INFORMATION SECURITY FOR SUPPLIERS

SECURITY REQUIREMENTS TO BE FOLOWED BASED ON DATA CLASSIFCATION AND CRITICALITY

MINISTRY OF
MOS
SECURITY

Information Security for Suppliers

Based on data shared & its classification

Activity	**Required Based on Data Classification?** *(An “X” in any square below means the applicable Activity is required for the applicable Data Classification. A blank square means the applicable Activity is not required for the applicable Data Classification.)*			
	Public	**Internal Use**	**Restricted**	**Secret**
Policies and Training				
a. Information Security and Privacy Policies and standards must be formalized and documented, reviewed at least every two years, and updated as needed.		X	X	X
b. Personnel must be required to sign a document or electronic acknowledgement, indicating their understanding of, and agreement to abide by, all policies and standards at least annually.			X	X
c. Training and awareness activities must be conducted to heighten workforce understanding of the importance of data security. The Third Party must document existence of and participation in training and awareness activities.		X	X	X
Human Resources				
a. Where permissible by law, all Services Personnel must clear screening and/or background checks (i.e., employment verification, professional references, academic / professional credentials) prior to handling Organisation Data.	X	X	X	X
b. The Third Party shall ensure any subcontractor, business partner, or other Services Personnel involved in performing the services or who have access to Organisation Data comply with the applicable Organisation Information Security requirements defined within this exhibit and will provide evidence of compliance upon request.		X	X	X

	Required Based on Data Classification? *(An "X" in any square below means the applicable Activity is required for the applicable Data Classification. A blank square means the applicable Activity is not required for the applicable Data Classification.)*			
Activity	**Public**	**Internal Use**	**Restricted**	**Secret**
System Authentication and Authorization				
a. All users of information systems must be given a unique User Account and password.		X	X	X
b. The use of a User Account by multiple individuals is prohibited.		X	X	X
c. Sharing of User Account passwords is prohibited.		X	X	X
d. The Third Party must have controls in place to detect and prevent repetitive "brute force" attempts and temporarily suspend the involved end user account.			X	X
e. There must be a password policy, available for Organisation review, which requires all of the following (i. through iii.):				
i.At least eight (8) characters in length.		X	X	X
ii. At least two (2) complexity controls (e.g., uppercase letter, number, and special character). **NOTE**: if the required complexity cannot be achieved, minimum password lengths of fifteen (15) characters in an adequate mitigating control.		X	X	X
iii. Change at least every 180 days, without reuse of previous six (6) passwords.		X	X	X
f. System and Service Accounts (e.g., operating system, application) must have default passwords changed prior to Operational Use.		X	X	X
g. Entities having access to Organisation Data and resources must be appropriately identified. Access to System, Service, or Shared Accounts by an individual must be accountable to that individual.		X	X	X
h. Embedded passwords (i.e., System Accounts, Service Accounts) must meet all of the following controls (i. through iii.):				

Activity	**Required Based on Data Classification?** *(An "X" in any square below means the applicable Activity is required for the applicable Data Classification. A blank square means the applicable Activity is not required for the applicable Data Classification.)*			
	Public	**Internal Use**	**Restricted**	**Secret**
i.Be protected from unauthorized access and accidental disclosure.		X	X	X
ii. Passwords must be changed in response to an event that creates exposure of the account password to unauthorized users		X	X	X
iii. Have a complexity level requiring: A. At least fifteen (15) characters in length. B. At least two (2) complexity controls (i.e., uppercase letter, number, and special character). **NOTE:** If the required complexity cannot be achieved, a minimum password length of twenty (20) characters is an adequate mitigating control. C. Change annually, without reuse of previous six (6) passwords D. Change password in the event an individual's authorization to use the account has been revoked.		X	X	X
i. Credentials used for verification of identity or authentication must be encrypted at rest and in motion.		X	X	X
j. Third Parties must authorize and inventory devices that are owned or controlled by the Third Party that access, process or store Organisation Data.			X	X
k. Access controls or other processes used to grant authorized access to Organisation Data and Systems must be: 1) in place; 2) based on the Principle of Least Privilege access rights; and 3) role based.		X	X	X

Activity	**Required Based on Data Classification?** *(An "X" in any square below means the applicable Activity is required for the applicable Data Classification. A blank square means the applicable Activity is not required for the applicable Data Classification.)*			
	Public	**Internal Use**	**Restricted**	**Secret**
l. User access rights must be reviewed (i.e., recertification) based on the sensitivity of the information being accessed as follows:				
i.Privileged Users/Accounts	Not Required, unless regulatory requirement supersedes	Not Required, unless regulatory requirement supersedes	X (every 180 calendar days)	X (every 90 calendar days)
ii. Standard Users/Accounts	Not Required, unless regulatory requirement supersedes	Not Required, unless regulatory requirement supersedes	X (every 12 months)	X (every 12 months)
m. When a Third Party employee is terminated or otherwise ceases to provide services related to Organisation, access must be terminated as follows:				
i.Effective access to Organisation Data must be removed or disabled (e.g., disabling network access, remote connectivity).		X (72 hours)	X (48 hours)	X (48 hours)
ii. User Accounts associated to an individual within an application or system that contains Organisation Data must be deactivated or deprovisioned.		X (180 calendar days)	X (90 calendar days)	X (30 calendar days)
iii. A process for emergency, immediate removal of user access must exist.		X	X	X
n. Access when a user is shifting departments/roles must be reassessed within thirty (30) days of the user's job change completion.			X	X
o. Emergency access changes must be completed per a documented change control process.		X	X	X
Data Protection				
a. Organisation Data in motion must be encrypted using industry standard technologies.			X	X
i.Organisation Data in motion (email platform) must be encrypted using industry standard technologies.			X	X

	Required Based on Data Classification? *(An "X" in any square below means the applicable Activity is required for the applicable Data Classification. A blank square means the applicable Activity is not required for the applicable Data Classification.)*			
Activity	**Public**	**Internal Use**	**Restricted**	**Secret**
b. Organisation Data must be encrypted when at rest using industry standard technologies.				X
c. A plan must be in place to address the secure return or destruction of Organisation Data as part of contract termination.		X	X	X
d. All removable media with Organisation Data must be encrypted using industry standard technologies.			X	X
e. Organisation production data must be prevented from being used in non-production environments. If exceptions exist, sensitive information must be masked before use in non-production environments, and controls put in place to prevent reintroduction of test data into production.			X	X
f. Devices that contain Organisation Data must have screens that lock automatically after, at most, fifteen (15) minutes of inactivity.			X	X
g. Physical media containing Organisation Data must be protected from unauthorized access during transport.			X (Sealed packaging)	X (Locked container)
h. Delivery tracking and signature is required for transportation of physical media containing Organisation Data.			X	X
Infrastructure Protection				
a. Standardized and current antivirus software or host-based intrusion prevention software must be deployed on all end user systems and servers. A standard policy must exist to ensure that systems and servers containing Organisation Data are actively scanned for malicious software.	X	X	X	X
b. Antivirus software must be configured to prevent users from changing any settings or	X	X	X	X

	Required Based on Data Classification? *(An “X” in any square below means the applicable Activity is required for the applicable Data Classification. A blank square means the applicable Activity is not required for the applicable Data Classification.)*			
Activity	**Public**	**Internal Use**	**Restricted**	**Secret**
disabling the antivirus protection.				
c. Firewall and content filtering logs must be created and saved for at least a 14 day period and be available for review in the event of an incident.			X	X
d. An Intrusion Detection/Prevention System must be in place, on all egress/ingress points to the internet, with active, automated alerts enabled and monitored.			X	X
e. Activity Event Logs recording important information security events related to Organisation Data must be produced, retained, and reviewed in a risk-based manner as follows:				
i.Activity must be logged at a level of detail that maintains individual accountability for actions.			X	X
ii. Log information must be protected against loss, tampering, and unauthorized access.			X	X
f. Identified vulnerabilities (e.g., patches, configuration) must be prioritized, based on a defined evaluation procedure, and remediated in an established timeframe.			X	X
g. Remote access to the Third Party’s network must have security controls in place to ensure authenticated and authorized access.		X	X	X
h. Wireless access points on the Third Party’s internal network must be encrypted and user authentication enabled in accordance with industry standards.		X	X	X
Incident Response				
a. A process must exist to establish, document, and annually assess for validity and effectiveness of an information security incident response plan.	X	X	X	X
b. A notification process must be in place to inform Organisation if	X	X	X	X

	Required Based on Data Classification? *(An "X" in any square below means the applicable Activity is required for the applicable Data Classification. A blank square means the applicable Activity is not required for the applicable Data Classification.)*			
Activity	**Public**	**Internal Use**	**Restricted**	**Secret**
the Third Party experiences or suspects a Data Security Incident affecting Organisation Data.				
c. All reported Data Security Incidents must be documented by the Third Party, and Organisation must be notified immediately and, in any event, no later than 24 hours upon discovery of a Data Security Incident involving Organisation Data.	X	X	X	X
Physical Security				
a. Physical security and access control measures must be in place to ensure that only authorized personnel and visitors are allowed access, on an as-needed basis, to areas containing Organisation Data.		X	X	X
b. Visitors must be escorted at all times in areas containing Organisation Data. (e.g., data center).			X	X
c. Facilities containing Organisation Data must be monitored (e.g., guard station, video recording, alarm service) for unauthorized access.			X	X
d. Auditing of physical access controls must occur once every twelve (12) months.			X	X
e. Access privileges, activity logs, and visitor logs must be reviewed for irregularities in a defined manner.			X	X
f. Physical security incidents must be documented and analyzed with appropriate corrective actions implemented.			X	X
g. Ensure Organisation Data is not viewable by personnel supporting non-Organisation systems in work areas performing Help Desk and/or Support services that are shared in support of other customers.			X	X
h. Physical security standards, policies, and procedures must be			X	X

	Required Based on Data Classification? *(An “X” in any square below means the applicable Activity is required for the applicable Data Classification.* *A blank square means the applicable Activity is not required for the applicable Data Classification.)*			
Activity	**Public**	**Internal Use**	**Restricted**	**Secret**
established, documented, and communicated to Third Party Personnel.				
i. Organisation Data and computer access to Organisation Data must not be left unsecured when an individual is away from their desk.			X	X
Disaster Recovery				
a. The Third Party will develop and maintain appropriate Disaster Recovery Plans in alignment with Organisation business requirements specific to the solution.	X	X	X	X

DID YOU FIND THIS CHECKLIST USEFUL

FOLLOW FOR FREE INFOSEC CHECKLISTS | PLAYBOOKS TRAININGS | VIDEOS

MINISTRY OF
MOS
SECURITY

WWW.MINISTRYOFSECURITY.CO