ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
6.1	Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	**Screening process**	Interview human resource department to verify the screening process	Analyse screening process documents and their adherence to legal requirements		Review the evidence of a sample of recent screening activity to verify its adherence to the defined process
		Suitability verification	Interview responsible personnel to verify how competence for people hired for specific information security roles is evaluated	Analyse competence evaluation documents		Review the evidence of a sample of recently performed competence evaluations
		Periodic verification checks	Interview human resource department to verify the periodic verification checks activities and their periodicity	Analyse verification check documents and their adherence to legal requirements		Review the evidence of a sample of recent verification check activity to verify its adherence to the defined process and its timeliness
6.2	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	**Employment contracts**	Interview responsible personnel to understand how employment contracts are managed	Analyse employment contract templates to verify contractual obligations regarding information security are included and can change accordingly to the employee's role		Review a sample of recent employment contracts to verify contractual obligation regarding information security are included in different roles
		Employment clauses		Analyse employment contract templates to verify they include as applicable: 1) confidentiality or non-disclosure agreements 2) legal responsibilities 3) information classification and handling responsibilities 4) actions to be undertaken in case of security requirements disregard		Review a sample of recent employment contracts to verify they include as applicable: 1) confidentiality or non-disclosure agreements 2) legal responsibilities 3) information classification and handling responsibilities 4) actions to be undertaken in case of security requirements disregard
6.3	Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	**Information security awareness programme**	Interview responsible personnel to understand the structure of the information security awareness programme and to verify that is in line with the organization's policies	Analyse the information security awareness programme to verify that it provides multiple methods and channels, both physical and virtual		
		Information security awareness activities coverage	Interview responsible personnel to understand the topics covered by the information security awareness programme and that its outreach comprises all of the organization's staff, with specific regards for the newly hired and relevant third parties.			Review records of a sample information security awareness initiatives to verify that all the following topics are covered: 1) management's commitment towards information security 2) information security rules and obligations 3) personal accountability for own actions and inactions 4) baseline information security procedures and controls 5) contact points and resources

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
		Information security awareness effectiveness	Interview a sample of personnel with different roles to verify they have completed the awareness training retaining the expected knowledge about: -authentication policies, procedures and good practices - how to behave to avoid and contain malware			Review records of information security awareness sessions evaluations of understanding to ensure the initiatives are evaluated and effective.
		Education and training programme update	Interview responsible personnel to understand the education and training programme and to verify that is in line with the organization's policies	Analyse the information security awareness programme to verify that it is aimed to increase specific skill sets and expertise as appropriate for the recipient's job position needs.		
		Technical staff information security skills	Interview a sample of technical staff to verify how they keep their technical skills up-to-date			Observe records for technical staff participation into conferences and events or subscribing to newsletter and magazines
6.4	A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	**Evidence of policy violation**		Analyse that the disciplinary process is formally defined based on evidence of violation of information security policy		Observe disciplinary process records to verify they have been initiated after an evidence of policy violation has been provided
		Graduated response		Analyse that the disciplinary process is gradual and evaluates the gravity and consequences of the breach, whether the offence was intentional or unintentional, if it is a repetition and if the violator was trained		Observe disciplinary process records to verify they are gradual and proportionate to the situation, in line with the described process
		Legislation, regulations, contractual and business requirements		Verify that the disciplinary process takes into consideration relevant legislation, regulations, contractual and business requirements		Observe disciplinary process records to verify they takes into consideration relevant legislation, regulations, contractual and business requirements
6.5	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.	**Responsibilities and duties**		Analyse employment contract templates to verify the presence of clauses imposing information security responsibilities and duties to remain valid after termination or change		Review a sample of recent employment contracts to verify they include information security responsibilities and duties to be valid after termination or change
		Responsibilities and duties transfer	Interview human resources personnel to verify how information security roles and responsibilities are transferred from an individual leaving or changing job role			Review the records of recent information security roles and responsibilities transfer from an individual leaving or changing job role
		Leaving or changing role notification	Interview human resources personnel to verify how personnel and other interested parties are notified about individuals leaving or changing role			Review the records of recent notifications about individuals leaving or changing role

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
6.6	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	**Confidentiality or non-disclosure agreements**	Interview responsible personnel to understand how confidentiality or non-disclosure agreements are managed	Analyse confidentiality or non-disclosure agreements templates to verify they include obligations to interested parties and personnel valid during employment and after change or termination of employment		Review a sample of recent contracts to verify confidentiality or non-disclosure agreements are duly included
		Confidentiality or non-disclosure agreements clauses		Analyse confidentiality or non-disclosure agreements templates to verify they include as applicable: 1) a definition of the information to be protected 2) the expected duration of an agreement 3) the required actions when an agreement is terminated; 4) the responsibilities and actions of signatories to avoid unauthorized information disclosure; 5) the ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information; 6) the permitted use of confidential information and rights of the signatory to use information; 7) the right to audit and monitor activities that involve confidential information; 8) the process for notification and reporting of unauthorized disclosure or confidential information leakage; 9) the terms for information to be returned or destroyed at agreement termination; 10) the expected actions to be taken in the case of non-conformance with the agreement.		Review confidentiality or non-disclosure agreements to verify they include as applicable: 1) a definition of the information to be protected 2) the expected duration of an agreement 3) the required actions when an agreement is terminated; 4) the responsibilities and actions of signatories to avoid unauthorized information disclosure; 5) the ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information; 6) the permitted use of confidential information and rights of the signatory to use information; 7) the right to audit and monitor activities that involve confidential information; 8) the process for notification and reporting of unauthorized disclosure or confidential information leakage; 9) the terms for information to be returned or destroyed at agreement termination; 10) the expected actions to be taken in the case of non-conformance with the agreement.
		Confidentiality or non-disclosure agreements review	Interview responsible personnel to verify how confidentiality or non-disclosure agreements are reviewed periodically or upon changing situations			Review records of confidentiality or non-disclosure agreements recent reviews

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
6.7	Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	**Remote working policy**	Interview responsible personnel to verify that a topic-specific policy on remote working is established and communicated to all relevant interested parties	Analyse remote working policy to verify it defines the relevant conditions and restrictions about remote working, including, when applicable: 1) the existing or proposed physical security of the remote working site; 2) rules and security mechanisms for the remote physical environment 3) the expected physical remote working environments; 4) the communications security requirements; 5) the use of remote access such as virtual desktop access that establishes appropriate processing and storage of information on privately owned equipment; 6) the threat of unauthorized access to information or resources from other persons at the remote working site and in public places; 7) the use of home networks and public networks, and requirements or restrictions on the configuration of wireless network services; 8) use of security measures, such as firewalls and protection against malware; 9) secure mechanisms for deploying and initializing systems remotely and for authentication and enablement of access privileges		
		Equipment and guidance	Interview personnel working remotely to verify which guidelines, communication equipment, storage furniture and devices are provided for remote working activities	Analyse guidance for remote working to verify they include considerations about: 1) physical security 2) family and visitor access to equipment and information 3) backup and business continuity procedures 4) hardware and software support and maintenance 5) accessible information based on classification	Review remote equipment configuration to verify it is set to provide: 1) secure remote access methods 2) screen locks and inactivity timers 3) device location tracking 4) remote wipe capability	

ID	Control	Testing Procedure	Interview	Document	Configuration	Observation
6.8	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	**Reporting procedures awareness**	Interview responsible personnel to verify that users and personnel are aware of the procedures to report information security events as quickly as possible, including the point of contact to which the events should be reported			Observe a sample of reported information security events to verify that they are made correctly and timely and the following events are considered: 1) ineffective information security control; 2) breach of information confidentiality, integrity or availability expectations; 3) human errors; 4) non-conformance with the information security policy, topic-specific policies or applicable standards; 5) breaches of physical security measures; 6) system changes that have not gone through the change management process; 7) malfunctions or other anomalous system behaviour of software or hardware; 8) access violations; 9) vulnerabilities; 10) suspected malware infection.