Smarttech

Supplier Security Requirements Policy

1. Security Policy

a. The Supplier must have an Information Security policy in place which meets applicable industry standards and which is subject to review by Smarttech under a Non-Disclosure Agreement (NDA). This policy must comply with the laws, regulations, operational procedures and systems security configurations implemented. This policy must be reviewed on a regular basis by the Supplier.

2. Organising Information Security

a. Information Security Roles and responsibilities must be clearly defined and implemented.

b. Non-disclosure agreements must be signed by Suppliers prior to being granted access to Smarttech information.

c. All interactions with Smarttech or involving Smarttech information must be secured and approved by Smarttech.

d. All subcontracted activities involving Smarttech information must be approved and secured by the Supplier.

3. Asset Management

a. Smarttech will generally inform the Supplier of the classification of Smarttech data provided to Supplier. In the event Supplier is not certain of the classification of any item of Smarttech data, Supplier will seek clarification from its Smarttech Business Contact.

b. An appropriate set of procedures for information labeling and handling must be developed and implemented.

c. Personal use of Smarttech equipment and information is not allowed.

4. Human Resources Security

a. Security roles and responsibilities of employees, contractors and third party users must be defined and documented to incorporate Smarttech's data protection control requirements including background checks to the extent permitted by applicable law.

b. All employees, contractors, and third-party users must be notified of the consequences for not following your security policy in handling Smarttech information classified as confidential and above.

c. All assets used to manage or store Smarttech information must be protected against unauthorised access, disclosure, modification, destruction or interference.

d. All employees, contractors and third party users must be provided with education and training in privacy and security procedures and the correct information processing requirements.

5. Physical and Environmental Security

a. Information processing facilities where Smarttech confidential and above information is stored must be secured and protected from unauthorised access, damage, and interference.

b. Physical security must be appropriate to the classification of the assets and information being managed and could include, card key access, security cameras, and solid wall construction for all exterior walls. Additional controls may be needed for Restricted Secret and Top Secret information or assets.

c. The number of entrances to the information processing facilities in which Smarttech's information is stored must be limited. Every entrance into these areas requires screening. (e.g. Security guard, badge reader, electronic lock, a monitored closed caption television (CCTV)). Logs must be recorded and maintained.

d. Physical access must be restricted to those with a business need. Access lists must be reviewed and updated at least once per quarter.

e. Process, training and policies must be in place to determine visitor access, after-hours access, and prevent tailgating into controlled areas.

f. Emergency exits in controlled areas must sound an alarm when opened and include automatic closure. Any alarms must trigger an emergency response.

6. Communications and Operations Management

a. Operating procedures must be documented and managed by a change control process.

b. Supplier must have a separation of duties process to prevent one individual from controlling all key aspects of a critical transaction or business process.

c. Suppliers are responsible for data protection, privacy compliance, and security control validation/ certification of their sub-contractors.

d. Development, test, and operational environments must be separated to reduce the risks of unauthorised access or changes to the operational system.

e. Acceptance criteria for new information systems, upgrades, and new versions must be established and suitable tests of the system(s) carried out during development and prior to acceptance.

f. Supplier must support standards and procedures that ensure confidentiality, integrity and availability of information and services with continuous oversight on new threats and vulnerabilities by a documented risk assessment process driving risk mitigation implementation on a timely basis.

g. System administrators must have adequate training and experience to securely administer the infrastructure within their responsibility.

h. Suppliers must maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a third party. The Supplier must ensure they retain visibility into security activities such as change management, identification of vulnerabilities, and information security incident reporting/response by the third party.

i. Audit logs recording user activities, exceptions, and information security events must be maintained for an agreed period to assist in future investigations and access control monitoring.

7. Access Control

a. The access control policy must clearly state the rules and rights for each user or group of users including applications and information sharing and must include a process for granting and removing access to all information systems and services. A record of all privileges allocated must be maintained.

b. Each user must have a unique user ID and practice the use of strong passwords which are at least eight characters long and composed of letters, numbers and special characters where feasible. If other biometric controls are used in lieu of passwords or in addition to they must be documented and disclosed in compliance to Smarttech Information Security policy.

i. The use of group IDs is only permitted where necessary and must be approved and documented.

ii. Group and individual accounts should not have administrative access unless absolutely necessary for successful service delivery.

c. Access to applications and data must be reviewed at regular intervals to prevent unauthenticated users from accessing data or using vital system resources and revoked when no longer required.

d. Applications, ports, services, and similar access points installed on a computer or network facility, which are not specifically required for business functionality, must be disabled or removed.

e. Network segments connected to the Internet must be protected by a firewall which is configured to secure all devices behind it.

f. User connection capability must be documented with regard to messaging, electronic mail, file transfer, interactive access, and application access.

g. All extranet connectivity into Smarttech is strictly prohibited by non-Smarttech personnel.

h. All restricted and above data exchanged with Smarttech for mission or business critical functions and Business to Business (B2B), require secure exchange of communication.

i. All production servers must be located in a secure, access controlled location.

j. Supplier is responsible for implementing the secure protocols at their sites and managing the protocols by a change control process.

k. Firewall must be configured properly to address all known security concerns.

l. Infrastructure diagrams, documentation and configurations must be up to date, controlled and available to assist in issue resolution.

m. Systems must have the ability to detect a potential hostile attack. Examples include but are not limited to Network Intrusion Detection (NID) or Host Intrusion Detection (HID) / Prevention. All systems must be updated to current release and actively monitored.

n. Network segments where Smarttech data resides should be isolated from non-Smarttech data, logically or physically unless approved by Smarttech and the access to Smarttech data is strictly prohibited.

o. Access controlled applications must implement a lock out for a minimum of 30 minutes after 5 consecutive failed login attempts and 1 hour after a total of 10 failed login attempts.

p. Access controlled applications must never be reinitialised by using the back button.

q. Applications containing Confidential data and above must require a password change every 90 days or less.

8. Information Security Incident Management

a. A documented information security event management process for Physical and Data security must be implemented which includes incident response, escalation, and remediation.

i. Information security events and incidents include:

1. loss of service, equipment or facilities,

2. system malfunctions or overloads,

3. human errors,

4. non-compliances with policies or guidelines,

5. breaches of physical security arrangements,

6. uncontrolled system changes,

7. malfunctions of software or hardware,

8. access violations,

9. legal and regulatory violations

10. Malware

11. Suspicious and benign behaviors that may lead to an event.

b. Both companies will act in good faith to preserve the other company's evidence and reasonably cooperate with each other and the authorities if needed during an investigation.

f. Each company will be responsible for investigating incidents and taking actions to protect their own interests.

9. Business Continuity (BC) Management

a. Disaster Recovery (DR) plan must be documented and tested annually.

b. All system media has a regularly scheduled backup and restore capability implemented and tested.

c. Disaster recovery resources and / or subcontractors must be documented and made available to Smarttech upon request.

10. Compliance

a. Supplier must have a process to document non-compliance of any legal, regulatory or privacy instance or control that does not meet local laws and regulations and must identify and quantify the risks and mitigation plans and document the business decision for alternate controls or risk acceptance. The mitigation plan and business decision must be signed off by the Chief Information Officer (CIO) or an authorised individual who can accept responsibility and accountability on behalf of the Supplier.

b. Supplier must know and be compliant with all regulatory and local governing laws that are applicable

c. Remote Control/Access: These types of technologies must not be used. If these types of technologies are part of the project scope, you must contact the Smarttech business owner to obtain a Privacy assessment for the project.