**Policies**

**and Procedures**

**Summary**

# Table of contents

Physical Security Policies and Procedures

Closed-Circuit Television (CCTV) Policies and Procedures

Tangent Enterprise Risk Management and Integrated Framework

Third Party Management Policies and Procedures

Business Continuity Management Policies and Procedures

Incident Management Policies and Procedures

Change Management Policies and Procedures

Tangent Health and Safety Manual (THSM)

Quality Manual

Anti-Virus Management Policies and Procedures

Access Control Policies and Procedures

Audit Logging and Monitoring Policies and Procedures

Card Data Encryption Policies and Procedures

Cardholder Data Retention and Disposal Policies and Procedures

Configuration Management Policies and Procedures

Daily Operational Security Policies and Procedures

Data Back-up Policies and Procedures

Key Management Policies and Procedures

Payment Card Industry Data Security Standard PCI DSS Charter

Remote Access Policies and Procedures

Secure Software Development Life Cycle Policies and Standards

Software Development Policies and Procedures

Technology Usage Policies and Standards

Vulnerability Management Policies and Procedures

# Physical Security Policies and Procedures

## Camera/Monitoring/Surveillance/Recording Archival (Page 7)

* Cameras are to be strategically placed throughout the facility as deemed necessary and capable of capturing and recording all activity. Additionally, this requires the use of monitoring devices whereby authorized personnel can view all activity in real-time, while viewing, recording is to be in place that allows for capturing any activity. Moreover, archival measure are to be in place (**minimum of 90 days)** for retention of data caught on camera.

## Facility Access (Page 9)

* For individuals who have been granted an actual access control badge—thus allowing to bypass many of the provisioning steps in place for visitors, contractors, and other third party individuals—the software utility that allows access is to be reviewed on a regular basis. The regular review is to ensure that all terminated users do not have access and access for current users is commensurate with their roles and responsibilities.
* The entire identification, provisioning, and de-provisioning process is to be recorded and archived for purposes of producing audit records as needed, such as for access control breaches, daily operational review activities, and for regulatory compliance requirements.

## Media Management Controls (Page 11)

* Logs shall be established to properly maintain the inventories of all media and its movement. Their inventory logs should be reviewed at least annually.

## Confidential Area Access

* Video cameras and/or access control mechanisms shall monitor individual physical access to sensitive areas and this data shall be stored for at least three months, unless otherwise restricted by rule, regulation, statute, or law.

## Visitors

* Visitor Access Register is maintained for 3 months.
* Expected visitors should submit softcopy[ies] of the Company ID to the business contact 3 days before the scheduled visit.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# Closed-Circuit Television (CCTV) Policies and Procedures

## Policy Statements (Page 6)

* CCTV system will be operated 24 hours a day, 365 days.
* Video cameras shall monitor individual access to sensitive areas and this data shall be stored for at least 90 days (3 months) unless otherwise restricted by rule, regulation, statute, or law.

## Digital Recording (Page 10)

1. **Rules for Retention of Data**

* The CC-IARCO shall check daily to ensure the system is operational.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the

# Information Security Policies and Procedures

## Policy Statements (Page 6)

* Conduct regular or at least annual POS terminal inspections to all merchants to ensure the devices are not tampered.

## To the Information Technology Team (Page 8)

* Ensure compliance with this policy alongside CCIARCO and is reviewed regularly.

## System and Application Administrators (Page 9)

* Retain audit logs for at least one year.

## To the Human Capital Management Team (Page 10)

Responsible for tracking employee participation in the security awareness program:

* Facilitating participation upon hire at least annually.

## Compliance with Security Policies and Standards, and Technical Compliance (Page 11)

* Information systems shall be regularly checked for compliance with security standards.

## Information Security Incident Management

**Monitoring** (Page 17)

* Where practical, audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
* Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewee regularly.

## Business Continuity Management

**Information Security aspects of Business Continuity Management** (Page 21)

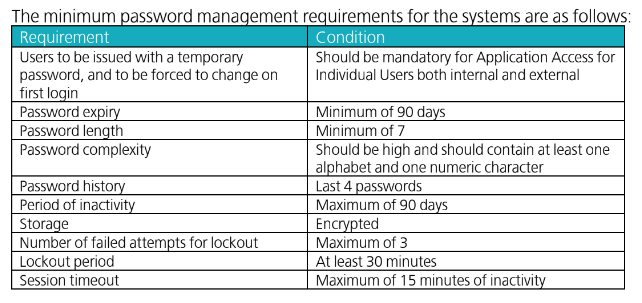
* Business continuity plans shall be tested and updated regularly to ensure that they are up-to-date and effective.

## Access Control

**User Access Management** (Page 25)

* Access rights are reviewed by CCIARCO quarterly and their adequacy is confirmed.

## Password Management (Page 28)



## Security Education, Training, and Awareness (Page 29)

* Annual information security awareness (old & new)

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# Tangent Enterprise Risk Management and Integrated Framework

## POLICIES AND GUIDELINES

**Policy Framework Statements** (Page 8)

* Review and update Business Objectives and Strategies annually.
* Review and update the Employee Code of Conduct annually.
* Review, update, and communicate Departmental Risk Register to team members on a quarterly basis.

## To the CC-IARCO (Page 9)

* Regularly collaborate with the Board, OPC, and Executive Committee on the Tangent Risk Profile.
* Monthly ManCom Meetings to discuss key business performance and regular matters to effectively monitor significant variances and deviation from standard operating procedures and budget.
* Provide monthly and annual report to the Board/OPC as compliance.

## Internal Control System (Page 12)

* Review of internal policies and standard operating procedures on an annual basis to ensure its relevance and effectiveness carried out by CC-IARCO as third layer of defense.
* An annual internal audit plan approved by the Board/OPC will be conducted and results and recommendations will be discussed and presented to the Executive and Management Committee.
* Periodically review, monitor, and update the assurance map that lists the organization’s risk categories as sources of risk, assurance provider, controls and descriptions to ensure effectiveness.

## Risk Reporting and Monitoring (Page 14)

* Risk monitoring is reviewed regularly for proper disclosure to assure the shareholders that risks are being managed effectively.
* Review the risk register at least once a year and whenever there are incidents that suggest the controls in place are not working well.

## Information Technology Controls and Security (Page 15)

**Disaster Recovery Backup Plan**

* DR drills are conducted by the Professional and Technical Services Division together with external service provider at least once a year with continuous effort to enhance the DR capability to cover all key aspects of the business.
* Schedule an annual certification exercise to ensure PCIDSS compliant.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Business Continuity Management Policies and Procedures

## Business Continuity Plan (BCP) (Page 15)

* The OPC must approve and sign the BCP. In order to be considered compliant with this policies and guidelines, CC-IARCO should set clear testing and reviewing schedules for BCP of at least once a year or following an important change in BCP components.

## Testing and Reviewing (Page 15)

* At least annually, exercises will be applied to the Business Continuity Plans; with any corrective or preventative actions implemented as a result.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# Incident Management Policies and Procedures

## INCIDENT RESPONSE SUPPORT (Page 13)

* There should be a designated security employee who should be available 24/7 to respond to unauthorized activity, detection of unauthorized wireless access point, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.

## TRAINING (Page 13)

* The staff providing incident response must be appropriately and periodically trained to respond to security breaches. Training requirements must be assessed on the basis of incident response plan testing and performance of incident response employee[s].

## INCIDENT RESPONSE PLAN UPDATING (Page 14)

* There must exist a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. Annual Security Incident Response Test Procedure can be used for this purpose. Any lesson-learned during the test phase must be incorporated into the Production Procedure.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# Change Management Policies and Procedures

## Policy Statements (Page 6 and 7)

* CRF cannot be submitted more than 45 days before the planned implementation start date.
* CRF cannot span more than 60 days between the implementation start and end date.

## POLICY COMPLIANCE AND MONITORING (Page 25)

* CRFs and CMFs will be audited on a periodic basis by CC-IARCO for policy compliance. The PTSD Division Head will be notified of any individual who violates the policy. The violation may be subject for review and further actions.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# Tangent Health and Safety Manual (THSM)

## Guide to Stakeholders

**Workplace Safety Audit** (Page 10)

* The findings of these audits will be available to the HSMC and the action plans to address any issues will be implemented as soon as reasonable. Specific Roles and Responsibilities

**Specific Roles and Responsibilities**

## Safety Officer (Page 12)

* Conduct monthly health and safety meetings.
* Conduct regular workplace inspections as per the annual schedule as well as assessment of workplace.
* Prepare the monthly SHARE report (Safety and Health Accomplishments, Records and Evaluation Report).
* Schedule and lead monthly safety meetings of the HSMC.
* Monthly inspections will be scheduled for fire extinguishers, emergency lighting inspections, etc.

## Occupational Health Physician (Page 13)

* Maintain and analyze records of all medical cases and to prepare and submit to the Company annual medical reports, using form DOLE/BWC/OH-47, as required by the OSH Standards.

## Occupational Health Nurse (Page 13)

* Maintain a reporting and records system, and if a physician is not available, prepare and submit an annual medical report using form DOLE/BWC/HSD/OH-47, to the Company, as required by the OSH Standards.

## Other Occupational Services (Page 27)

Annual Physical Examination is given annually or every January for all regular employees which includes the following:

* Chest x-ray examination
* Urinalysis examination
* Fecalysis examination
* Complete blood count
* ECG (for employees over 35 years old)
* General physical and medical history taking
* Drug test

## Health and Safety Programs (Page 29)

**Training and Education for All Employees**

* The functional unit heads will ensure that all employees are trained upon hiring and are given refresher training annually.

## Planned Inspections (Page 31)

* Planned inspections should occur on a monthly basis and shall involve the Functional Unit Heads (FUHs) and employees. This type of inspection should cover all areas of operations.

## Types of Inspections (Page 31)

**Annual Comprehensive Safety and Sanitation Inspections**

* The Safety Officer performs these inspections annually at each functional area. Follow-up inspections are performed to ensure that corrective action has been taken.

## Annual Fire Safety Inspections (Page 32)

* Certified fire safety inspectors perform fire safety inspections annually at each functional area.

## Fire Extinguishing Equipment Inspections (Page 32)

* Certified inspectors, on a regular basis, conduct fire extinguishing equipment inspections. General Administration thru Safety Officer perform monthly visual inspection of all fire extinguishers.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# Quality Manual

## Training Plan (Page 23)

* Top Management shall provide guidance on company strategy and objectives on an annual basis to the Management Committee (ManCom) who consider the implications on their functional unit and plan training needs accordingly, in line with the requirements of the company business plan. Tangent Solutions, Inc. shall summarize major training initiatives and activities planned for a given budget year.
* The Functional Unit Heads should develop, implement, and monitor a training plan for their teams, based on the outcome of the Training Needs Analysis (TNA). Training plans must be reviewed regularly to ensure that they are up to date and meet current demands.

## Annual Appraisal Reviews (Page 26)

* Training needs are also identified through the Annual Appraisal Review process. The HCMD and the Functional Unit Heads should be responsible for sourcing suitable training from an approved provider and for pre-course arrangements and administration. The training is provided as per the plan, while training effectiveness is discussed and reviewed during the appraisal process.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Anti-Virus Management Policies and Procedures

## Avoiding Virus Infection (Page 7)

* Make regular backups, store on the local directory and do not store information on the PC so that if infection does occur, data can be recovered.

## Controls against Malicious Code (Page 9)

* Anti-malware software shall conduct scans of critical computing devices on boot and every 24 hours.

## PROCEDURES (Page 12)

* The anti-virus product installed on desktops and servers must be configured to update on a daily or more frequent basis.

## Anti-Virus Program (Page 16)

**Servers**

* Windows – any server running a Windows operating system is required to have Windows Defender running. Windows Defender must be configured to automatically update daily.

**Workstations, Laptops, and other Personal Computers**

* Windows – any personal computer running a Windows operating system is required to have an anti-virus program running. The anti-virus program must be configured to automatically update daily.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Access Control Policies and Procedures

## Inactive or Temporary User Accounts (Page 10)

* User accounts will be disabled after 3 months of inactivity or have not logged in since 90 days.

## Logs and Other Security Tools (Page 14)

* CC-IARCO will prepare regular reports for BOD/OPC regarding security access issues, incidents, status, degree of compliance, changes, and initiatives and other relevant events.

## 

## REVIEW AND REVISION (Page 15)

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Audit Logging and Monitoring Policies and Procedures

## Audit Logging and Monitoring System in User (Page 5)

* All critical systems (including but not limited to servers, network devices, databases, applications and security devices) must be configured to enable the audit logging and to send all the logs on **real time** or at **least daily basis** to central log management (syslog) system.
* Audit logs generated by system components for which user activity audit logging is configured should **be reviewed daily** by the Information Security Team. The schedule/matrix of audit log requirements and the audit log reports are classified as confidential information and must be handled in line with the requirements of Information Security Policies and Guidelines for handling confidential information.
* System Administrators are prohibited from erasing or deactivating logs of their own activities. Monitoring reports are **reviewed daily** by the Information Technology Team. Any evidence of system misuse is reported to the Information Security Team who investigates further, and the disciplinary process may be invoked.

## Administrator and Operator Logs (Page 6)

* Logs are to be retained for a**t least one year** with stored online for a minimum period of **3 months** for immediate analysis or review.

.

## Log Management (Page 8)

* All log monitoring systems are placed in a segregated network and protected by the firewall. No direct access to the backend database holding the audit logs are allowed. Logs are to be retained for at least one year with stored online for a minimum period of 3 months for immediate analysis or review.

## Audit Log Review Process (Page 8)

* **Daily log reviews** by personnel or automated means must be performed to identify and proactively address unauthorized access to the cardholder data environment (CDE) and other security events.
* **Daily review** of all security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components all system components that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD), or that could impact the security of CHD and/or SAD and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues.

## Guidelines to Tangent Stakeholders (Page 9)

**To the Systems and Network Administrators**

* .Responsible for configuring logging on individual systems and network devices, analyzing those logs **periodically**, reporting on the results of log management activities, and performing regular maintenance of the logs and logging software.

## 

## Frequency of Review (Page 12)

* .Log monitoring is done on a daily, quarterly and annual basis. Available logs should be reviewed in response to suspected or reported security problems.

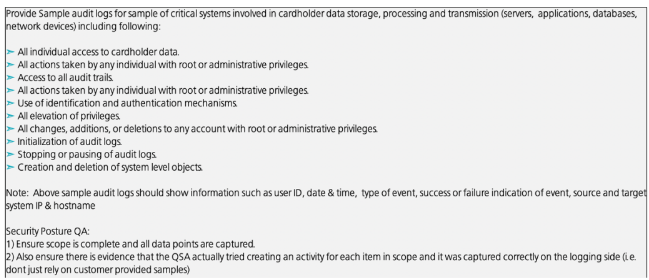
## Retention (Page 12)

* Active logging must be available for at least 3 months or 90 days.
* Once logging data has gone beyond 90 days, the data must be archived for 1 year, unless otherwise instructed by other entity (i.e. evidence, investigation, etc.).
* Logging data must be backed-up as part of the system’s regular backup process.
* The data itself must also be periodically audited by the IST for availability and integrity purposes.
* Management has given consideration to extending retention of audit logs associated with online activities involving pending incidents/breaches, investigations, litigation, and disciplinary action. All incidents that are logged are reviewed by management at a minimum annually.

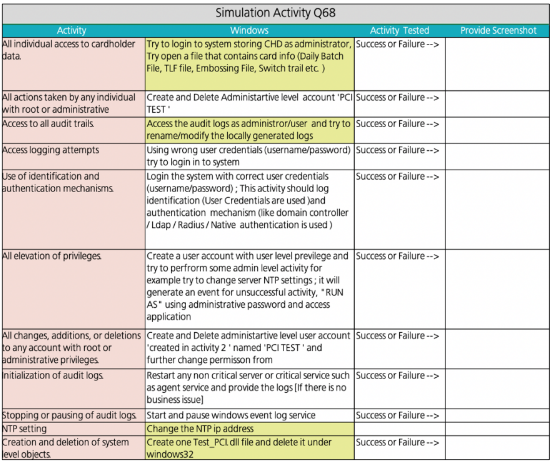
## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

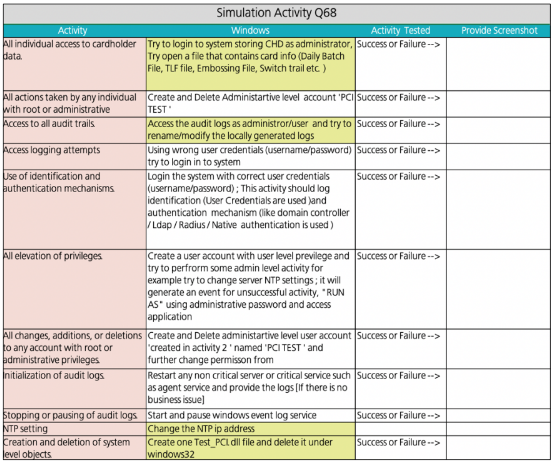
## Logging and Monitoring Event Logs



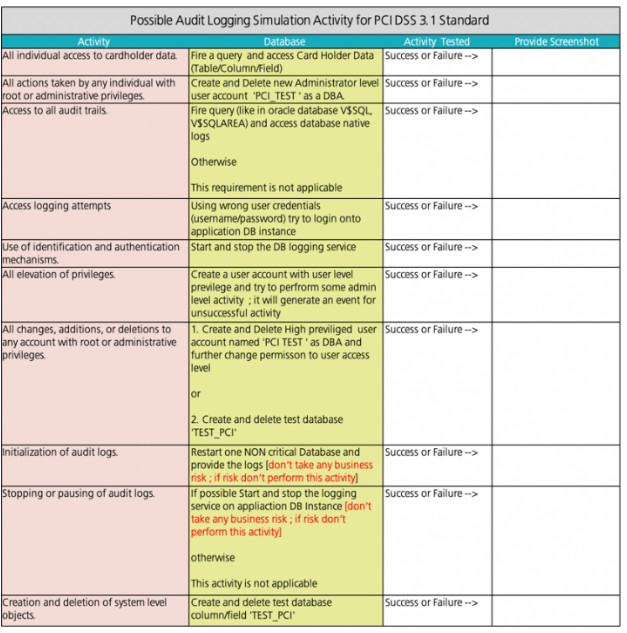
## For Windows:



For Network:

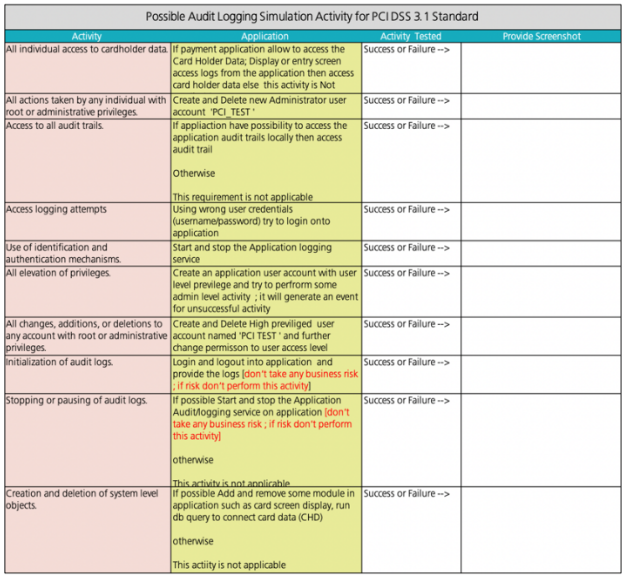


For Database



:

For Application:



# 

# Card Data Encryption Policies and Procedures

## Data Encryption at Rest

* Quarterly review must be performed to ensure card data is not stored exceeding retention period.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Cardholder Data Retention and Disposal Policies and Procedures

## Data Handling

* Conduct a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.

## PROCEDURES

* A quarterly review must be conducted to verify that stored CHD does not exceed retention requirements. If utilizing the Payment Gateway server, an automatic process will be used to remove stored cardholder data that exceeds the retention limit as defined herein.
* Cardholder data should be retained for two (2) years, depending on the business needs not exceeding five (5) years. Business needs include the ability to access cardholder data for purposes of processing credits on previous payments. It is not anticipated that cardholder data would be needed beyond a five-year period for legal, regulatory, or business reasons. Therefore, Tangent has established a general cardholder data retention period limit of five years.

.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Configuration Management Policies and Procedures

## Firewall Logging and Alerting (Page 14)

* Event log information related to the traffic passing through the firewall must be exportable to reporting and analysis tools. Event logs (audit trails) shall be available on demand online for analysis purposes for a minimum period of 90 days. Firewall event logs must be archived offline for at least 365 days (one year). Event logs must be managed and maintained in a manner compliant with the Tangent implemented audit and relevant standards for Information Security. All the event logs must be monitored by the Information Technology Team and trigger alerts if any..

**Connection Accounting**

* Logs must be retained for at least 30 calendar days.

**Active Connections**

* The installed firewalls or the related management server shall provide facilities to view in real time all connections currently active through the gateway.

.

## Firewall Administration (Page 15)

* Unauthorized access attempts from the external network must be reported via a real-time alert.

## Review of Firewall Rule Sets (Page 18)

* Firewall rule sets must be reviewed at least bi-annually. Vulnerability assessment scans shall include scans of rule sets for common configuration errors.

## Router Change Control (Page 22)

**Authentication**

* Passwords must be changed every 90 days on all routers.

## Review of Firewall Rule Sets (Page 18)

* Firewall rule sets must be reviewed at least bi-annually. Vulnerability assessment scans shall include scans of rule sets for common configuration errors.

## 

## Backup (Page 23)

* Backup of router configuration file must be taken every Quarter at-least.

## Router Logging and Alerting (Page 26 and 27)

* The audit logs of internet-facing routers must be monitored on a daily basis and a quarterly report on critical events must be submitted to IT Head/ Head IT security.
* Event logs (audit trails) shall be available on demand online for analysis purposes for a minimum period of 90 days. This period can be extended if system resources allow sufficient storage area for the duration.
* Router event logs must be archived offline for at least 365 days (one year). Event logs must be managed and maintained in a manner compliant with the Tangent implemented audit and relevant standards for Information Security.
* Connection Accounting - Logs must be retained for at least 30 calendar days.
* Active Connections - The installed routers shall provide facilities to view in real time all connections currently active through the gateway.
* Real-Time Alerting Mechanisms - Unauthorized access attempts from the external network must be reported via a real- time alert.

## 

## Review of Router Configuration (Page 30)

* Internet facing routers running configuration must be reviewed at least Quarterly and routers which are confined to intranet routing must be reviewed Bi-annually. Vulnerability assessment scans shall include scans of running configuration for common configuration errors.

## Patch Management (Page 32)



* Patch implementation steps must be monitored on a periodic basis and patch completion records must be archived for future reference with relevant details.

## Administration Specific

* IT Operations is responsible for ensuring implementation of Antivirus software and related automatic updates on all Computing resources. All systems should be configured to have daily virus signature update or whenever signature released from Anti-virus software vendor.
* All computing resources must be scanned at least once every week for adequate protection from malicious code.
* Tangent shall ensure that all anti-virus audit logs are retained for at-least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).

## 

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Daily Operational Security Policies and Procedures

## Maintain a Vulnerability Management Program

* Protect all systems against malware and regularly update anti-virus software of programs.(Page 12)

(a) Deploy anti-virus software to protect systems

* + - For systems considered not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats to confirm whether such systems continue not to require anti- virus software (PCI DSS Requirement 5.1.2).

(b) Ensure that all anti-virus mechanisms are current

* + - Anti-virus software must be capable of generating audit logs and audit logs must be retained for one year (PCI DSS Requirement 5.2c).

(c) Ensure that all anti-virus mechanisms are actively running.

* + - All anti-virus software installations and configurations must be actively running at all times (PCI DSS Requirement 5.3).

## 

* Develop and Maintain Secure Systems and Applications.(Page 13)

(b) Regularly update systems and software

ning.

* + - All critical system and software patches must be installed within 30 days of vendor release (PCI DSS Requirement 6.2b).
* Protection from Tampering and Substitution.(Page 15)
  + - Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) (PCI DSS Requirement 9.9.2).

## Regularly Monitor and Test Networks (Page 16)

## Important components of overall system security are the regular testing of networks for exposed vulnerabilities and the continuous monitoring of security indicators (logs, system events, etc.).

## 

(c) Log Review (Page 17)

Review logs and security events for all system components to identify anomalies or suspicious activity by performing the following: (PCI DSS Requirement 20.6)

* Review the following at least daily: (PCI DSS Requirement 10.6.1)

- All security events

- Logs of all system components that store, process, or transmit or affect the security of cardholder data.

- Logs of all critical system components

- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion- detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, ecommerce redirection servers, etc.).

* Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment (PCI DSS Requirement 10.6.2)

(d) Audit Trail History (Page 18)

* Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (e.g. online, archived, or restorable from backup) (PCI DSS Requirement 10.7).

## Regularly Test Security Systems and Processes

(a) Rogue Wireless Network Detection (Page 18)

* Tangent will have a documented process for quarterly assessments to detect unauthorized wireless networks/devices within the card- processing environment (PCI DSS Requirement 11.1 and 11.1.2).

(b) Vulnerability Assessment Scans (Page 19)

* Internal and external vulnerability assessment scans must be performed at least quarterly and after any significant change in the cardholder data network (e.g. changes in firewall rules, or upgrades to products within the environment, etc.) (PCI DSS Requirement 11.2).
* Internal vulnerability scans must be: (PCI DSS Requirement 11.2.1a-c)
  + Performed quarterly
* External vulnerability scans must (PCI DSS Requirement 11.2.2a-c).
  + Be performed quarterly.
* Internal and external scans per the above policies are required quarterly and after any change deemed to be significant (PCI DSS Requirement 11.2.3).

(c) Penetration Testing

* If segmentation is used to isolate the CDE from other networks, a segmentation test is required to confirm all methods of segmentation are effective in isolating the CDE from out-of-scope systems or networks. These tests must be documented and performed at least annually and after any changes to segmentation controls or methods (PCI DSS Requirement 11.3.4).

## Maintain an Information Security Policy

**Maintain a Security Policy that Addresses Information Security for All Employees** (Page 20)

(a) Publish, Distribute, and Update the Information Security Policy

* The information security policy must be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment (PCI DSS Requirement 12.1.1).

(f) Policies for Sharing Data with Merchants, Service Providers, and Clients

* Tangent shall annually review evidence provided by applicable service providers demonstrating their continuing PCI DSS compliance (PCI DSS Requirement 12.8.4).

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Data Back-up Policies and Procedures

## POLICY STATEMENTS (Page 5)

* All user-level and system-level information maintained by Tangent Solutions, Inc.shall be backed up periodically. The backup media shall be stored with sufficient protection and proper environmental conditions.
* Backups must be periodically tested to ensure that they are recoverable. To confirm media reliability and information integrity, the backup information shall be tested at some specified frequency.

## PROCEDURES (Page 6)

A. Backup Plan

* Server backups will be performed every business night, excluding holidays.
* Backups performed on Friday will be kept for a month before recycling.
* The last backup of every month will be considered the monthly backup and kept for a year before recycling.
* Monthly backup tapes will be stored in a fireproof safe.
* The last two monthly tapes will be stored offsite in a fireproof safe.
* Tapes will be inserted routinely every night before leaving work.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Key Management Policies and Procedures

## Policy Statements

**Key Injection Room (**Page 5)

(d) Footages from the surveillance camera is available for a duration of 90 days

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Payment Card Industry Data Security Standard PCI DSS Charter

## 

## ACCOUNTABILITY FOR PCI DSS COMPLIANCE

## Deputy Director for Professional and Technical Services

* As directed by the President and CEO, will be responsible for the periodic re-evaluation of current operational methods to identify possible areas for security improvement.

## COMMUNICATION (Page 7)

**Annual Security Training**

* Pursuant to PCI DSS requirements 12.6 that Tangent Solutions, Inc. shall implement a formal security awareness program to make all employees aware of the importance of cardholder data security at least annually.

**System Vulnerability Scans (as appropriate and applicable)**

* Tangent Solutions, Inc. is required to perform a quarterly internal vulnerability scans and rescans as needed, until all “high risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified employees.

**System Penetration Testing (as appropriate and applicable)**

* Tangent Solutions, Inc.shall perform external and internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

**Periodic Reviews and Audits of Functional Areas**

* Tangent Solutions, Inc. will regularly review the completed vulnerability scans, along with penetration tests, all employees, attestations, training, procedures, controls and documentation within the Cardholder Data Environment (CDE). Periodically, additional information and follow-up interviews may be requested and visits to certain CDE areas with or without notice. These activities are implemented to reduce the Company’s risk by ensuring it complies with PCI DSS requirements.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Remote Access Policies and Procedures

## POLICY STATEMENTS

* Network team / Information Security team shall maintain the list of users with remote access and their access privileges. List of authorized remote users shall be reviewed on a periodic basis by Network team / Information Security team.
* Any remote access account inactive for a period of 90 days must be disabled and communicated to the individuals concerned.
* All remote access logs must be maintained for a period of one year and must be reviewed every week.
* Authentication User IDs must be set to expire in 3 months or less and renewed on a 'need to have' basis.
* Users of non-Tangent assets must be able to prove that security measures have been taken to avoid abuse or security breaches. These measures can be audited by Internal Audit Team at any time.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Secure Software Development Life Cycle Policies and Standards

## 

**Policy Statements**

## (a) Vulnerability Management (Page 5)

* Vulnerability Scanning as part of the PCI DSS Compliance requirements, Tangent will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
* Quarterly Internal Vulnerability Scans must be performed by Tangent or a third party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.
* Quarterly External Vulnerability Scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by Information Technology staff. The scan process should include re-scans until passing results are obtained.

## (b) Vulnerability Management (Page 6)

* Automatic Updates – all systems must have automatic software updates enabled for system patches released from their respective vendors. Security patches have to be installed within one month of release from the respective vendor and have to follow the process in accordance with change control process.

## (e) Awareness Testing (Page11)

* Meetings – review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day practice.
* Policy Audit – Tangent security policies must be reviewed annually and updated as needed.

## (h) Disposal of Stored Data

* All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.

## (i) Network Security and Monitoring (Page 14)

* Audit Network Security – firewalls must be implemented at each internet connection and any demilitarized zone and the internal company network. A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
* Review Topology – disclosure of private IP addresses to external entities must be authorized. A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network. The firewall rules will be reviewed on a six months basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base.

**WEB APPLICATION SECURITY BEST PRACTICES** (Page 25)

(e) Setup status calls internally and externally. Internal status calls should take places twice a week and include the testers and the project/client manager. External status calls should take place once a week and include the internal team and the customer[s]. If possible, the project manager should walk through team status and then pass to team members for details.

## E. Buffer Overflows (Page 39)

* Keep up with the latest bug reports for all Web and Application server products and other products in the Internet infrastructure. Apply the latest patches to these products. Quarterly scan all website with one or more of the commonly available scanners that look for buffer overflow flaws in server products and custom web applications.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Software Development Policies and Procedures

**POLICIES STATEMENTS**

* All the resources responsible for application development, testing and code review shall be trained periodically by professionals on their specific domain related to secure coding techniques, security testing and secure code review. The training shall include the industry standard practices and guidelines.
* Public-facing web applications must be reviewed using the tools and/or methods as follows: (a) At least annually

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Technology Usage Policies and Standards

C. Asset Management

* Tangent Solutions, Inc. shall maintains inventory of information assets (servers, network devices, security devices, database, applications etc.) and Company approved products listed in Tangent Asset Inventory to include information such as device name, type, owner, contact information, hosting location and purpose. Tangent Solutions, Inc. shall perform review of this inventory after every major change and on annual basis.

F. Guidelines to Tangent Stakeholders **(Page 7)**

* Provide Information Security Awareness Training as part onboarding orientation and annual training to all employees.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

# 

# Third Party Management Policies and Procedures

**POLICIES AND GUIDELINES**

## **A. General Policy Statements** (Page 4 and 5)

* List of all service providers / third parties to Tangent Solutions, Inc. with details of service offering and sensitive information (e.g. Cardholder or payment information) in scope of service must be maintained and reviewed at least on annual basis for any update;
* All risks resulting from third party access must be reassessed on a periodic basis, or whenever such risks change;

## Third Party Access Control Requirements (Page 7)

* Remote access connections with third parties shall be monitored on an ongoing basis.

## Third Party Service Delivery (Page 7)

* Tangent shall develop, disseminate and update at least annually a list of current service providers.

## Third Party Service Providers Monitoring and Review (Page 8)

## The services, reports and records provided by the third party Service Provider shall be monitored and reviewed on an annual basis, and audits shall be carried out to ensure compliance with the third party Service Provider agreements is maintained.

* The results of monitoring activities of third party Service Provider shall be compared against the SLA or contracts at least annually.
* Regular progress meetings shall be conducted as required by the SLA or contract to review reports, audit trails, security events, operational issues, failures and disruptions, and ensure identified issues are investigated and resolved accordingly.
* Network connections with third party Service Providers shall be periodically audited to ensure that they have implemented any required security features and meet all requirements agreed to with Tangent.

## Exit Plan / Termination (Page 9)

* The plan must be reviewed and updated on an annual basis, or in the even of a significant change, to ensure that it remains appropriate.

## Information Gathering

* Due diligence should be performed not only prior to selecting a third party relationship, but also periodically during the course of the relationship,particularly when considering a renewal of a contract. The following items may be included:
  + Audited financial statements, annual reports, Securities and Exchange Commission filings, and other available financial information;

## BOARD AND MANAGEMENT OVERSIGHT

* Determine if the board initially approved significant third party arrangements, and what the Board considered in reaching that approval. Additionally, determine if the board oversees and reviews, at least annually, significant third-party arrangements, and reviews these arrangements and written agreements whenever there is a material change to the program.
* Determine if management periodically reviews the third party’s operations in order to verify that they are consistent with the terms of the written agreement and that risks are being controlled. CC-IARCO should also ensure continuing compliance with applicable laws and regulations, as well as internal policies and procedures.
* Determine if the results of oversight activities for material third-party arrangements are periodically reported to Tangent’s BOD or designated committee. Identified weaknesses should be documented and promptly addressed.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

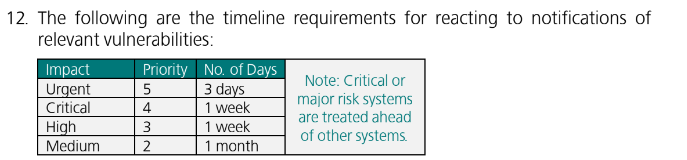
# 

# Vulnerability Management Policies and Procedures

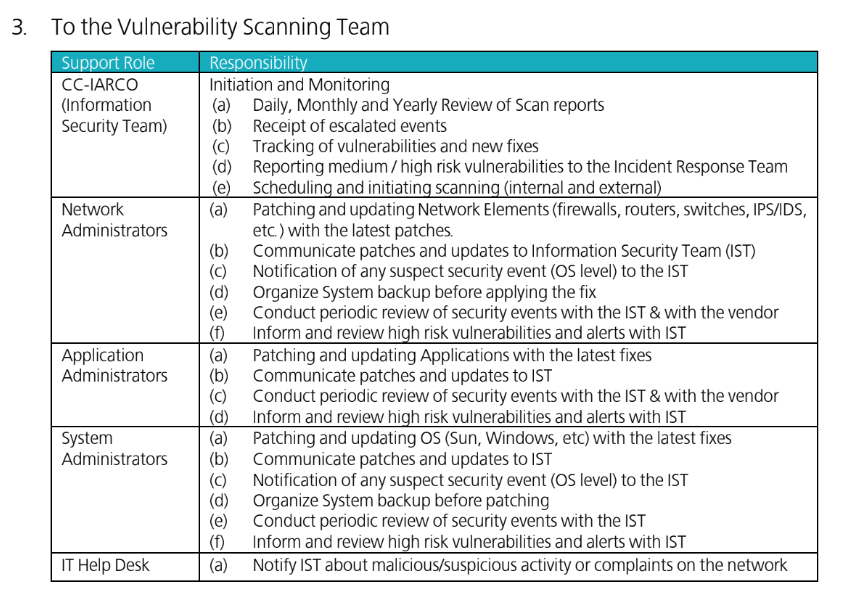
**POLICIES AND GUIDELINES**

## A. Policy Statements (Page 5 and 6)

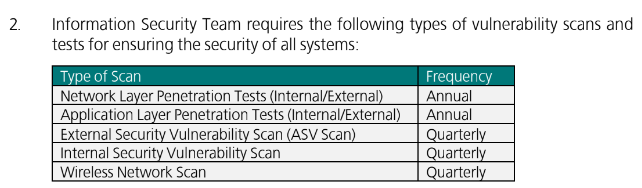
* Periodic vulnerability assessment of its information assets, network equipment, and applications have to be conducted and fix all gaps found during the assessment.
* On a quarterly basis internal and external security testing of the devices in the cardholder environment are conducted. Scans are repeated until “clean results” are obtained.
* Internal vulnerability scanning must be performed on IP’s in scope on quarterly and after any significant change in the network (such as new system component installations, changes in the network topology, firewall rule modifications, product upgrades) on all the assets in scope.
* Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the PCI SSC. Perform rescans as needed, until passing scans are achieved. All external/public IP’s must be included in the ASV scan.
* The penetration tests must be carried out either by third party organization specialized in Security Testing or by specialized internal resource. It shall be ensured that penetration test (PCI DSS Requirement 11.3):
  + includes review and consideration of threats and vulnerabilities experienced in the last 12 months
* Wireless network scan are performed using Wireless Analyzer on quarterly basis



## 

****

**VULNERABILITY MANAGEMENT AND TESTING**

**A. Scan Type and Schedule** (Page 10****

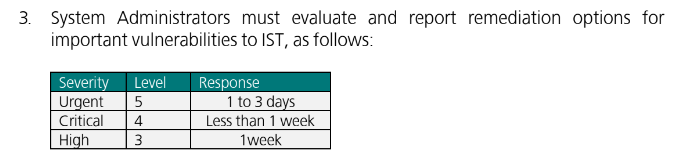
* Quarterly wireless scan should be performed using industry standard tools for detection of unauthorized or rouge wireless access points or devices across all PCI DSS scope locations. The scan report generated through tool should be retained as record along with justification or explanation for detected wireless access points or devices.

## C. Scan Review

* Information Security Team must review all vulnerability scans for a system within 24 hours of scanning. If a scan occurs during the weekend or on a holiday, scan review must occur on the first business day following the scan.

## D. Remediation

* System Administrators are responsible for remediating vulnerabilities identified during vulnerability scanning. System Administrators must evaluate vulnerabilities identified as critical by the scan engine or high risk through analysis within 24 hours of discovery.



## Reporting

The System Administrator must document and report any exceptions on their systems to the information Security Team at completion of evaluation or remediation. The System Administrator will include Application, Database and Data Owners as needed on a per scan basis. The System Administrator must provide the Information Security Team with a report.

If reporting involves a designee of the System Owner, the designee must provide a monthly summary of scanning activity and exception documents to the System Owner.

## REVIEW AND REVISION

* This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. Refer to related references.