Cybersecurity Compliance Requirement

The Maxis **Cybersecurity Compliance Requirement** list the expected security controls that Maxis Suppliers are required to adopt when (a) accessing Maxis facilities, networks and/or information systems, (b) handling Maxis Confidential Information including Personal Data.

Maxis Supplier is responsible for compliance with these Standards by its personnel and subcontractors, including ensuring that all its' personnel and subcontractors are bound by contractual terms consistent with the requirements of these Standards. Additional security compliance requirements may be specified in the agreement or individual statement of work.

Part A: Border Control
Part B: Access to Systems and Applications
Part C: Systems and Application Configuration
Part D: Protect Maxis and related Confidential Data.
Part E: Malware Protection
Part F: Patch Management and Application Security.
Part G: Restrict Access to PII
Part H: User IDs and traceability of user access.
Part I: Physical access to systems and data.
Part J: Handing of Media and Data.
Part K: Track and Monitor all access network resources and PII.
Part L: Regularly Test the security systems and processes
Part M: Information Security Policies, Acceptable Use and Risk Mgmt
Part N: Security on Human Resources/Personnel

A Border Control to protect information related to Maxis.

Ensures that the controls measures surrounding the systems are adequate and managed effectively.

a.1 Managed border control devices (Firewalls, Routers, IPSec, etc.) which are designed to protect the Maxis related infrastructure and data from unauthorized access and abuse are employed effectively to cover all the relevant systems.

a.2 Access to these border control devices should be limited those with a need and logged to provide traceability of work done.

a.3 The network traffic and access control rules applied to such devices should be reviewed regularly to ensure the services rendered are secure.

a.4 Network and Systems design documents detailing the storage, access, transport, protection of Maxis related data shall be kept current for audit purposes.

B Access to Systems and Applications.

Ensures that the applications servicing Maxis are secured and access to these applications are managed effectively to allow only authorized users access to them.

b.1 Public accessibility of the system component should be prohibited from all vectors of access (example: wired and wireless).

b.2 Data repositories containing Maxis Confidential Data (Database, files, etc) should be placed in a securely protected internal network segment.

b.3 Access to such data should be limited to only to authorized users under the control of the Service Provider and authorized to work on the contract.

b.4 The authorized user list should be validated periodically to ensure the list is current.

b.5 Remote access to such data should be strictly controlled and monitored to ensure network connectivity is made over encrypted secure channels and authentication performed to validate the authorized users.

b.6 Appropriate controls implemented to ensure there are network segmentation for client data storage and processing. Please specify controls to ensure secure Internet Access

b.7 Implement security controls to ensure data are secured especially when using 3rd party data centre

b.8 If the system holds Credit Card data (CHD) the instance of the dataset must be kept secure (e.g.: encrypted, limited access, no cached plain text copies) for those who need to know only.

C System and Application configuration

Ensure the Systems and Applications used to service Maxis are safe, secure and managed to provide optimal service.

c.1 Systems hosting services for Maxis should be configured to perform safely, securely and provide availability to the defined SLAs.

c.2 Place logical and physical separation on systems used for delivering the services of Maxis from others. If a shared hosting model is used, protect the Maxis related services to ensure separation of the data and access.

c.3 Disable unnecessary and insecure services and protocols.

c.4 Configure the systems to prevent misuse.

c.5 Encrypt all non-console administrative access using industry standards. (eg: SSH, VPN, SSL/TLS.)

c.6 Ensure logging and audit trails are enabled to identify access to Maxis related systems and service platforms.

c.7 Enable processes to provide timely forensic investigation in the event of compromise of any hosted system relating to Maxis.

D Protect Maxis and related Confidential Data.

Keep Maxis Confidential data secure, develop a data retention and disposal policy, and limit the storage and retention to a limit that is required for business, legal and/or regulatory purpose.

d.1 If access to Personal data is supplied, available or provided as part of the service all controls necessary to comply with the Personal Data Protection Act (PDPA 2010) has been implemented to maintain Maxis' compliance to the Act.

d.2 Do not store authentication data in any readable format even if encrypted.

d.3 Keep Personally Identifiable Information (PII) protected from casual access all the times.

d.4 Use strong encryption to protect PII and all confidential data stored at endpoints, servers and database

d.5 Implement controls to protect data leakage from endpoints/servers accessing/storing Maxis data and servers are hardened to protect and monitor data leakage.

d.6 Have an appropriate procedure/standard for disposal of Maxis' Confidential data.

d.7 Implement control to track the successful disposal of Maxis data and provide report to track activity

d.8 Ensure change management process is in place for changes deployed to infrastructure, application or Database where in Maxis data is stored, processed or transmitted.

d.9 Ensure control is implemented to validate the adherence of change management policy and to identify unapproved changes.

d.10 Manage access to confidential data centrally and reduce the number of repositories that hold such data.

d.11 Do not allow confidential data to be copied to removable media unencrypted by keys available to the service provider.

d.12 Protect the keys used to encrypt Maxis confidential information against disclosure and misuse.

d.13 Document and enforce all key-management processes and procedures and avoid single points of failure in the key management scheme.

d.14 Keep confidential data separate from the access and authentication keys used to access the data and ensure both are securely protected.

d.15 Use strong cryptography and security protocols when providing access to PII over open public networks.

d.16 Never allow the transmission of access control information (usernames & passcodes) over an unencrypted channel.

d.17 Established a process for encrypting emails, removable media and endpoints/servers which contains confidential data

d.18 Protect the keys used to encrypt Maxis confidential information against disclosure and misuse.

d.19 Ensure all systems that process, store and transmit Credit Card information is compliant to the PCI/DSS controls. Supplier will provide Maxis with the most recent PCI SSC “Attestation of Compliance” (AoC) reports prepared by a third-party PCI Qualified Security Assessor (QSA) for both Supplier's systems and for any third-parties used by the Supplier for handling payment card data.

d.20 Data flow diagrams are required to be developed and/or produced to Maxis for tracking of data movement.

E Malware protection.

Maxis related infrastructure should be protected from malware at all times.

e.1 Ensure all systems related to the Maxis Service delivery are protected by Malware prevention systems and are kept updated and active all the times.

e.2 All computing equipment either requiring connectivity or not requiring connectivity to Maxis Enterprise Network (MEN) must first be approved and registered with Maxis CMDB before access to the network is authorized.

e.3 All computing equipment connected to the Maxis Enterprise Network shall have the mandatory Maxis APT and Security software installed and running. For setup that does not connect to Maxis Enterprise Network, an effective solution for handling Advance Persistent Threats (APT) needs to be in place.

F Patch Management and Application Security.

Systems become vulnerable as software becomes obsolete or new exploits are discovered. Proper patch management and vulnerability assessment mitigates this risk.

f.1 Ensure all system components have the latest vendor supplied patches

f.2 Ensure usage of Maxis related services are done using software applications which have been secured using industry best practices.

f.2.1 Testing security patches prior to release.

f.2.2 Validation of Input to prevent or safely recover from malicious content.

f.2.3 Implementing secure communications.

f.3 Separate development/test and live systems.

f.3.1 Not using live PII in tests.

f.3.2 Ensuring no test or preproduction data and scripts exist in live systems environments.

f.3.3 Proper and documented code review process to remove vulnerabilities prior to release to the live environment.

f.3.4 Documented change review process.

f.3.5 If web development is done, it should be based on secure coding guidelines (like OWASP) to prevent common coding vulnerabilities.

f.3.6 For public facing web application ensure ongoing application vulnerability assessment (VA) and use of web-application firewall (WAF).

G Restrict access to PII

Handling and access to Personally Identifiable Information can result in leakage of confidentialty which affects Maxis and its reputation. Limiting access to this information is the one step in mitigating this risk.

g.1 Practice principle of least privilege - provide privileged access to as few features as necessary to perform their job function.

g.2 Provide privileged access to as few people as necessary to perform their job duties for Service Delivery.

g.3 Collect and monitor and periodically audit use of privileged access.

g.4 Access to sensitive and PII information should be denied to all and selectively allowed based on right to know.

g.5 Establish control to ensure that Maxis data, application processing Maxis data or servers containing such data are accessible from identified IP segment alone by privileged user including controls around remote access.

g.6 Supplier will complete a documented security questionnaire and provide written responses about its security practices, to enable Maxis to assess compliance with the requirements of these Standards.

H User IDs and traceability of user access.

User's access to systems and applications that deal with PII should be kept to a minimum. However, where access is allowed it must be traceable back to an individual to account for the access.

h.1 Users shall be given unique IDs and sharing of IDs or group IDs should be strictly prohibited.

h.2 Use of multifactor authentication apart from passcodes where the information is confidential or where access is gained remotely.

h.3 Render all authentication tokens (Username/passwords) unreadable between the end points of the system and client devices during the authentication process by using strong cryptography.

h.4 Have proper ID management process to ensure access is granted to valid individuals and passcodes are changed regularly.

h.5 Regularly cleanup IDs of terminated users and disable access of inactive users.

h.6 Restrict access to systems by vendors for the period of activity only and based on change management request.

h.7 Ensure that passwords meet the best practices for complexity, size, validity and non-predictability.

h.8 Password failures after an acceptable number of times should lock out the account to prevent any further attempts to login.

h.9 Established a security policy that will govern user access management

I Physical access to systems and data.

Most controls are place on remotely accessing systems and networks, however, if physical access to the system is not controlled then the hardware containing confidential systems may be removed together with the data in it.

i.1 Use appropriate facility entry controls to limit and monitor physical access to systems holding or carrying Maxis Information.

i.2 Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas* and review the collected data against other entries (like work order requests, change requests etc.) regularly for intrusion.

i.3 Restrict access to private network* (wired and wireless) at public or common areas like meeting rooms or lobbies.

i.4 Provide identification (eg Badges) for authorized personnel to differentiate them from outsiders and enforce the use of such identification.

i.5 Ensure proper handling of visitors by requiring identification, authorization, badging, and auditable logging of all entry and exit to areas hosting or serving Maxis infrastructure and services. Retain logs for a period of at least 3 months.

J Handing of Media and Data.

Media storage does not always reside on the harddisk of systems or in backup tapes, it also transits networks or is copied to alternate media for efficient service delivery. Ensure these vectors of acess to media is properly handled for security and privacy.

J.1 Store backup media in a secure location, preferably a secure off-site facility and review the security of the site and the media transfer process at least annually.

j.2 Physically secure all paper and electronic media that contain PII data (eg: Bills, Statements, Customer lists etc.)

J.3 Maintain strict control over the internal and external distribution of any kind of media that contains PII data. Identify it as confidential and transfer it by secured courier or other methods that ensure the privacy and traceability of the transfer.

j.4 Maintain strict control over the storage and accessibility of the PII Media. Ensure inventory logs of all media is maintained and checked regularly.

j.5 Destroy media containing PII or Confidential information when it is no longer needed for business, regulatory or administrative use; or as described in the terms of use.

J.6 Have controls implemented for detecting and protecting unauthorized data movement.

J.7 Established a process for periodic review of classification of data and controls are implemented for data protection.

J.8 Have an appropriate procedure/standard for disposal of Maxis' data. Permanent removal of Maxis data is within 3 months from the termination or end of the agreement. Supplier are responsible to provide a report and artefact showing the before and after of the removal process

J.9 Implement control to track the successful disposal of Maxis data and provide report to track activity

J.10 Implement controls to protect data leakage from endpoints/servers accessing/storing Maxis data and hardened to protect and monitor data leakage.

J.11 Endpoints are restricted/ controlled to transfer files through USB / CD / DVD / any external storage

J.12 Endpoints/servers are protected adequately by implementing antivirus to protect from malware, malicious contents and any other measures as per industry standards

J.13 Controls are implemented to ensure that data accessed by outsourced agency are processed and stored securely

J.14 Controls are implemented to ensure secure handling of hard copies of Maxis data and disposal of hardcopies

j.15 Supplier will maintain a list of its subcontractors, the country/countries to which confidential information may be transferred to or accessed from and will provide that list to Maxis upon reasonable notice.

K Track and Monitor all access network, resources and PII.

Logging mechanisms and the ability to track user activities are critical in preventing, detecting or minimizing the impact of data compromise. The existence of these logs allow the investigation of incidents and identifying improvements to networks.

k.1 Ensure all network access to system components is tied to individual accounts which are not shared.

k.2 Implement automated audit trails for all system components to identify individual access, action taken with elevated privileges, use of identification and authentication tokens, invalid logical access attempts, changes in audit logs, creation and deletion of system-level objects.

k.3 Record at least the following information in the audit trail entries: user identification, date and time, type of event, success or failure of attempt, origin of event, identity or name of affected data, system or resource component.

k.4 Synchronize all critical systems clocks and times to approved NTP servers of at least level 2.

k.5 Secure audit logs so they cannot be altered and use file integrity monitoring tools to detect changes and issue alerts when such changes occur.

k.6 Limit access to audit trail logs to those with a need to know.

k.7 Keep audit logs in a central log server or media that is outside the control or access of administrators whose system components are being logged.

k.8 Keep audit logs of systems components on the external segments secured on internally hosted central log servers.

k.9 Review logs of all system components at least daily; the following systems should be included in such reviews: security control devices like firewalls, intrusion detection and/or prevention tools, AAA servers like RADIUS, TACACS etc.

k.10 Keep audit trail logs for at least 1 year; consider keeping 3 months online and the rest offline if resource is a constraint.

k.11 Ensure all the critical logs are forwarded to a SIEM solution with log correlation capability

k.12 Ensure SOC (Security Operation Centre) is available on a 24X7 monitoring and capable to manage alerts and escalation for prompt action.

k.13 Implement controls to validate effectiveness of data security controls at data center/cloud service provider.

k.14 Immediately inform Maxis about any security/data breach or at least within 24 hours after confirming the breach

L Regularly Test the security systems and processes

Vulnerabiities to systems and networks can be revealed by checking the process and auditing the security controls regularly. Ensure this is done by an independent body to ensure impartial results.

l.1 Test for access points not part of the design of the facility: eg: look for wireless access points, open network jacks that lead to the core network from common areas like public meeting rooms and lobbies.

l.2 Execute internal and external Vulnerability Assessment by qualified network security personnel at least quarterly or after any significant change in the network.

l.3 Perform internal and external Penetration Test at least once a year or after significant infrastructure and application upgrade. Ensure the tests include the network and application layers of the services provided.

l.4 Consider the use of Intrusion Detection or Prevention Systems (IDS/ IPS) to monitor all traffic to networks that handle PII data. And keep the IDS/IPS engines updated regularly.

l.5 Deploy automated file-integrity monitoring software to regularly alert personnel to unauthorized modification of critical system files, configuration files, or content files.

l.6 Provide Maxis with a third-party external Data Security assessment either the SOC 2 or ISO27001 and VAPT status report on annual basis

M Information Security Policies, Acceptable Use and Risk Mgmt

A strong security policy sets the tone for the company on the importance of security and what is expected of them. The policy should be made mandatory for anyone having contact with the systems and networks handling sensitive material to be compliant and enforced by the management.

m.1 Your company are aligned with an industry standard for information security (e.g.: ISO27001, ISO22307, CoBIT, etc.).

m.2 Established process for mitigating non-compliances against data security policy

m.3 Risk Management team or Data Security team reviews the risk assessment methodology and identified security risks on a quarterly basis m.4 Establish, publish, maintain and disseminate a security policy that accomplishes the following: addresses data classification, privacy, and confidentiality, includes annual threat analysis, and verification of security controls.

m.5 Develop and enforce operational security procedures which are consistent with the requirements of the policy. (eg: account management, log audits, etc.)

m.6 Develop and enforce an acceptable use policy for use of the company's infrastructure in a manner that promotes the approved use of infrastructure and end point devices which maintain the security and availability of services.

m.6.i Explicit management approval of systems and network access technology used.

m.6.ii Authentication for use of infrastructure and systems.

m.6.iii Use of company approved products on the corporate infrastructure.

m.6.iv Approved remote access technology.

m.6.v Prohibit the copy or storage of PII on client-side devices, removable and fixed media.

m.7 Ensure that the security policy and procedures clearly define information security responsibilities for all users of the systems and networks and have all users endorse their compliance annually.

m.8 Assign the task of managing information security responsibility to a qualified team.

m.9 Implement continuous and formal security awareness program and make all users aware of the importance of keeping PII data private and secure.

m.10 Screen employees with access to PII data and systems which hold such data to minimize risk of deliberate or malicious disclosure of such data.

m.11 Ensure any subcontractors of the Service Provider carry the same responsibility of compliance to the policies.

m.12 Maintain a written agreement that includes acknowledgement that the subcontractors are responsible for the security of PII held by them.

m.13 Implement an incident response plan and be prepared to respond immediately to a system breach.

m.13.i Ensure the plan covers: Roles, responsibilities, communication and contact strategies in the event of a compromise.

m.13.ii Has well defined procedures to follow.

m.13.iii Has Business recovery and continuity procedures.

m.13.iv Data Backup procedure.

m.13.v Process of disclosure to Maxis in the event of incident or compromise.

m.13.vi Coverage and response of all critical system components.

m.14 A validation and test of the Incident Response Plan at least annually.

m.15 Availability of key personnel on the Incident Response Team on a 24x7 window.

m.16 Establish controls to ensure that reported, identified incidents, problems are acted and closed on timely basis.

m.17 Appropriate training for security breach response responsibilities.

m.18 Logs from intrusion detection, intrusion prevention and file-integrity monitoring systems are readily available for incident analysis.

m.19 Ensure change management process is in place for changes deployed to infrastructure, application or Database where in Maxis data is stored, processed or transmitted.

m.20 Have a plan to review and evolve the incident response plan according to the lessons learned and to incorporate industry changes.

N Security on Human Resources/Personnel

n.1 Supplier will perform background checks, consistent with local laws and regulations, for all their personnel. The level of verification performed should be proportional to risk correlated to roles within the organization.

n.2 Supplier must have formal disciplinary processes in place for personnel and take appropriate action against personnel who violate Supplier's organizational policies, based upon the nature and gravity of the violation.

n.3 Supplier must have a comprehensive security awareness program for all personnel that encompasses education, training and updates for security policies, procedures and requirements.

n.4 Upon termination of employment, Supplier will promptly remove personnel access to information systems, networks and applications. Personnel must also return all company provided computers and mobile devices. Supplier will remind personnel that they must not retain any confidential information.