ISO 27001

CONTROLS MADE EASY

MAKING INFOSEC RELATABLE THROUGH SCHOOL SCENARIOS!

PART 2

MINISTRY OF MOS SECURITY

Control Number	Control Name	Real Life Example	Implementation Guidance
6.1	**Screening**	Schools conduct background checks before hiring teachers, administrative staff, or support staff. Just like how they verify teaching credentials, past employment, and criminal records to ensure student safety, they also check references to confirm the person's reliability and trustworthiness. **Information Security Connection:** Organizations must verify potential employees' backgrounds before giving them access to sensitive information. Like schools protecting students through staff screening, companies need thorough verification processes to prevent security risks from inappropriate hires.	• Create screening policy and procedures • Define verification requirements by role • 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**	Schools include clear security responsibilities in teacher contracts - maintaining student confidentiality, protecting exam materials, proper handling of student records. These terms are explained and agreed upon before starting employment. **Information Security Connection:** Organizations must clearly define security responsibilities in employment terms. Like schools making teachers understand their obligations to protect student information, companies need clear security expectations in employment agreements.	• 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**	Schools regularly train teachers and staff on various aspects - from new teaching methods to emergency procedures, child psychology to first aid. New teachers undergo orientation	• Create security awareness program • Develop training materials • Conduct regular sessions • Track participation

		programs, while existing staff attend regular workshops to stay updated. When new smart boards are installed, teachers receive training on their proper use and maintenance. **Information Security Connection:** Similarly, organizations must provide regular security awareness and training to employees. Like schools ensuring teachers are competent through ongoing training, companies need comprehensive security training programs to keep staff updated on security threats, proper information handling, and security procedures.	• Test understanding • Update training content • Measure effectiveness • Document completion
6.4	**Disciplinary process**	Schools maintain clear disciplinary procedures for all staff - from being late to classes, improper behavior, or not following school policies. Each violation has defined consequences and fair hearing processes, ensuring consistent handling of all cases, just like how student disciplinary issues are handled systematically. **Information Security Connection:** Organizations need similar formal processes for handling security violations. Like schools managing policy breaches fairly and consistently, companies must have clear procedures for addressing security violations, ensuring fair treatment while maintaining accountability.	• stablish disciplinary procedures • Define violation categories • Document consequences • Ensure fair process • Maintain violation records • Communicate procedures • Train managers • Review effectiveness
6.5	**Responsibilities after termination or change of employment**	When teachers leave or change roles within school - like moving from class teacher to department head - schools ensure proper handover. Departing teachers return all materials, hand over student records, provide status of ongoing projects, and transfer responsibilities. Their access to	• Create termination/change checklist • Document handover requirements • Manage access right changes • Collect organization assets • Update security records

		school resources is adjusted or removed based on their new situation. **Information Security Connection:** Organizations must manage security responsibilities during role changes or exits. Like schools ensuring proper handover of teaching materials, companies need procedures to handle access rights, return of assets, and transfer of responsibilities when employees change roles or leave.	• Brief on ongoing obligations • Verify completion of process • Archive relevant documentation
6.6	**Confidentiality or non-disclosure agreements**	Schools have staff sign agreements about maintaining confidentiality - protecting student personal information, internal school matters, or sensitive situations like student counselling cases. Even temporary staff and volunteers sign these agreements before working with students. **Information Security Connection:** Organizations need binding agreements to protect sensitive information. Like schools ensuring staff maintain student confidentiality, companies must have formal agreements preventing unauthorized disclosure of business information by employees and contractors.	• 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**	During situations like snow days or teacher conferences, schools manage remote teaching. Teachers follow guidelines for conducting online classes, accessing school systems from home, and protecting student information while working remotely. Like having rules for field trips, remote work has specific safety protocols. **Information Security Connection:**	• 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

		Organizations must secure remote work environments. Like schools managing remote teaching safely, companies need policies and controls to protect information when employees work outside office premises.	
6.8	**Information security event reporting**	Schools have clear reporting procedures for various incidents - from missing attendance registers to unauthorized visitors on campus. Staff know exactly whom to inform, like reporting to the nurse for health issues or to the principal for serious disciplinary cases. **Information Security Connection:** Organizations need clear security incident reporting procedures. Like schools having defined reporting channels for different situations, companies must establish how employees report security concerns or incidents.	• 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
7.1	**Physical security perimeters**	Schools have multiple security layers - boundary walls, security gates, locked building entrances, and restricted areas like staff rooms and labs. Each layer adds protection, just like an onion's layers, ensuring students and assets remain safe from unauthorized access. **Information Security Connection:** Organizations must establish clear physical security boundaries. Like schools protecting their premises through multiple barriers, companies need defined security perimeters to protect their information assets and systems.	• 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
7.2	**Physical entry**	Schools control who enters their premises - visitors sign in at reception, wear badges, parents need appointments, and delivery personnel have designated areas. Different areas have different access levels, like how science	• Establish entry control procedures • Implement visitor management • Create access authorization process

		labs are only accessible during class hours with teacher supervision. **Information Security Connection:** Organizations must control physical access to facilities. Like schools managing visitors and access to different areas, companies need proper entry controls to protect areas containing sensitive information and systems.	• Maintain access logs • Monitor entry points • Regular access reviews • Train security personnel • Document unauthorized attempts
7.3	**Securing offices, rooms and facilities**	Schools secure different areas based on their purpose - principal's office for confidential meetings, examination room for storing question papers, server room for IT equipment. Each room has specific security needs, like keeping the chemistry lab locked when not in use for safety. **Information Security Connection:** Organizations must implement appropriate physical security for different areas. Like schools having extra locks for the exam room, companies must apply stronger security for server rooms, R&D labs, and areas containing sensitive documents. This includes special locks, restricted access lists, and proper monitoring of these secure spaces.	• 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**	Schools monitor their premises through various methods - security guards patrolling, CCTV cameras covering key areas, motion sensors after hours. Like a watchful eye, these systems help detect and respond to unauthorized activities, just as teachers monitor hallways during breaks. **Information Security Connection:** Organizations must implement continuous monitoring of secure areas. Like schools using CCTV	• 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

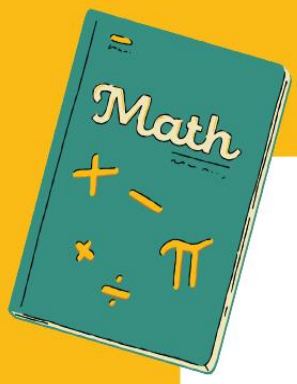
		for campus security, companies need surveillance systems, security patrols, and alarm systems to protect data centres, document storage rooms, and other sensitive areas from unauthorized access.	• Update systems as needed
7.5	**Protecting against physical and environmental threats**	Schools protect against various threats - fire alarms and extinguishers for fire safety, lightning rods for storms, proper drainage for floods, and earthquake protocols. Like having a school nurse for health emergencies, they prepare for different physical threats. **Information Security Connection:** Organizations must protect information assets from environmental threats. Like schools safeguarding against natural disasters, companies need protection against fire, flood, power issues, and other physical threats that could damage IT equipment or sensitive information.	• 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**	Schools have specific procedures Schools manage work in sensitive areas - maintenance staff supervised in server rooms, cleaners given specific times for exam storage areas, contractors escorted in administrative offices. Like having teachers present during lab sessions, work in secure areas needs supervision. **Information Security Connection:** Organizations must control activities in secure areas. Like schools supervising maintenance work in sensitive areas, companies need procedures for supervising contractors, cleaning staff, and visitors in areas containing sensitive information or critical systems.	• 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

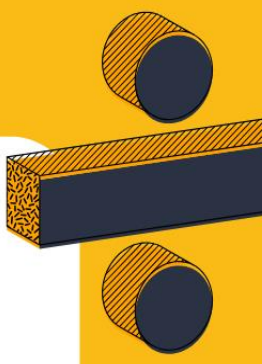
7.7	**Clear desk and clear screen**	Schools practice tidiness - teachers secure student records after use, clear their desks before leaving, lock computer screens when stepping away. Like keeping exam papers secure when not in use, sensitive materials are never left unattended. **Information Security Connection:** Organizations need clear desk and screen policies. Like schools securing student information, companies must ensure sensitive documents aren't left on desks and computer screens are locked when unattended to prevent unauthorized viewing.	• 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**	Schools carefully place their equipment - computers away from windows to prevent rain damage, servers in temperature-controlled rooms, projectors securely mounted. Like placing science equipment in proper storage cabinets, each device needs appropriate placement and protection. **Information Security Connection:** Organizations must carefully position and protect equipment. Like schools protecting their educational equipment, companies need to properly locate servers, workstations, and network equipment to protect from environmental threats, unauthorized access, and accidental 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**	Schools protect assets taken outside - laptops for field trips, sports equipment for tournaments, student records for external exams. Like tracking library books borrowed by students, all assets leaving school premises are monitored.	• Create off-site asset policy • Track asset movement • Define protection requirements • Train users on security • Regular asset checks

		Information Security Connection: Organizations must secure assets used outside office premises. Like schools tracking equipment on field trips, companies need procedures for protecting laptops, mobile devices, and documents when used off-site.	• Document asset location • Monitor asset usage • Review security measures
7.10	**Storage media**	Schools manage various storage devices - USB drives with teaching materials, CDs with student performances, external hard drives with school records. Like organizing the school library books, each storage media is labelled, tracked, and stored properly. **Information Security Connection:** Organizations must protect all storage media. Like schools managing educational material storage, companies need procedures for handling USB drives, hard disks, and other media containing sensitive information, including proper labelling, secure storage, and safe disposal.	• Create media handling procedures • Implement secure storage • Track media movement • Label media appropriately • Control media access • Secure media disposal • Document media inventory • Regular storage audits
7.11	**Supporting utilities**	Schools maintain essential utilities - backup generators for power cuts, water tanks for supply issues, multiple internet connections. Like having backup bells for power failures, schools ensure critical services continue working. **Information Security Connection:** Organizations must ensure supporting utilities are reliable. Like schools maintaining backup power, companies need redundant utilities to protect information processing facilities from failures in power, cooling, or network connectivity.	• 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**	Schools protect their cables and wiring - computer lab cables	• Plan cable installations

		properly organized, PA system wiring secured, science lab connections safely installed. Like having properly labelled electrical connections in labs, all cables are protected and identifiable. **Information Security Connection:** Organizations must secure network and power cabling. Like schools protecting lab equipment connections, companies need to protect data and power cables from damage, interference, or interception through proper installation and physical protection.	• 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
7.13	**Equipment maintenance**	Schools regularly maintain their equipment - servicing laboratory instruments, maintaining computers, checking projectors. Like scheduled maintenance of school buses, all equipment follows service schedules to keep working properly. **Information Security Connection:** Organizations must maintain information processing equipment. Like schools maintaining educational equipment, companies need regular maintenance of servers, computers, and network devices to ensure availability and integrity of information systems.	• 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**	Schools handle old equipment carefully - wiping computers before disposal, shredding old record books, proper disposal of storage devices. Like cleaning student lockers at year-end, all equipment is cleared before disposal or reuse. **Information Security Connection:** Organizations must securely dispose of or repurpose equipment. Like schools clearing	• Define disposal procedures • Verify data removal • Document disposal actions • Control disposal process • Train disposal staff • Check cleared equipment • Maintain disposal records • Review disposal methods

		old computers, companies need procedures to ensure no sensitive information remains on equipment before disposal, sale, or reuse.	





DID YOU FIND THIS CHECKLIST USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

MINISTRY OF MOS SECURITY

WWW.MINISTRYOFSECURITY.CO