MINISTRY OF SECURITY

VENDOR SECURITY CHECKLIST

Information Security		
Control statement	**Control Implemented (Yes, No, Partial, NA)**	**Remarks**
Do you have a valid third-party information security/cybersecurity attestation or certification?		
Do you have company-wide, publicly available information security policies in place?		
Is the Information Security Policy is reviewed at planned intervals, or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness?		
What mechanisms are in place to ensure your policies are enforced within your supply chain?		
Are the roles and responsibilities pertaining to information security defined and communicated to all employees?		

Asset Management		
Control statement	**Control Implemented (Yes, No, Partial, NA)**	**Remarks**
Do you have an asset management program approved by management for your IT assets?		
What are your methods to manage IT assets on the network?		
How do you manage other IT hardware and software assets, which are not network connected, regardless of network presence?		
Do you have documented policies or procedures to manage enterprise assets throughout their lifecycle.		
Do you have policies or procedures to ensure your enterprise software platforms applications, and hardware		

assets, are classified according to their criticality.		
Do you have policies or procedures to ensure appropriate controls are in place for internal or third-party cloud services.		
Do you maintain an up-to-date inventory of hardware and software assets to ensure their accountability and integrity.		
Do you have processes or procedures for secure disposal of your assets.		
Does media containing information protected against unauthorized access, misuse or corruption during transportation beyond the organization's physical boundary.		
Do you maintain information labelling and handling procedures. Are documented information tagged/labelled as per your asset classification schema.		

Identity and Access Management		
Control statement	**Control Implemented (Yes, No, Partial, NA)**	**Remarks**
Are Procedures defined and followed for provisioning access (logical and Physical) to information systems and information processing facilities.		
Are Procedures defined and followed for provisioning access to Network and Network devices.		
Are procedures defined and followed for management of privilege access rights.		
Do you have specific procedures established and maintained to avoid the unauthorized use of generic administration user IDs (super admin, super user IDs), according to systems' configuration capabilities.		

While provisioning access rights and privileges on information and information systems do you determine if access rights, and privileges are based upon business needs/requirements and that these provide for adequate segregation of duties.		
Are user access provisions monitored and reviewed on an ongoing basis to ensure additions, deletions and changes to the accounts and access rights are properly tracked.		
Are procedures defined and followed for removal of all access rights (Logical Access and Physical Access).		
Do you have procedures defined and followed for Password management (covering password strength, password history, password expiry, password reset, etc.) for accessing information and information assets.		
Have you deployed password security controls within the environment on application, OS, database and network layers.		
Do you have a secure log-on procedure documented.		
Does the User Account get automatically Locked out after predetermined unauthorized attempts.		

Human Resource Security		
Control statement	**Control Implemented (Yes, No, Partial, NA)**	**Remarks**
Do you have procedures defined and followed for onboarding personnel.		
Do you have procedures defined and followed for conducting background checks of your employees, contractors		

and third parties as permitted by the country in which you operate.		
Are employees, contractors and third parties mandated to sign a non-disclosure or confidentiality agreement / NDA / Code of conduct.		
Do you have an information security awareness program mandatory for all employees' contractors and third parties.		
Are all staff required to take the information security awareness trainings and sessions upon hire and periodically thereafter.		
Is there additional security training provided to users with elevated privileges.		
Are you aware of security training practices performed by your sub-suppliers to their personnel.		
Do you have disciplinary procedures/code of conduct defined and followed for employees who have committed a security breach.		
Are the employees aware of the fact that in case they breach security there could be a disciplinary action taken against them.		
Do you have procedures defined and followed for offboarding personnel.		
Does the process include a process to transfer knowledge to other personnel.		
What is the process to remove access to all company documents, applications, assets, etc.		
What is the process to recover all company assets.		

Physical Security		
Control statement	**Control Implemented (Yes, No, Partial, NA)**	**Remarks**
Do you have physical security procedures defined and followed that address the control of physical access, environmental protection, equipment maintenance, equipment siting, visitor management etc.		
Is access to sensitive areas (server location, tape library, computer room, etc.) physically restricted to authorized personnel, If yes, does the physical access system log the access capturing the data, time, door access, employee coordinates during logging physical access.		
Are all physical access control logs periodically reviewed and retained per retention requirements.		
Are visitors signed into the building by an employee who accepts responsibility for the visitors during the course of their visit.		
Do you have fire alarm/suppression systems installed across office (secure areas/work areas).		
Do you use CCTV cameras to monitor the facility on a 24x7?		
Are redundant power supplies available for supplying power to critical equipment?		
Is there an Uninterruptible Power Supply (UPS) or DG set backup for the premises?		
Is lightning protection applied to the buildings and lightning protection filters fitted to all incoming power and communications lines at the premise housing work area and information processing facilities?		
Are all the information systems equipment's maintained in accordance		

with the supplier's recommended service intervals and specifications		
Are records kept of all suspected or actual faults and all maintenance activities performed on equipment's Is the maintenance carried out by authorized personnel only?		
Do you have process in place to manage movement of assets in and out of the organization		
Do you have processes in place to prevent counterfeit parts from entering your supply chain?		
Do you have process in place to protect unattended equipment within the organization		
Do you have a clear desk and clear screen policy in force in the organization.		
Do you have a documented Security Incident Response process covering physical security incidents		

Operations Security		
Control statement	**Control Implemented (Yes, No, Partial, NA)**	**Remarks**
Are applications and operating system software implemented after extensive and successful security testing.		
Is there a log maintained to track installation of operational software on workstations.		
Do operational systems hold only approved Software's and there is a periodic audit to track Software Compliance.		
Are users disallowed to install software on their workstations.		
Are external drives such as CDs and USB drives disabled on all desktops and		

laptops, servers containing personal data, customer data, business data.		
Are audit logs maintained that record user activities, exceptions, success and failure logons, policy changes, events, and information security events in order to assist in future investigations and access control monitoring.		
Are system administrator and system operator activities monitored and logged.		
Can system administrator activities be tracked to individual system administrators.		
Do you have a policy/procedure on change management.		
Are all changes to production environment recorded and follows the change management procedure.		
Do you maintain a policy, operational plan and procedures for teleworking activities and whether teleworking activity is authorized and controlled by management and does it ensure that suitable arrangements are in place for this way of working.		
Does patch management process ensure all system are installed with latest security patches (OS layer, Application layer, Data base layer, Network layer).		
Do you have a formal vulnerability assessment and penetration testing (VAPT) process / procedure / policy / manual is documented and operational.		
Do you have security hardening (technical specification, minimum baseline security MBSS guidelines for all infrastructure elements such as Application, OS, Network and Database).		
Have you deployed controls to protect computer systems against virus and spywares, malwares, Trojans, malicious codes, etc.		

Have you implemented data protection and privacy measures such DLP, IRM / DRM etc.		
Have you deployed any encryption / protection mechanism (data at rest) on databases, file servers, desktops and laptops handling business data, customer data, personal data (account numbers, employee details, bank accounts, password, card magnetic stripe data, etc.) in compliance with all relevant rules, laws, regulations, legal and contractual obligations, country specific data privacy laws, sector specific data privacy laws.		
Have you deployed any encryption mechanism (data in transit and rest) to secure data in rest and motion.		
Do you agree to allow Auditors or Contracted Third Parties conduct IS Audit at your premise.		
Do you have documented procedures for the identification, capture, tracking, escalation and resolution of operational problems/incidents (all systems, applications or facility-related problems).		
Whether any Firewall, deep packet inspection solution, IPS/IDS, DLP, Anti APT, SIEM, Anti Spoofing and other such security solutions (Perimeter, Endpoint, Web, Infrastructure) have been implemented in the network infrastructure.		
Are Users Handling organization data given access to Corporate / Public Mails. If Yes, are there any restrictions on domains to which the mails can be sent.		
Are users handling organization data provided access to the Internet.		
Is there a Proxy / Content Filtering Solution in place for controlled access to Internet.		

Are the system clocks of all information processing system within the organization or security domain synchronized with an agreed accurate time source.		
Are the system utility programs that could be used to override system and application controls strictly controlled and their use restricted and that admin privileges are not assigned to all users.		
Do you have an organization-wide strategy for managing development, acquisition, life cycle support, and disposal of systems, system components.		
How does your company safeguard your product or service against fraudulent and/or fake IP components.		
To reduce security risks, does your company define, adhere to, and validate safe coding practices.		
Does your organization verify that third-party software provides required security requirements/controls.		

Supply Chain Security		
Control statement	**Control Implemented (Yes, No, Partial, NA)**	**Remarks**
Do you have written Supply Chain Risk Management requirements in your contracts with your suppliers.		
Do you perform due diligence on vendors before onboarding.		
Does your business take into account supplier diversification to prevent reliance on a single source and to lessen the likelihood that suppliers may face the same risks to their resilience.		
Does your business take into account alternative providing delivery channels, such as cloud, network,		

communications, transportation, and packaging, to offset prolonged supplier outages.		

Business Continuity		
Control statement	**Control Implemented (Yes, No, Partial, NA)**	**Remarks**
Do you maintain a formal business continuity plan necessary to maintain operations through disruptions and significant loss of staff.		
Do you have a Disaster Recovery Plan in place to support recovery of key products & services		
Do you maintain a formally trained and dedicated crisis management team, including on-call staff, assigned to address catastrophic or systemic risks to your supply chain processes?		
Do you have a Test Calendar in place to test Business Continuity Plan?		

Authors

Niranjan V
ISO 27001 LA