Suntex International

Data Privacy and Security Policy

Policy Area	IT Policy Library
Approved Date	August 26, 2019
Approved By	Policy Committee
Effective Date	August 27, 2019
Current Version	1.0

I. Overview

Security systems and processes help protect Suntex International's Information Resources and ensure system confidentiality, availability, and integrity.

II. Purpose

This policy identifies security safeguards and controls that help Suntex International manage risks, meet business requirements, and comply with regulations. In addition, it establishes general privacy requirements for information automatically generated by computer systems and network devices, including systems and devices involved in the transmission and storage of voice data. The policy further delimits the conditions under which network data may be disclosed.

III. Scope

This policy applies to all Staff that use Suntex International's Information Resources.

IV. Policy

A. Security Overview

The CSO shall ensure security safeguards and controls are implemented and maintained to achieve the desired security objectives:

- Availability. Information Resources are available and operational when and where they are needed.
- Confidentiality. Only authorized individuals have access to information.
- Integrity. The value and state of information is protected from unauthorized modification.

The Chief Security Officer (CSO) is responsible for implementing and maintaining:

- Administrative safeguards
- Technical safeguards
- Physical safeguards

B. Administrative Safeguards

Administrative safeguards provide top down security direction and guidance. Administrative safeguards are written documents grouped into major categories.

Confidentiality. The requirements for non-disclosure (e.g. confidentiality agreements) reflect Suntex International's need to protect data and operational details. Such requirements shall be identified, documented, and reviewed at planned intervals.

Data Owners. The roles and responsibilities of the Data Owners and department head custodians shall be formally defined. Equipment and data shall not be taken off-premise without prior approval from the Data Owner.

Independent Reviews (Audits). Where possible, the CSO shall use Certified Information Systems Auditors, or equivalent, to audit the security controls of Suntex International's Information Systems. Security audits shall be performed on an annual basis or more frequently if major changes occur to Information Resources. Refer to Company Audit Policy for more information.

Insurance. Property and cyber insurance can be used to transfer risk. The CSO shall work with the Risk Management Officer (RMO) to determine required coverages.

Job descriptions. Executive Management shall ensure job descriptions exist for all employees. Each job description shall identify the position title, purpose of the position, specific duties and responsibilities, reporting relationships, position requirements, and related information.

Plans. Written plans shall be developed and maintained to ensure safeguards controls business risks. Important plans include:

- Business Continuity Plan. The purpose of this plan is to protect Information Resources and our ability to continue business operations in the event of a disaster or component failure.
- Incident Response Plan. The Incident Response Plan helps protect the integrity, availability and confidentiality of information, prevent loss of service, and comply with legal requirements. Staff shall act in a timely and coordinated manner prevent and to respond to breaches of security to help prevent damage. However, if action is taken, it should not jeopardize the security of systems. Refer to the Incident Response Policy and Incident Response Plan for more information.
- Security Awareness and Training Plan. The Security Awareness and Training Plan help ensure security awareness and training controls protect Information Resources and ensure information availability, confidentiality, and integrity.
- System Security Plan. The System Security Plan (Plan) is to provide an overview of the security requirements of DSGA's Information Resources. This Plan also describes the controls necessary to ensure information availability, confidentiality, and integrity.

Policies. The Chief Security Officer (CSO) shall be responsible for implementing and maintaining security policies, procedures, plans, forms, and related documents.

- Account management. Policies and procedures shall manage the process of creating, monitoring, controlling, and removing of accounts. Refer to the Account Management Policy for more information.
- Classification. All users, hosts, and data shall be classified per the Data Classification Policy.

- Logging. Host security log files shall be configured and reviewed for anomalies. Logs must be of sufficient size to provide useful information in case of a security event (at least 90 days of logs).
- Updates. On an annual basis, or more frequently if needed, policies, procedures, plans, forms, etc. shall be reviewed and updated by the CSO to address organizational changes and ensure continual improvements in the information security management system. Any new documents, or updates to existing documents, shall be approved by Executive Management prior to being distributed to Suntex International Staff.
- Use. Users are a first line of defense and shall follow safe computing practices as outlined in the Acceptable Use Policy.

Risk Assessment. Risk assessments help identify business processes that are of high priority and importance to the organization. They also ensure the proper controls are implemented to reduce risks to acceptable levels. The risk assessment and risk analysis shall identify threats including the likelihood of the event and impact on the organization. Preventive, detective, and corrective controls shall be identified and implemented as needed.

Staffing. All departments shall have appropriately supervised staff sufficient to maintain information security. The staffing level should be appropriate to the environment, i.e. the amount and type of information for which they are responsible and the level of risk.

C. Technical Safeguards

Technical safeguards protect and control access to Information Resources.

Access Controls.

- Authentication data. Information Systems shall protect authentication data as it is entered including suppressing the display of the password as it is entered, and orienting keyboards away from view.
- Inactive IDs. User IDs that are inactive on the system for a period of three months shall be deleted.
- Inactivity – users shall be automatically logged off after 15 minutes of inactivity.
- Logon attempts – users shall be locked out after five consecutive failed logon attempts within a 24 hour period. The lockout duration shall be at least 30 minutes or until a system administrator enables the user ID.
- Passwords – passwords are a key component to system security and restricting access to systems.
- Screen savers - protected screen savers are required and shall be activated after 15 minutes of inactivity.
- User interfaces. Access to specific functions shall be restricted, never allowing users to request information, functions, or other resources for which they do not have access. Three major user interfaces include menus, database views, and physically constrained user interface (e.g. access card, key, etc.).

Clear desk. Staff shall ensure sensitive information remains secure by clearing their desks when they will be away from their office, positioning monitors to prohibit unauthorized viewing, etc.

Communications

- Border routers. Border routers may be used to filter traffic and protect against spoofed IP addresses.
- Firewalls. Firewalls shall protect the network and limit traffic to only approved activities. For more information see the Firewall Policy.
- Transaction. Transaction based access criteria can be used. For example, access to a particular account could be granted only for the duration of a transaction. When completed, the access authorization is terminated.

Data handling. Controls and safeguards shall be implemented to protect the integrity of electronic data that is stored, accessed, or transmitted. Refer to the Data Integrity Policy.

Lifecycle. The CSO shall ensure that information is protected during its entire lifecycle. Information shall only be retained for the duration of its useful life. The disposal of hardware, software, and information requires special consideration. Refer to the Data Retention Policy, Disposal Policy, Encryption Policy, and Removable Media Policy for more information. Suntex International's IT Department shall be responsible for developing, maintaining, and managing a Software Development Life Cycle (SDLC). Please refer to the Software Development Policy for more information.

Monitoring. Monitoring systems and audit trails shall be used to prevent unauthorized personnel from accessing Suntex International's Information Resources. Audit trails can also be used as an incident detection and response mechanism. Refer to the Audit Trails Policy and Logging Policy for more information.

Network management

- Backups. Backups shall be protected against accidental or deliberate destruction of data. Refer to the Backup Policy for more information.
- Configurations. Information Systems shall be configured according to applicable security guidelines and standards. As received from the vendor, computers and other devices may not be configured for security and may require initial as well as ongoing review of the configuration and security of the operating system and software. Staff must protect data by implementing and maintaining authorized hardware and software configurations. Network administrators shall implement and maintain documented security configuration standards for all authorized operating systems and software. Network administrators shall use a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur. For more information see the Network Configuration Policy, Server Hardening Policy, and Workstation Security Policy for more information.
- Management. Networks shall be managed and controlled to protect information in systems and applications. The network and security architecture, including data flow diagrams, shall be documented and aligned with industry best practice standards. For more information see the Configuration Management Policy and Network Security Policy.
- Service levels. Service levels and management requirements of all network and security services shall be identified, documented, and agreed upon by Data Owners and IT Staff. Service levels and requirements shall be included in appropriate third-party service level agreements (SLA). Metric based performance shall be reported according to agreed upon schedules.

- Segments. Network equipment (e.g. routers, servers, workstations) shall be classified and placed in a network segment appropriate to its level of classification. Access to these segments must be controlled in an appropriate manner. Whenever data travels over a network segmentation of a lower security classification then the data shall be protected in a manner appropriate to its classification level. Groups of information services, users, and information systems shall be segregated on networks. IT security Staff shall consider the use of ACLs and Virtual Local Area Networks (VLANs) to segment systems and enhance security. ACLs are a register of users (e.g. groups, machines, processes) permitted to use a particular system resource and the types of access they have been permitted.

Security protection

- Change. Every change to an Information Resource (e.g. operating system, computing hardware, networks, applications, data centers) is subject to the Change Management Policy and must follow appropriate change management procedures. Where appropriate, change detection systems (e.g. file-integrity monitoring tools) shall alert personnel to unauthorized modification of critical system files, configuration files, or content files. Such systems shall be configured to perform critical file comparisons at least weekly. Note: For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by IT security Staff. IT security Staff shall implement a process to respond to any alerts generated by the change detection solution.
- Encryption. Systems and media may contain Sensitive Information. Refer to the Encryption Policy for more information on restricting access to Sensitive Information.
- Forensic investigations. Processes shall provide for timely forensic investigation in the event of a incident.
- Intrusions. Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) shall be used to detect and/or prevent intrusions into the network. All IPS engines, baselines, and signatures shall be kept up-to-date.
- Malware. Security systems shall be in place to protect systems against computer malicious software. Refer to the Anti-Malware Policy for more information.
- Software. Installing unapproved software can cause damage, invalidate warranties, or have other negative consequences. Refer to the Approved Application Policy and the Software Licensing Policy for more information.
- Patching. Information Systems shall be patched and updated in a timely manner. See the Patch Management Policy for more information.
- Monitoring. Systems shall monitor all traffic at the perimeter of environments containing Sensitive Information as well as at critical points in the environment containing Sensitive Information. Such monitoring systems shall issue alerts to personnel of any suspected compromises.
- Shared environments. For multiple entity shared environments the CSO shall ensure mechanisms protect each entity's environment and data. Each entity only runs processes that have access to that entity's data environment. Each entity's access and privileges shall be restricted to its own data environment. Logging and audit trails shall be enabled and unique to each entity's environment.

Third party access. Prior to granting individuals physical or logical access to information resources, agreements with staff, third party users, and customers shall be in place and include responsibility for information security. Refer to the Third Party Service Providers Policy for more information.

D. Physical Safeguards

Physical safeguards include mechanisms that protect physical assets (e.g. access cards, data center server racks, locking cabinets, cameras, uninterruptable power, guards, etc.). Physical safeguards shall ensure only authorized Staff have access to Information Systems, equipment, and operating environments. For more information see:

- Facility Security Plan
- Physical Access Policy
- Physical Security Policy

Media. Media shall be handled according to the Removable Media Policy.

Operations.

- Acquisitions. Only hardware or software acquired through Suntex International's approved policies and procedures may be installed. Refer to the Acquisition and Procurement Policy.
- Diagnostic ports. Physical and logical access to diagnostic and configuration ports shall be controlled. Refer to the Network Configuration Policy and Physical Access Policy.
- Location. Access to Information Resources may be based upon physical or logical location. Similarly, users can be restricted based upon network addresses (e.g., internal users may be permitted greater access than those from outside the organization).
- Time. Time and day restrictions may be used to limit access to data (e.g. access to personnel files may only be allowed during normal working hours).

Physical security protection

- Access. Access to Information Resources shall be controlled and restricted as much as possible. Devices not in use for extended periods shall be turned off. Workstations and servers shall have appropriate and secure physical controls. Refer to the Physical Security Policy for more information.
- Display. Staff shall be made be aware of the visibility of data on their computer or handheld device display screens. Staff shall position equipment or furniture to eliminate over-the-shoulder viewing.
- Environmental conditions. Staff shall minimize costly disruptions caused by data or hardware loss. Refer to the Physical Security Policy to reduce risks related to environmental threats and hazards and opportunities for unauthorized access.

E. Network Data

In the course of normal network operations, computer systems, voice systems, access control systems, and network devices may automatically generate and track logging data, source and destination internet protocol (IP) addresses, session times, port numbers, file sizes, etc. (Network Data).

It is the general policy of Suntex International to treat Network Data as private. This information may be obtained, stored, and reported for legitimate business purposes but shall not be exposed to unauthorized individuals except as specifically listed below.

F. Exceptions

Network Data may be exposed or disclosed under the circumstances listed below.

To maintain the integrity and availability of network operations. Network Data may intentionally or inadvertently expose Information Resources stored on networked machines or transmitted through the network in the following situations:

- Network performance monitoring or troubleshooting.
- Moving data through the network via automated store-and-forward systems.
- Copying, archiving, or otherwise preserving portions of messages transmitted over the network in the course of routine network maintenance activities.

In the event that messages or data files within the network indicate the presence of activities that violate internal policies or law.

In the event of recognized network security threats. Suntex International reserves the right to investigate and remediate possible network security threats, including by means of capture, logging, and examination of files, communications, and other traffic and transmissions over or on the network.

In response to a court order.

In the event of a legitimate health or safety emergency.

In pursuit of reasonable business interests, such as fulfillment of partnership agreements.

G. Requests for Network Data

All requests to retrieve and share Network Data must be submitted to the IT Department and must be approved by the appropriate Department head. Such requests shall include:

- Name and role of the requestor.
- Reason for the request, in accordance with the principles set forth in this policy.
- Intended use of the requested data.

Any network data intentionally shared with third parties must be sanitized to preserve the anonymity of network users.

V. Enforcement

Any Staff found to have violated this policy may be subject to disciplinary action, up to and including termination.

VI. Distribution

This policy is to be distributed to all Suntex International Staff that use Suntex International's Information Resources.

Policy History

Version	Date	Description	Approved By
1.0	1/1/2019	Initial policy release	NR
	5/5/2020	Review	NR
	1/5/2022	Review	NR
	2/14/2023	Review	NR

References:
COBIT EDM03.02, EDM03.07, APO13.07, APO14.10, DSS05.02, DSS05.07, MEA02.11
GDPR Article 25, 30, 32
HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)
ISO 27001:2013 A.5, A.7.2.2, A8.1.3, A.8.2.1, A.9-14, A.16-18
NIST SP 800-37 3.4, 3.7
NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29
NIST Cybersecurity Framework ID.AM-5, ID.GV-1, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2
PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8, PCI Software Security Framework