Cybersecurity General Policy

MAXIS PUBLIC

This Cybersecurity General Policy sets forth the technical and organizational measures that Supplier shall follow concerning maintaining the Cybersecurity and security of Maxis Confidential Information and Personal Data in connection with the Agreement in place between the Parties.

1. Controlling Standards

1.1. Standards

Supplier shall comply and maintain globally applicable policies, standards, and procedures intended to protect data and other confidential materials within Maxis' environments, and, except as otherwise set forth herein, will comply with such policies in connection with the provision of the Services under this Agreement. Such policies shall govern and control Maxis' environment when accessing Maxis' systems or facilities.

2. Technical and Organizational Measures

Without limiting the generality of the foregoing, the Parties have implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Maxis Confidential Information & Personal Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction, as follows:

2.1. Organization of Information Security

2.1.1. Security Ownership

Supplier shall appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.

2.1.2. Security Roles and Responsibilities

Supplier's personnel with access to Maxis Confidential Information & Personal Data will be subject to confidentiality obligations.

2.1.3. Risk Management Program

Supplier shall have a risk management program to identify, assess and take appropriate actions concerning risks related to processing the Maxis Confidential Information & Personal Data in connection with the applicable agreement between the parties. Master Supplier shall participate and cooperate with Maxis annually or as requested in conducting the cybersecurity risks management program.

2.2. Asset Management

2.2.1. Asset Inventory

Supplier shall maintain an inventory of all media stored in the Maxis data.

Access to the inventories of such media is restricted to the authorized party in writing to have such access.

2.2.2. **Data Handling**

(i) Maxis Confidential Information & Personal Data shall be classified to allow access and appropriately restricted (e.g., through encryption). Data without classification shall be considered confidential by default and requires appropriate treatment unless granted exception by the Maxis Cybersecurity Governance, Risk, Compliance (GRC) team (“Maxis Cybersecurity").

(ii) Supplier shall limit printing of Maxis Confidential Information & Personal Data to what is minimally necessary to perform the Services under this Agreement and have procedures for disposing of printed materials and storage that contain Maxis Confidential Information & Personal Data.

(iii) Supplier is not allowed to store unencrypted Maxis Confidential Information & Personal Data on portable devices. However, if required, Supplier will need its personnel to obtain appropriate authorization before storing these data on mobile devices, remotely accessing or processing outside the authorized facilities.

2.3. **Human Resources Security**

2.3.1. **Security Training**

(i) Supplier shall inform its personnel about relevant security procedures and their respective roles. Supplier shall also inform its personnel of possible consequences of breaching the security rules and procedures.

(ii) Supplier shall only use anonymous data in training.

(iii) Supplier shall ensure that its personnel carefully chosen, including background verification checks, as well as adequately briefed and constantly trained on security issues.

2.4. **Physical and Environmental Security**

2.4.1. **Physical Access to Facilities**

Supplier shall only allow authorized individuals to access facilities where the information systems located that process Maxis Confidential Information & Personal Data.

2.4.2. **Physical Access to Components**

Supplier shall maintain records of the incoming and outgoing media containing

Maxis Confidential Information & Personal Data, including the kind of media, the authorized sender/recipients, date and time, the number of media, and the types of Maxis Confidential Information & Personal Data they contain.

2.4.3. **Protection from Disruptions**

Supplier shall use various industry standard (e.g., ISO 27001, CIS Sans 20, NIST Cyber-Security Framework, and/or RMiT as applicable) systems to protect against data loss due to power supply failure or line interference.

2.4.4. **Component Disposal**

Supplier shall use industry standard (e.g., ISO 27001, CIS Sans 20, NIST Cyber-Security Framework, and/or RMiT as applicable) processes to delete Maxis Confidential Information & Personal Data whenever it is no longer required by following Maxis' retention policy.

2.5. **Communications and Operations Management**

2.5.1. **Operational Policy**

Supplier shall maintain security documents describing their security measures and the relevant procedures and responsibilities of their personnel with access to Maxis Confidential Information & Personal Data.

2.5.2. **Mobile Device Management (MDM)**

Supplier shall maintain a mobile device policy that:

(i) Enforces device encryption;
(ii) Protects and limits the use of Maxis Confidential Information & Personal Data accessed or used on a mobile device; and
(iii) Prohibits enrolment of mobile devices that have been "jailbroken."

2.5.3. **Environments**

To the extent technically possible, limit the ability of personnel to access non-authorized environments from Supplier's systems.

2.5.4. **Data Recovery Procedures**

(i) Supplier shall have specific data recovery procedures in place designed to enable the recovery of Maxis Confidential Information & Personal Data maintained in systems.
(ii) Supplier shall review its data recovery procedures at least annually.
(iii) Supplier shall log data restoration efforts, including the person responsible, the description of the restored data, and where applicable, the person responsible and which data (if any) had to

be input manually in the data recovery process.

2.5.5. **Malicious Software**

Supplier shall have anti-malware controls to help avoid malicious software gaining unauthorized access to Maxis Confidential Information & Personal Data, including malicious software originating from public networks.

2.5.6. **Data Beyond Boundaries**

(i) Supplier shall encrypt Maxis Confidential Information & Personal Data that is transmitted over public networks.

(ii) Supplier shall implement or support multi-factor authentication (MFA) for remote access over a virtual private network (VPN).

(iii) Supplier shall protect Maxis Confidential Information & Personal Data in media leaving their facilities (e.g., through encryption or via Data Leakage Prevention (DLP) controls).

2.5.7. **Event Logging**

(i) Ensure individual accounts and is not shared for all network access to system components.

(ii) 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.

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

(iv) Synchronize all critical systems clocks and times to approved NTP (Network Time Protocol) servers.

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

(vi) Limit access to audit trail logs to those with a need-to-know basis.

(vii) 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.

(viii) Keep audit logs of systems components on the external segments secured on internally hosted central log servers.

(ix) Keep audit trail logs for at least 1 year; consider keeping 3 months online and the rest offline if the resource is constrained.

(x) All the critical logs (involving Maxis Confidential Information and

Personal Data) shall forward to SIEM (Security Information & Event Management) solution with log correlation capability.

(xi) SOC (Security Operation Centre) shall be available on a 24 hours and 7 days monitoring and capable of managing alerts and escalation for prompt action.

2.6. Access Control

2.6.1. Access Policy

Supplier shall maintain a record of security privileges of individuals having access to Maxis Confidential Information & Personal Data.

2.6.2. Access Authorization

(i) Supplier shall maintain and update a record of personnel authorized to access Maxis Confidential Information & Personal Data.

(ii) When responsible for access provisioning, Supplier will promptly provision authentication credentials.

(iii) Supplier shall deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed 3 months).

(iv) Supplier shall deactivate authentication credentials upon notification that access is no longer needed (e.g., employee termination, project reassignment, etc.) within two (2) business days.

(v) Supplier shall identify that personnel who may grant, alter or cancel authorized access to data and resources.

(vi) Supplier shall ensure that where more than one individual has access to systems containing Maxis Confidential Information & Personal Data, the individuals have unique identifiers/log-ins.

2.6.3. Least Privilege

(i) Technical support personnel shall only be permitted access to Maxis Confidential Information & Personal Data when required.

(ii) Supplier shall restrict access to Maxis Confidential Information & Personal Data to those who require such access to perform their job function.

(iii) Supplier shall limit access to Maxis Confidential Information & Personal Data to only that minimally necessary data to perform the Services under this Agreement.

2.6.4. Integrity and Confidentiality

Supplier shall instruct its personnel to disable administrative sessions when leaving premises or when computers are left unattended.

(i) 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) have been implemented to maintain Maxis' compliance with the Act.

(ii) Do not store authentication data in any readable format unless encrypted.

(iii) Keep Personal Data protected from casual access.

(iv) Use strong encryption to protect Personal Data and all Maxis Confidential Information stored at endpoints, servers, and databases.

(v) Implement controls to protect data leakage and monitor the endpoints/servers accessing/storing Maxis data. Controls shall include hardening of the endpoint/servers.

(vi) Have an appropriate procedure/standard for disposing Maxis Confidential Information.

(vii) Shall implement control to track the successful disposal of Maxis data and provide a report to track activity.

(viii) Change management process shall be in place for changes deployed to infrastructure, application, or database where data is stored, processed, or transmitted in Maxis.

(ix) Shall implement control to validate the adherence to change management policy and to identify unapproved changes.

(x) Manage access to Maxis Confidential Information centrally via a DBFW (Database Firewall) and reduce the number of repositories that hold such data.

(xi) Do not allow Maxis Confidential Information to be copied to removable media unencrypted by keys available to the service provider.

(xii) Protect the keys to encrypt Maxis Confidential Information against disclosure and misuse.

(xiii) Document and enforce all key-management processes and procedures and avoid single points of failure in the key management scheme.

(xiv) Keep Maxis Confidential Information separate from the access and authentication keys to access the data. And ensure both are securely protected.

(xv) Use strong cryptography and security protocols when providing and accessing Personal Data over open public networks.

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

2.6.5. **Authentication**

(i) Supplier shall use the industry standard (e.g., ISO 27001, CIS, Sans 20, NIST Cyber-Security Framework, and/or RMiT as applicable) practices to identify and authenticate users who attempt to access information systems.

(ii) Where authentication mechanisms are based on passwords, Supplier shall require that the passwords are renewed every 60 days.

(iii) Where authentication mechanisms are based on passwords, Supplier shall require setting the password to a minimum of at least eight (8) but preferably following Maxis standards of a minimum of fourteen (14) characters long. For remote and privileged access, multi-factor authentication (MFA) is mandatory for critical and financial systems.

(iv) Supplier shall ensure that de-activated or expired identifiers are not granted to other individuals.

(v) Supplier shall monitor repeated attempts to access to information systems using an invalid password.

(vi) Supplier shall maintain industry standard (e.g., ISO 27001, CIS, Sans 20, NIST Cyber-Security Framework, and/or RMiT as applicable) procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

(vii) Supplier shall use industry standard (e.g., ISO 27001, CIS, Sans 20, NIST Cyber-Security Framework, and/or RMiT as applicable) password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, as well as during storage.

2.6.6. **Network Design**

Supplier shall have controls to avoid individuals gaining unauthorized access to Maxis Confidential Information & Personal Data.

(i) Public accessibility of the system component should be prohibited from all vectors of access (eg., wired and wireless).

(ii) Data repositories containing Maxis Confidential Information (database, files, etc) should be placed in a securely protected internal network segment.

(iii) Access to such data should be limited to only authorized users under the control of the service provider and authorized to work on the contract.

(iv) The authorized user list shall be validated periodically to ensure the list is up-to-date.

(v) Remote access to such data shall be strictly controlled and

monitored to ensure network connectivity over encrypted secure channels and authentication performed to validate the authorized users.

2.7. **Patch Management**

2.7.1. Supplier shall have a patch management procedure that deploys security patches for systems used to process Maxis Confidential Information & Personal Data that includes:

(i) Defined time allowed to implement patches (not to exceed 90 days for all patches); and
(ii) Established a process to handle emergency patches in a shorter time frame.
(iii) System components shall have the latest vendor-supplied patches and software applications that have been secured using industry best practices.
(iv) Proper and documented code review process to remove vulnerabilities prior to release to the live environment.
(v) Documented change review process.
(vi) If the web development is complete, it should be based on secure coding guidelines (e.g., OWASP) to prevent common coding vulnerabilities.
(vii) For public-facing web applications, ensure ongoing application vulnerability assessment and use the web-application firewall (WAF) is mandatory.

2.7.2. Supplier shall agree to use no software or hardware end-of-life (EOL) in the scope of the Services under this Agreement without risk management process for such items.

2.8. **Workstations**

2.8.1. Supplier will implement controls for all workstations it provides that are used in connection with service delivery/receipt incorporating the following:

(i) Encrypted hard drive.
(ii) Software agent that manages overall compliance of workstation and reports a minimum monthly to a central server.
(iii) Patching process to ensure workstations are current on all required patches.
(iv) Ability to prevent certain types of software from being installed (e.g., peer-to-peer software).
(v) Antivirus and or end-point detection and response (EDR) with a

minimum weekly scan.

(vi) Firewall, advance persistent threats (APT) agent installed.

(vii) Data loss prevention (DLP) tool installed.

(viii) Web filtering to control access to unauthorized sites.

2.9. **Information Security Breach Management**

Supplier shall always operate the incident detection systems according to industry standards, allowing attack detection at least at the network perimeters. Supplier shall manage a process to detect and mitigate Information Security Incidents.

2.9.1. **Security Breach Response Process**

Supplier shall maintain a record of security breaches with a description of the breach, the time, the period, the consequences of the breach, the name of the reporter, to whom the breach was reported, and the process for recovering data.

2.9.2. **Service Monitoring**

Supplier's security personnel shall review logs as part of their security breach response process to propose remediation efforts if necessary.

2.9.3. **Data Breach Notification**

Suppliers are to inform Maxis in the event of an actual customer data breach within 24 hours of confirmation. Maxis has the right to perform audit or to appoint 3rd party auditor or accessor to Supplier's setup in the event of such a security incident or as and when the situation requires for such.

2.9.4. **Data Breach Insurance**

Suppliers shall provide sufficient insurance coverage as a protection in the event of a Maxis Confidential Information data breach incident due to lack of Supplier proactive measures to prevent such occurrence.

2.10. **Business Continuity Management**

2.10.1. Supplier shall maintain emergency and contingency plans for the facilities in which the Parties' information systems that process Maxis Confidential Information & Personal Data are located.

2.10.2. Supplier's redundant storage and procedures for recovering data will be designed to reconstruct Maxis Confidential Information & Personal Data in its original state from before the time it was lost or destroyed.

2.11. **Compliance Management**

2.11.1. Supplier shall comply with all Maxis policies and guidelines.

2.11.2. Supplier shall comply with all guidelines enforced by local regulators/regulations such as MCMC/BNM/MTFSB/RMIT where applicable.

2.12. Software Development

2.12.1. Illicit Code

Supplier represents and warrants that unless authorized in writing by Maxis, any software, algorithm, or code associated with software provided to Maxis shall, regardless of if pre-existing or developed for Maxis:

(i) contain no code and/or services, catering for unauthorized functionality, e.g., malware, backdoor, unauthorized remote access to or from Maxis' Network

(ii) not alter, damage, or erase any data or computer programs without the control of a person operating the computing equipment.

(iii) applies secure development lifecycle practices during design, development, and test cycles.

(iv) Products shall be subject to security design review, including threat considerations and data handling practices.

(v) The Services under this Agreement shall be subject to a secure release review prior to promotion to production.

2.12.2. Integration

Supplier shall ensure that all software, whether pre-existing or developed for Maxis, is fully integrated into any relevant Maxis security requirements, backup, and disaster recovery plan and procedure.

2.12.3. Security Testing

As part of the secure development lifecycle,

(i) Performs rigorous security testing, including, as technically feasible, static code analysis, source code peer reviews, dynamic and interactive security testing and security logic, or security "QA" testing.

(ii) Ensures that Internet-facing applications are subject to application security assessment, reviews, and testing to identify common security vulnerabilities as identified by industry-recognized organizations (e.g., OWASP Top 10 Vulnerabilities, CWE/SANS Top 25 vulnerabilities).

(iii) For all mobile applications running on mobile operating systems that collect, transmit, or display protected data, conduct an application security assessment review to identify and remediate industry-recognized vulnerabilities specific to mobile applications.

(iv) Does NOT use Personal Data or live data for testing.

(v) Makes all reasonable effort to identify and remediate software vulnerabilities prior to release.

2.12.4. **Annual Penetration Testing**

(i) Engages qualified, independent third-party penetration testers to perform an annual penetration test against its products and environments where protected data is hosted.

(ii) Requires sub-processors to perform similar penetration testing against their systems, environments and networks.

(iii) Ensures remediation of all findings in a commercially reasonable period of time.

2.12.5. **Product Vulnerability Management**

(i) Uses commercially reasonable efforts to identify software security vulnerabilities regularly.

(ii) Provides relevant updates, upgrades, and bug fixes for known software security vulnerabilities and software logic validation for any software provided or in which any Maxis Confidential Information is processed.

(iii) Ensures that all findings resulting from internal and external testing are evaluated according to industry standard practices, including CVSS score and assessment of impact, likelihood and severity, and are remediated following industry standard timelines.

2.12.6. **Open Source and Third-Party Software**

(i) Maintains an asset registry of all third-party software (TPS) and open-source software (OSS) incorporated into the Services under this Agreement.

(ii) Uses commercially reasonable efforts to ensure open-source and third-party software's secure development and security.

(iii) Uses commercially reasonable efforts to evaluate, track and remediate vulnerabilities of open-source software (OSS) and other third-party libraries that are incorporated into the Services under this Agreement.

3. Other applicable policies/guidelines

In addition to this Maxis Cybersecurity General Policy, Supplier shall respond and adhere to the other Maxis Cybersecurity guidelines such as the Vendor, Application, Mobile Applications & Cloud Security Compliance requirement where applicable.

End Of Document