the violation.	- Communicate procedures - Train managers - Review effectiveness
6.5	Responsibilities after termination or change of employment	To protect the organization’s interests as part of the process of changing or terminating employment or contracts.	- Create termination/change checklist - Document handover requirements - Manage access right changes - Collect organization assets - Update security records - Brief on ongoing obligations - Verify completion of process - Archive relevant documentation
6.6	Confidentiality or non-disclosure agreements	To maintain confidentiality of information accessible by personnel or external parties.	- Develop standard NDAs - Define signing requirements - Maintain signed agreements - Review agreements periodically - Train on confidentiality obligations - Track agreement expiry - Update when requirements change - Monitor compliance
6.7	Remote working	To ensure the security of information when personnel are working remotely	- Create remote working policy - Define security requirements - Implement remote access controls - Provide secure equipment - Train on remote security - Monitor remote access - Review security measures - Document approved arrangements

DID YOU FIND THIS CHECKLIST USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

MINISTRY OF MOS SECURITY

WWW.MINISTRYOFSECURITY.CO