

# **Cybersecurity General Policy**

**Document Version: v1.1**

**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.

In addition to this Maxis Cybersecurity General Policy, Supplier shall respond and adhere to the other Maxis Cybersecurity guidelines such as but not limited to Application, IoT, Mobile Applications & Cloud Security Compliance requirements where applicable.

All clauses mentioned in this annexure/appendix is part of the Maxis Cybersecurity requirements for the subjected contracts and said services. Agreed partner/vendor/service provider to ensure all requirements (which are applicable) are delivered without any commercial impact to Maxis.

## **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. **Inventory and Asset Management**

### 2.2.1. **Asset Inventory**

Supplier shall maintain an updated inventory of all services, components and data respective to Maxis. Access to the inventories of such media is restricted to the authorized party in writing to have such access.

## 2.3. **Secure Configuration Management**

### 2.3.1. **Establish and Maintain a Secure Configuration Process**

- (i) Shall establish and enforce strict configuration management practices to ensure all systems, devices, and applications are securely configured following industry standard benchmark, i.e.: CIS or NIST. Regularly review and update configurations to address any vulnerabilities identified through risk assessments.
- (ii) This includes such as but not limited to underlying servers, databases, and web servers, and also applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Also need to ensure that logical and physical separation of the Maxis related data and its services.
- (iii) Disable unnecessary and insecure services and protocols.
- (iv) Secure all administrative access with multifactor / Two factor authentication, tamper proof access logs and encrypted channel between user and endpoint end-to-end.
- (v) shall implement control to validate the adherence to change management policy and to identify unapproved changes, where data is stored, processed, or transmitted

## 2.4. **Log Management**

- (i) Implement automated untampered audit trails for all system components such as authentication logs, authorization logs, system logs, application logs, network logs, firewall logs, database logs, security logs and audit logs.
- (ii) Synchronize all critical systems clocks and times to approved NTP (Network Time Protocol) servers.
- (iii) Keep audit trail logs for at least 2 years; consider keeping 3 months online and the rest offline if the resource is constrained.
- (iv) Implement automated audit trails for all system and service components that includes system, application and databases logs and shall forward to SIEM (Security Information & Event Management) solution or centralized logs server with log correlation capability.
- (v) Review of all logs by dedicated team such as SOC (Security Operation Centre) and capable of managing alerts and escalation for prompt action.

## 2.5. **Vulnerability Management**

- 2.5.1. Supplier shall have a patch management procedure that deploys security patches for systems that includes:
- (i) Execute internal and external Vulnerability Assessment by qualified network security personnel at least quarterly or after any significant change in the network.
  - (ii) Defined time allowed to implement patches (not to exceed 90 days for all patches); and
  - (iii) Established a process to handle emergency patches in a shorter time frame.
  - (iv) System components shall have at least the latest minus one (N-1) updated vendor-supplied patches and software applications that have been secured using industry best practices.

## 2.6. **Identity and Access Management**

### 2.6.1. **Access Policy**

- (i) Supplier shall maintain a record of security privileges of individuals having access to Maxis data.
- (ii) Have proper ID management process that is based on best practices and industry standards to ensure access is granted to valid individuals and passcodes are changed regularly.

### 2.6.2. **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) Supplier shall ensure that de-activated or expired identifiers are not granted to other individuals.
- (iii) When password-based authentication is in use, the Supplier must apply industry standard. For remote access, particularly when dealing with critical, Personally Identifiable Information (PII) and personal data, the deployment of multi-factor authentication (MFA) is mandatory. This requirement is also extended to business critical systems and systems managing financial transactions.
- (iv) Supplier shall not allow dictionary password and monitor for repeated attempts to access to information systems using an invalid password.
- (v) 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.

- (vi) Regularly review and update the accounts and roles.
- (vii) Restrict access to systems by vendors for the period of activity only and based on documented change management request.

### 2.6.3. Access Authorization

- (i) Supplier shall maintain and update a record of personnel authorized to access Maxis data.
- (ii) Suppliers are strongly recommended to implement industry-standard authentication mechanisms such as but not limited to Single Sign-On (SSO), Lightweight Directory Access Protocol (LDAP), and Active Directory (AD) Integration
- (iii) All suppliers are required to register the system with Maxis IDM. This is particularly crucial for systems containing Personally Identifiable Information (PII), personal data and critical systems.
- (iv) Ensure that all suppliers accessing our systems and data, especially those containing Personally Identifiable Information (PII) and critical systems, are required to use Maxis ID. This is to uphold strict access control principles and maintain unique user identification.
- (v) When responsible for access provisioning, Supplier will promptly provision authentication credentials.
- (vi) 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) or upon notification that access is no longer needed (e.g., employee termination, project reassignment, etc.), within two (2) business days.

### 2.6.4. Least Privilege

- (i) Technical support personnel shall only be permitted access to Maxis data when required.
- (ii) Supplier shall limit access to Maxis data to only that minimally necessary data to perform the Services under this Agreement.

## 2.7. Data Protection

### 2.7.1. Data Handling

- (i) Maxis 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 team.
- (ii) Supplier shall limit printing of Maxis 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 data.

- (iii) Supplier is not allowed to store unencrypted Maxis 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.
- (iv) The data management policies and procedures include a tamper audit or software integrity function for unauthorized access to Maxis data
- (v) Ensure all systems that process, store and transmit Credit Card information is compliant to the PCI/DSS controls. Non-Maxis agents must submit a copy of the recent SAQ as proof of compliance.
- (vi) Data flow diagrams are required to be developed and/or produced to Maxis for tracking of data movement

#### 2.7.2. Integrity and Confidentiality

- (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 based on best practices and industry standards for disposing Maxis Confidential Information.
- (vii) Manage access to Maxis Confidential Information centrally via a DBFW (Database Firewall) and reduce the number of repositories that hold such data.
- (viii) Do not allow Maxis Confidential Information to be copied to removable media unencrypted by keys available to the service provider.
- (ix) Implement a secure key-management processes and procedures based on best practices and industry standards and avoid single points of failure in the key management scheme.
- (x) Keep Maxis Confidential Information separate from the access and authentication keys to access the data. Ensure both are securely protected.
- (xi) Use strong cryptography and security protocols when providing and accessing Personal Data over open public networks.

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

### 2.7.3. **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.”

### 2.7.4. **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.

### 2.7.5. **Physical Security**

- (i) Supplier shall only allow authorized individuals to access facilities where the information systems located that process Maxis Confidential Information & Personal Data.
- (ii) Use appropriate facility entry controls to limit and monitor physical access to systems holding or carrying Maxis Information.
- (iii) 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.
- (iv) 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.
- (v) 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.
- (vi) Store backup media in a secure location, preferably an secure off-site facility and review the security of the site and the media transfer

process at least annually.

- (vii) Physically secure all paper and electronic media that contain PII data (eg: Bills, Statements, Customer lists etc.)
- (viii) 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.
- (ix) Maintain strict control over the storage and accessibility of the PII Media. Ensure inventory logs of all media is maintained and checked regularly.

#### 2.7.6. **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.

#### 2.7.7. **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.

### 2.8. **Application Development**

#### 2.8.1. **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) Products shall be subject to security design and code review, including threat considerations and data handling practices.
- (ii) Ensure it contains no code and/or services catering for unauthorized functionality, e.g., malware, backdoor, unauthorized remote access to or from Maxis' Network
- (iii) not alter, damage, or erase any data or computer programs without the control of a person operating the computing equipment.
- (iv) applies secure development lifecycle practices during design, development, and test cycles.
- (v) The Services under this Agreement shall be subject to a secure release review prior to promotion to production.

#### 2.8.2. **Application Security**

If the web development is done, it should be based on secure coding guidelines (e.g., OWASP) to prevent common coding vulnerabilities.

### 2.8.3. **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.

The use of API must adhere to Maxis standards and comply to API security requirement, addresses among others the vulnerabilities such as broken authentication and authorization, lack of rate limiting, and code injection.

### 2.8.4. **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) 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.
- (iii) Does NOT use Personal Data or live data for testing.
- (iv) Makes all reasonable effort to identify and remediate software vulnerabilities prior to release.
- (v) Implement application security best practices including but not limited to testing of security patches prior to release, input validation to prevent or safely recover from malicious content and secure communication between application components.

### 2.8.5. **Annual Penetration Testing**

- (i) Engages qualified, independent third-party penetration testers to perform penetration test at least once a year or after significant change 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.

### 2.8.6. **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.

#### 2.8.7. **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 evaluate, track and remediate vulnerabilities of open-source software (OSS) and other third-party libraries that are incorporated into the Services under this Agreement.

### 2.9. **Incident Management**

Supplier shall always operate the incident detection systems according to industry standards. Supplier shall manage a process to detect and mitigate Information Security Incidents.

#### 2.9.1. **Incident response plan**

- (i) Implement an incident response plan with well-defined procedures and be prepared to respond immediately to a system breach.
- (ii) Ensure the plan covers: Roles, responsibilities, communication, and contact strategies in the event of a compromise.
- (iii) Has data backup procedure, business recovery and continuity procedures.
- (iv) Has coverage and response for all critical system components.
- (v) Validate and test of the Incident Response Plan at least annually.
- (vi) Ensure availability of key personnel on the Incident Response Team on a 24x7 window.
- (vii) Ensure there is appropriate personnel training for security breach response responsibilities.
- (viii) Logs from intrusion detection, intrusion prevention and file-integrity monitoring systems are readily available for incident analysis.
- (ix) Have a plan to review and evolve the incident response plan according to the lessons learned and to incorporate industry changes.

#### 2.9.2. **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. Supplier shall also enable processes to provide timely forensic investigation in the event of compromise of any system relating to Maxis.

#### 2.9.3. **Service Monitoring**

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

#### 2.9.4. **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 3<sup>rd</sup> 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.

#### 2.9.5. **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. **Third Party Management**

2.10.1. Supplier shall comply with all Maxis policies and guidelines. Supplier shall also comply with all guidelines enforced by local regulators/regulations such as MCMC/BNM/MTFSB/RMIT where applicable.

2.10.2. The Supplier shall, at no cost to Maxis, co-operate fully with Maxis in participating in, and responding to, any Maxis' third party risks management evaluation programme and/or questionnaire, including in making relevant attestations and, if any security gaps are identified, complying with any reasonable directions from Maxis with respect to remedying such security gaps and fulfilling any ancillary measures.

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

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

2.10.5. Ensure any subcontractors of the Service Provider carry the same responsibility of compliance to the policies. Maintain a written agreement that includes acknowledgement that the subcontractors are responsible for the security of PII held by them.

#### 2.10.6. **Business Continuity Management**

- (i) 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.
- (ii) 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.

#### 2.10.7. **Information Security Policies and Acceptable Use**

- (i) 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.
- (ii) Develop and enforce operational security procedures which are consistent with the requirements of the policy. (eg: identity and access management, log management, etc.)
- (iii) 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.
- (iv) Prohibit the copy or storage of PII on client-side devices, removable and fixed media.
- (v) 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.
- (vi) Screen employees with access to PII data and systems.

#### 2.11. **Security Awareness and Training**

- (i) Implement continuous and formal security awareness program and make all users aware of the importance of keeping confidential and personal data private and secure.
- (ii) Supplier shall only use anonymous data in training.

#### 2.12. **Security Technology**

2.12.1. Supplier will implement controls for all endpoints 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 (WAF) to control access to unauthorized sites.

#### 2.12.2. **Network Design**

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

- (i) Ensure IT network security technologies are implemented and effectively managed. The network traffic and access control rules applied to such devices should be reviewed regularly.
- (ii) Network and Systems design documents detailing the storage, access, transport, protection of Maxis related data should be kept current to enable audits.
- (iii) Ensure timely detection, investigation, root cause analysis and response to incidents. Ensure all the security system engines, rules, signatures, and others are updated regularly.
- (iv) Public accessibility of the system component should be prohibited from all vectors of access (eg., wired and wireless).
- (v) Data repositories containing Maxis Confidential Information (database, files, etc) should be placed in a secure network segment.
- (vi) Access to the IT network security devices and Maxis data should be limited to authorized users with legitimate need and logged.
- (vii) The authorized user list shall be validated periodically to ensure the list is up-to-date.
- (viii) 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.

#### 2.12.3. **Malicious Software**

- (i) Supplier shall have anti-malware that are always kept updated and active.
- (ii) All computing equipment connected to the Maxis Enterprise Network shall have the mandatory Maxis APT and Security software installed and running while connected to the MEN (where applicable).
- (iii) All computing equipment requiring connectivity to Maxis Enterprise Network (MEN) must first be approved and registered with Maxis CMDB before access to the network is authorised (where applicable).

#### 2.12.4. **Data Beyond Boundaries**

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

- 2.12.5. Supplier shall agree not to use software or hardware near or already end-of-life (EOL) in the scope of the Services under this Agreement.

**END OF DOCUMENT**