ISO 27001:2022

AUDIT CHECKLIST

PART 3

A.6 PEOPLE CONTROLS

&

A.7 PHYSICAL CONTROLS

MINISTRY OF SECURITY

A.6 People Controls				
Control No.	**Control**	**Control Description**	**Assessment Questions**	**Response**
6.1	Screening	Background verification checks on all candidates to become personnel shall 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.	1. Is there a screening process for onboarding full-time, part-time and temporary staff. 2. Are background verification checks carried out on all new candidates for employment? 3. Does the background verification process consider checking professional experience, academic qualifications, independent identity verification, criminal records verification and credit review. 4. Are the checks compliant with relevant laws, regulations and ethics?	
6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	1. Is there a formal terms and conditions of employment documented and communicated to all full-time, part-time and temporary staff before onboarding. 2. Does the terms and conditions of employment include organization's information security policy and relevant topic-specific policies. 3. Does the terms and conditions of employment include legal responsibilities and rights like copyright laws or data protection legislations. 4. Does the terms and conditions of employment include responsibilities for the handling of information received from interested parties. 5. Does the terms and conditions of employment include actions to be taken if personnel disregard the organization's security requirements.	
6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall 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.	1. Do all employees, contractors and 3rd party users undergo regular security awareness training appropriate to their role and function within the organisation. 2. Does the Information security awareness program cover information security policy and topic-specific policies, standards, laws, statutes, regulations, contracts and agreements. 3. Does the Information security awareness program cover personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and interested parties. 4. Does the organization have a formal process to access the effectiveness of the information security awareness program by ensuring that all employees take up quiz.	

6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	1. Is there a formal disciplinary process which allows the organisation to take action against employees who have committed an information security breach. 2. Is the formal disciplinary process approved by the top management. 3. Is the formal disciplinary process communicated to all employees. 4. Does the formal disciplinary process take into consideration factors such as: • The nature (who, what, when, how) and gravity of the breach and its consequences • Whether the offence was intentional (malicious) or unintentional (accidental) • whether or not this is a first or repeated offence • whether or not the violator was properly trained	
6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	1. Does the employee termination process define the information security responsibilities and duties that shall remain valid after termination or change of job roles for all full-time, part-time, and temporary staff. 2. Are the responsibilities and duties that remain valid after termination of employment or contract included in the individual's terms and conditions of employment, contract or agreement.	
6.6	Confidentiality or non-disclosure agreements	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.	1. Are the full-time, part-time and temporary staff required to sign confidentiality or non-disclosure agreements prior to being given access to organization's confidential information and other associated assets. 2. Does the confidentiality or non-disclosure agreements include: • The definition of the information to be protected. • Validity of the agreement. • The ownership of information, trade secrets and intellectual property. • The terms for information to be returned or destroyed at agreement termination.	

6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	1. Is there a formal policy covering the information security requirements for allowing personnel to work and access organization's information remotely. 2. Is the remote working policy approved by the top management. 3. Is the remote working policy communicated to all full-time, part-time and temporary staff who work remotely. 4. Does the remote working policy consider physical security requirements. 5. Does the remote working policy consider of the remote working site such as lockable filing cabinets, secure transportation between locations and rules for remote access, clear desk, printing and disposal of information. 6. Does the remote working policy consider the communications security requirements. 7. Does the remote working policy consider the threat of unauthorized access to information or resources from other persons in public places. 8. Does the remote working policy consider use of security measures, such as firewalls and protection against malware.	
6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	1. Are all full-time, part-time, and temporary staff made aware of their responsibility to report information security events. 2. Are all full-time, part-time, and temporary staff made aware of the procedure for reporting information security. 3. Are all full-time, part-time and temporary staff made aware of the communication contact details and communication medium for reporting information security events.	

A.8 Physical Controls				
Control No.	**Control**	**Control Description**	**Assessment Questions**	**Response**
7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	1. Is there a designated security perimeter. 2. Are sensitive or critical information areas segregated and appropriately controlled. 3. Has the organization implemented physically sound perimeters for a building or site containing information processing facilities.	
7.2	Physical entry	Secure areas should be protected by appropriate entry controls and access points.	1. Has the organization established a formal process for the management of access rights to physical areas. 2. Does the process include the provisioning, periodical review, update and revocation of authorizations for physical access. 3. is there a process for maintaining and monitoring a physical logbook or electronic audit trail of all physical access. 4. Are adequate authentication mechanisms like access cards, biometrics or two-factor authentication such as an access card and secret PIN implemented for physical access to information processing facilities. 5. Is there a formal process for managing access to visitors. 6. Are the visitors given a Visitor Badge which distinguishes them from the employees. 7. Are the visitor logs maintained including the date, time in, time out, purpose of visit and personnel authorising the visitor's entry. 8. Are the visitors verified for their identity by checking the National ID or their company ID. 9. Are the visitors accompanied by organization's personal and escorted to all places within the organization. 10. Are the internal and external doors of delivery and loading are adequately secured. 11. Are the incoming deliveries inspected and examined for explosives, chemicals or other hazardous materials before they are moved from delivery and loading areas. 12. Are the incoming deliveries registered in accordance with asset management procedures. 13. Are the incoming deliveries inspected for tampering or meddling.	

7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	1. Are the offices, rooms and critical information processing facilities sited to prevent unauthorised access. 2. Are controls implemented for critical process facilities to prevent confidential information or activities from being visible and audible from the outside.	
7.4	Physical security monitoring	Premises should be continuously monitored for unauthorized physical access.	1. Are the organization's physical premises monitored by surveillance systems, security guards, or intruder alarms. 2. Are the entry and exit points of critical information processing facilities equipped with video monitoring systems. 3. Is the access to video monitoring/CCTV systems restricted to authorized personnel. 4. Is the video monitoring/CCTV footage retained as per organizations and legal requirements.	
7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.	1. Are the critical information processing facilities protected against physical and environmental threats. 2. Are adequate controls implemented to protect personnel and assets against fire, flooding, electrical surging, lightning, explosives etc.	
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.	1. Are the personnel aware of the existence of the secure areas. 2. Activities within secure areas communicated only to authorised personnel on need-to-know basis. 3. Are the secure areas periodically inspected to identify any vacant areas. 4. Are controls in place to restrict photographic, video, audio or other recording equipment, such as cameras in user endpoint devices, unless authorized within secure areas.	
7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	1. has the organization defined a formal clear desk and clear screen policy. 2. Is the clear desk and clear screen policy approved by the top management. 3. Is the clear desk and clear screen policy communicated to all full-time, part-time and temporary staff. 4. Does the clear desk and clear screen policy include the requirements for protecting user endpoint devices by key locks or other security means when not in use or unattended. 5. Does the clear desk and clear screen policy include the requirements for configuring user endpoint devices with a secure screen saver after certain period of inactivity. 6. Does the clear desk and clear screen	

			policy include the requirements for the use of printers with an authentication function. 7. Does the clear desk and clear screen policy include the requirements for securely storing documents and removable storage media containing sensitive information. 8. Does the clear desk and clear screen policy include the requirements for clearing sensitive or critical information on whiteboards and other types of display when no longer required.	
7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	1. Are the equipments handling sensitive data situated adequately to reduce the risk of information being viewed by unauthorized persons during their use. 2. Are the equipments situated adequately to protect against physical and environmental threats. 3. Has the organization established guidelines for eating, drinking, and smoking in proximity to information processing facilities. 4. Are controls in place for monitoring environmental conditions, such as temperature and humidity of the surroundings.	
7.9	Security of assets off-premises	Off-site assets shall be protected.	1. Has the organization defined a formal process for the protection of devices which store or process information outside the organization's premises. 2. Are the personnel made aware of guidelines for handling organization's assets off-premises. 3. Are logs maintained for tracking equipments taken outside the organization. 4. Are controls implemented to track location of the assets and remote wiping of devices.	

7.10	Storage media	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	1. Has the organization defined a formal process for managing removable storage media. 2. Is the removable media policy approved by the top management. 3. Is the removable media policy communicated to all full-time, part-time and temporary staff. 4. Does the removable storage media policy consider requirements for restricting the use of removable storage media only to authorised personnel on need to have basis. 5. Does the removable storage media policy consider requirements for managing an inventory of removable storage media. 6. Does the removable storage media policy consider requirements for maintaining audit logs for taking removable storage media outside the organization. 7. Does the removable storage media policy consider requirements for storing the removable storage media with adequate protection. 8. Does the removable storage media policy consider requirements for using cryptographic techniques for securing/protecting data within removable storage media. 9. Does the removable storage media policy consider requirements for enabling USB or SD card slots only on system with need to have basis.	
7.11	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	1. Are the equipments supporting the utilities is configured, operated and maintained in accordance with the relevant manufacturer's specifications. 2. Is there a process to manage the capacity requirements of supporting utilities. 3. Are the equipments supporting the utilities is inspected and tested regularly to ensure their proper functioning. 4. Are the emergency switches and valves to cut off power, water, gas or other utilities implemented. 5. Does the organization have adequate emergency lighting and communications.	
7.12	Cabling security	Cables carrying power, data or supporting information services should be protected from interception, interference, or damage.	1. Are the power and telecommunications lines into information processing facilities fed underground wherever possible or equipped with adequate protection like floor cable protector or utility poles. 2. Are the power and telecommunication cables separated to prevent interference. 3. Are the cables labelled at each end	

			with sufficient source and destination details to enable the physical identification and inspection of the cable.	
7.13	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.	1. Are the equipments maintained in accordance with the supplier's recommended service frequency and specifications. 2. Does the organization ensure only authorized maintenance personnel carrying out repairs and maintenance on equipment. 3. Is there a process to supervise maintenance personnel when carrying out maintenance on site. 4. Is there a process for authorizing and controlling access for remote maintenance. 5. Is there a process for inspecting the equipments before putting the back into operation after maintenance, to ensure that the equipment has not been tampered with and is functioning properly.	
7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	1. Has the organization defined a formal process for secure disposal and reuse of equipments/assets. 2. Does the organization ensure to physically destroy or erase the data in storage devices before disposal. 3. Does the organization ensure to remove labels and markings identifying the organization or indicating the classification, owner, system or network before disposal.	

FOLLOW US ON LINKEDIN FOR MORE FREE CHECKLISTS

PLAYBOOK MADE WITH 

MINISTRY OF SECURITY