PCI DSS Policies and Procedures

Presented To:
Grupo CSI

4/21/2017

Prepared By:
Justin Sulhoff

Table of Contents

9.10 Data disposal policy

Requirement 10 – Logging and Auditing

10.2 Events Logged
10.3 Event Log Structure
10.4 Network Time Protocol (NTP)
10.5 Log Security

Requirement 11 – Regularly Test Security Systems and Processes

11.1 Scan for rogue wireless devices
11.2 Vulnerability Scans
11.3 Vulnerability Penetration Testing
11.4 Use Intrusion Detection Systems (IDS's) and/or Intrusion Prevention Systems (IPS's)

Requirement 12 – Maintain an Information Security Policy

12.1 Establish, publish, maintain and disseminate an information security policy
12.3 Special technology use policy
12.2, 12.4 – 12.5 Information security roles and responsibilities
12.6 Security awareness program
12.7 Employee background checks
12.8 Third-party information sharing – due care and due diligence
12.9 Incident response plan

I. Introduction

The following document outlines Grupo CSI's information security policies and procedures. Grupo CSI takes the security of critical data and business-related assets very seriously. Therefore, management requires that all employees understand and comply with these policies.

It is Grupo CSI's intended purpose to protect client, employee, financial, protected third party and other corporate information from unauthorized disclosure, modification or destruction throughout the information's lifecycle.

To accomplish this, Grupo CSI has developed this set of IT Security Policies and Procedures in conjunction with a rigorous PCI DSS Compliance Assessment performed by a third party Qualified Security Assessor. These policies offer direction to specific departments and staff members, and it is each individual's responsibility to uphold those policies that directly relate to their position at Grupo CSI.

Violations of this policy or related standards may lead to disciplinary action, up to and including termination.

Brief Explanation of Payment Card Industry (PCI) Compliance

In September of 2006, the five biggest payment companies (VISA, American Express, Discover, JCB, and MasterCard) created the PCI Security Standards Council. Their mutual goal was to create a single process that would enable companies to secure credit card data across all brands.

Together, they devised the Payment Card Industry Data Security Standard (PCI DSS) Program. This program enables merchants and service providers to safely store and process credit card information, whether they are using manual or computerized credit card processing solutions. E-commerce websites and POS devices that process information over the Internet are subject to the most demanding PCI assessments due to the heightened risk of online data interception.

II. Scope of Policies and Procedures

These IT security compliance policies and procedures apply to all users of the computer systems and networks of Grupo CSI, including but not limited to all employees and associates of Grupo CSI and its wholly-owned subsidiaries. They also apply to the activities of all Grupo CSI personnel using or affecting Grupo CSI's computer systems and networks. In addition, these policies and procedures apply to the activities of all third-party consultants, contractors, vendors and temporary employees using Grupo CSI's computer systems and networks.

Any system component that is connected to the card-processing or data storage environment is in scope for PCI compliance. System components include servers, applications, employee PC's, and other network components.

Examples of everyday systems that are in scope for PCI compliance include:

- Web Servers and app servers that process credit card data.
- Databases and PC's used to store credit card data.
- Firewalls or network devices used to transport cardholder traffic.
- Printers, fax machines, and other devices that may temporarily hold data.
- Support systems, such as syslog server or Active Directory, primarily used by system admins.

The following policies and procedures are intentionally broad in scope. The standards are specific and are regularly updated to keep pace with changes in business, technology and the business environment. Standards include details such as business process flows, roles and responsibilities, technical specifics and contract requirements.

Requirement 1 - Firewall and Router Security Administration Policy

1.1 Policy Applicability

All Grupo CSI owned and operated routers and firewalls are in-scope for this policy. Exemptions may only be authorized with written approval from Grupo CSI management or approved Security Officer.

1.1.1 Firewall Configuration Changes

Firewalls are categorized as *production systems* as they support Grupo CSI information systems.

Any and all changes to the firewall must be approved in advance by the Information Security Department. The changes must be thoroughly tested (following production standards) as outlined in the Change Control Policy. Examples of changes include:

- Upgrades or patches to the firewall system.
- Modifications to any firewall software or system.
- Additions, deletions, or modifications to the firewall rules.

1.1.2 – 1.1.6 Device Management Responsibilities

The team responsible for managing Grupo CSI firewalls and routers will be comprised of the Information Security Department.

Information Security Department Roles and Responsibilities:

- Ensures that any changes to the firewall hardware, software, or security rules are authorized by the Information Security Department and follow appropriate change control policies.
- Ensures that all router configuration files are synchronized and secure.
- Uses Permitted Network Services and Protocols to document any firewall security rule changes.
- Mitigates security events by coordinating a sufficient response plan with the Information Security Department.
- Reviews and updates network diagrams after any changes are made. The diagrams must accurately describe firewalls, access control systems, anti-virus software, IDS/IPS, and any other connection to confidential or sensitive information.
- Reports any discovered vulnerabilities or security events to the Information Security Department.
- On a daily basis, monitors all logs that capture and report security events.
- Provides the Networks Operation Center read-only access to logs related to security events and the performance of critical systems.
- Keeps track/monitor system alerts related to critical systems. These alerts might include system reboots, firewall daemon failing etc.
- In the event of a security system failure, alerts the appropriate department.
- Assures Grupo CSI management that the security rules applying to firewalls are sufficient to protect assets from unauthorized access.

- Assures Grupo CSI management that the security rules applying to firewalls are sufficient to prevent internal security threats from exiting the network.
- Mitigates security risks by developing an appropriate response plan with the System Administrator.
- At least every six months, the Information Security Department must perform a thorough review of each firewall rule set. The results must be recorded, and must include the removal of any unnecessary access paths. As a result, any proposed changes must go through the change control process before they are implemented.
- Identifies internal or external threats by actively monitoring firewall security events.
- Performs a thorough review of any proposed firewall and router security rule change. Ensure they meet policy compliance before sending the proposal through the change management process.
- Ensures the proper documentation of all services allowed through the firewall.
- For risky protocols, performs or approve a risk assessment and ensure the protocol has a specific business need.

1.2 – 1.3 Allowed Services and Connection Paths

The Grupo CSI firewall must block every path and service that is not specifically approved by this policy. The Grupo CSI must maintain a "Permitted Network Services and Protocols" form, which outlines the list of currently approved paths and services.

All inbound Internet traffic must use a network segmented by a firewall. This segmented zone is known as the DMZ. This inbound traffic must be limited to only those ports deemed necessary for Grupo CSI business. With the exception of the DMZ, perimeter routers should never be configured to include a route to internal address space.

All firewalls' and routers' configuration files must be secured to prevent unauthorized tampering. In addition, the start-up configuration files must be synchronized with the secure settings of the running configuration files in order to prevent weaker rules from running in the event that one of these devices re-starts.

Network Address Translation (NAT) or Port Address Translation (PAT) must be used to hide internal IP addresses.

Perimeter devices must be equipped with anti-spoofing technologies. These devices will reject all traffic that includes:

- A destination IP address matching RFC 1918 address space.
- A source IP address matching RFC 1918 address space.
- A source IP address matching any Grupo CSI-owned address space.

Internal production systems with outbound traffic must also use the DMZ network. This type of traffic should also be limited to only required protocols and services.

Any Grupo CSI databases must be stored on an internal network that is segmented from the DMZ network. All inbound connections to internal production payment systems, and originating from Grupo CSI wireless networks, are forbidden.

Internet and wireless segmentation must employ a stateful packet inspection firewall. This will allow only established connections in or out of the network. For cardholder environment

segmentation, VLANs with compliant ACLs may be used – so long as the VLAN switch is PCI compliant and hardened to deter switch exploits such as ARP cache floods. VLANs must be established according to the same requirements that apply to firewalls.

1.4 Personal Firewalls

Personal firewall software must be installed and activated on any Internet-connected mobile or employee-owned computer that also accesses the Grupo CSI network. This software must have a non-user alterable configuration as deemed suitable by the Information Security Department.

Requirement 2 - System Configuration Policy

2.1 Policy Applicability

This policy applies to all Grupo CSI-operated servers and network devices, whether supervised by employees or third parties. All devices must have vendor-supplied defaults changed prior to deployment. Exemptions may only be authorized with written approval from the Information Security Department.

2.1.1 Changing Vendor Supplied Defaults of Wireless Access Points

Grupo CSI wireless networks must have default configurations changed at installation. Examples of vendor defaults that need to be changed at installation are the wireless encryption keys, passwords, and SNMP community strings.

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP versions 1 and 2c are subject to packet sniffing of the clear text community string from the network traffic, because they do not implement encryption. All versions of SNMP are subject to brute force and dictionary attacks for guessing the community strings, authentication strings, authentication keys, encryption strings, or encryption keys, because they do not implement a challenge-response handshake. Although SNMP works over TCP and other protocols, it is most commonly used over UDP that is connectionless and vulnerable to IP spoofing attacks. Thus, all versions are subject to bypassing device access lists that might have been implemented to restrict SNMP access. Therefore, it is critical to change the default SNMP community strings.

Grupo CSI wireless networks must be protected through secure data encryption methods, such as WPA or WPA 2 (if supported). Default settings using WEP as a key exchange protocol should not be used. WEP is considered an unsecure protocol. The minimum encryption strength for wireless networks is 128 bits and wireless encryption keys are to be changed at least once every 90 days, or whenever an employee with knowledge of the keys is terminated or leaves the organization.

2.2 System Configuration Standards and Deployment

Grupo CSI configuration standards for all system components must be maintained in accordance with industry-accepted system hardening standards. Grupo CSI shall develop and maintain standards based on one or a combination of the following sources:

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- SysAdmin Audit Network Security (SANS)
- National Institute of Standards Technology (NIST)

At the time of installation, a ‘System Configuration Record’ form must be completed for all deployed Grupo CSI systems. This record must be kept on file for the life of the system and must be updated in the event of a modification.

2.2.1 System Purpose

Grupo CSI computing systems should adhere to a ‘one primary function per server’ rule. For example: web servers, database servers and DNS should be operated from distinct and separate servers. Unless otherwise required by vendor documentation, no multi-purpose system may store, transmit, or process sensitive or confidential information. If Grupo CSI implements virtualization

technology, for example, multiple virtualized server instances on the same physical host; the virtual servers must be treated as individual server boundaries and thus secure configurations must be implemented to restrict communication between each other.

2.2.2 Limit System Functionality to Only What's Necessary

Only secure services, protocols and daemons that are necessary for a system to function are permitted. Functionality of system components should at all times match an up-to-date 'System Configuration Record' form that Grupo CSI maintains for all system component types. If any systems are configured to use insecure services, protocols or daemons, there must be a business justification to do so and additional security features must be documented and implemented in accordance with vendor-supplied documentation.

2.2.3 – 2.2.4 System Security Configuration Process

The following process is a guideline to be followed during new system deployment.

1. Install Operating System.
2. Update operating system software (following vendor recommendations).
3. Configure OS parameters to properly secure the system.
4. Install software and applications.
    a. If this is replacing an existing system, install system specific software according to the System Configuration Record.
    b. Install any software necessary for the systems objective.
    c. Configure NTP (Network Time Protocol).
5. Update all software (following vendor recommendations).
6. Configure application parameters according to build documentation.
7. Enable logging per Logging Controls in Section 15.
8. FIM (File Integrity Monitoring) software should be installed for systems containing sensitive or confidential information. Configure the FIM software to perform critical file comparisons on a weekly basis. This will alert the Information Security Department in the event of unauthorized modification of any critical system files.
9. Complete and archive a System Configuration Record for each specific system.

All Grupo CSI systems must install the following list of standard software. Any deviation or exemption from these configuration standards must include a reasonable business justification and an ac[Merchant DBA]ing risk assessment. The deviation must then be approved by the Information Security Department and logged in the System Configuration Record for the specific system.

- For Grupo CSI file servers, mail servers, and Windows-based systems:
    - Anti-Virus Software
- For critical production systems:
    - File Integrity software
- For Grupo CSI or personal notebooks/laptops:
    - Personal Firewall software
    - VPN Client software

Requirement 3 - Data Retention, Encryption and Key Management Policy

3.1 – 3.2 Data Retention Policy

Any and all data assets stored on Grupo CSI systems that are classified as sensitive or confidential must adhere to this policy. For credit card data, only the primary account number (PAN), cardholder name, expiration code and service code may be stored. In addition, an encrypted PAN is deemed to be PAN data that must adhere to this policy. The Information Security Department must provide written approval for any exemptions to this policy.

The data creator or authorized manager must establish a specific retention timeframe for any sensitive or confidential data stored on Grupo CSI systems. This information may be retained until legal, regulatory and business requirements have been met.

Generally speaking, single use cardholder data may be retained for up to 120 days. However, cardholder data used for recurring transactions may be retained for as long as the customer's account remains with Grupo CSI. In the event that the customer's account is deleted, that cardholder data must also be deleted/purged from the system within 120 days using approved disposal methods.

Specific cardholder authorization details, including PIN numbers and CVV2, will be retained only until the current transaction is completed. Retention of this data post-authorization is not allowed under any circumstance.

3.3 Displaying Credit Card Primary Account Number

No Grupo CSI employees shall have visibility to the full PAN except for those who have a legitimate business need to see the full PAN. Displaying full PAN on computer screens, receipts, faxes, or any kind of hard copy media is against Grupo CSI policy. A maximum of the first six and last four digits of the PAN may be displayed. All other digits must be masked. This policy is intended to protect credit card numbers as they are displayed and should not be confused with stricter requirements relating to storage of credit card numbers, which must utilize strong encryption, hashing or truncation.

Any application used by Grupo CSI that displays credit card information must be configured to hide or mask that sensitive or confidential data (if possible). If the purpose of the application involves displaying the full credit card number, or other personal data, approval for its use must be given by the Information Security Department. In all cases, this type of application must be limited to the fewest possible number of required users.

3.4 Encrypting Stored Cardholder Data

This encryption policy applies to all applicable Grupo CSI computer systems and primary as well as secondary storage locations, whether managed internally or by third party vendors. Examples of primary storage locations include but may not be limited to databases and flat files such as spreadsheets. Examples of secondary storage locations include but may not be limited to backup media such as USB thumb drives or tapes, and audit logs such as history, error, debugging, or transaction logs. Encryption must be employed for any stored credit card primary account numbers (PANs) and the entire PAN shall be encrypted. Card validation codes (CVV numbers) for card-

not-present transactions and PIN blocks must never be stored *post-authorization* under any circumstances.

One of the following methods must be employed to protect the PAN anywhere it is stored:

- Strong cryptography with associated key management processes and procedures.
- Truncation.
- Strong one-way hash functions with salts.
- Index tokens and securely stored pads.

3.6 Encryption Key Management

Encryption keys must be generated, accessed and stored in a secure manner.

In order to generate a strong key, a random or pseudo-random number generation algorithm must be used. The minimum length requirements for the encryption keys are 128 bits. Examples of acceptable algorithms are as follows:

- Triple-DES: 128 bits
- AES: 256 bits
- RSA: 1024 bits
- Follow vendor recommendations for other encryption types.

Any key used to either encrypt or decrypt cardholder data must be stored separately from general user access. Note: Key components may only be accessed by authorized key custodians.

The Information Security Department must authorize at least two key custodians in order to successfully perform a key action, such as key generation or loading the key. No individual key supervisor may have access to all pieces of a data encryption key.

A minimum of two authorized key custodians are required in order to generate keys. Each custodian will generate one text piece used in the key generation. Any type of access to the key generating procedures must be limited to authorized custodians and kept secure to prevent unauthorized key generation or replacement.

Encryption key component access will only be given to key custodians with a job duty that requires access. The Information Security Department will be responsible for granting access by utilizing an ‘Authorization Request Form’. Users who have been granted access must complete and sign an ‘Encryption Key Custodianship Form’. By signing the form, the user recognizes their responsibilities as a key custodian. Human Resources will maintain a copy of this form in the user’s employee records.

Only those authorized key custodians will be allowed to retrieve the key components from their secure location and distribute keys. Key custodians must track and log their activities within an ‘Encryption Key Management Log’. Before being returned to secure storage, the custodian must place the encryption keys in secure packaging.

During an encryption key change process, the key custodian generates a new key, decrypts the current production data and re-encrypts the sensitive data with the new encryption key.

On an annual basis, or whenever conditions warrant a change in key integrity, the encryption keys must be changed. Conditions for a key change include:

- **Annual Rotation**: Keys are to be changed once per year (minimum).
- **Suspicious Activity**: Keys are to be changed if any activity related to the key process raises concern or is otherwise deemed suspicious.
- **Resource Change**: Keys are to be changed if a key supervisor's employment ends or a key custodian accepts a position within Grupo CSI that does not involve the key encryption process.
- **Technical Requirement**: Keys are to be changed if a technical issue arises that questions the durability or security of a key (corruption or instability).

In order to dispose of an unwanted encryption key, key custodians must follow approved Grupo CSI methods for secure data disposal.

Requirement 4 – Secure Data Transmission

4.1 Transmission Over Un-Trusted Networks

To avoid interception or misuse of data, any confidential or sensitive information that is to be transmitted over public networks must be secured using strong encryption tactics, such as:

- Secure Socket Layer (SSL) or TLS
- Internet Protocol Security (IPSEC)

Grupo CSI wireless networks must be protected through secure data encryption methods, such as WPA or WPA 2 (if supported).

The minimum encryption strength for wireless networks is 128 bits and wireless encryption keys are to be changed at least once every 90 days, or whenever an employee with knowledge of the keys is terminated.

4.2 End User Messaging Technologies

Employees may never email unencrypted confidential or sensitive information such as credit card PANs. If a valid business justification exists, the Information Security Department will supply encrypted email software to said employee. In addition, employees shall never send unprotected PANs via other messaging technologies such as instant messaging, chat or text.

Requirement 5 - Anti-Virus Policy

5.1 – 5.2 Deploy Properly Configured Anti-Virus Software

All Grupo CSI computer assets, including file servers and email servers managed by employees or third parties, which runs the Microsoft Windows OS must comply with this policy. The Information Security Department must approve any policy exemption in writing.

The Information Security Department is responsible for approving anti-virus/anti-spyware software and configuring it for each system. Users must not be able to disable or otherwise configure the software. The approved software must perform real-time scans and log all anti-virus alerts with routing to a central logging solution. All anti-virus software should be configured to run daily virus signature updates.

In the event that a virus is detected during a real-time scan, the Information Security Department must be alerted at the same time.

Based on the Incident Response Policy, the Information Security Department will determine how best to resolve the virus alert.

All anti-virus software logs will be stored/archived in accordance with Grupo CSI logging and auditing policies and procedures. Generally speaking, logs must be retained for at least one year with three months immediately available for analysis. Logs must record all information necessary to reconstruct a security event. Logs should include:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component or resource

Requirement 6 – Develop and Maintain Secure Systems and Applications

6.1 Install the latest vendor-supplied security patches

When a vendor releases security patches, hot fixes and/or service packs it is the Information Security Department's responsibility to apply the changes as needed. The timeframe for installation on applicable systems is 30 days from the date of release, and the change management process must be followed.

6.2 Vulnerability Identification

Any issues or vulnerabilities related to Grupo CSI systems must be reported to the Information Security Department. Once identified, the Information Security Department is responsible for alerting system administrators and all relevant personnel.

In addition to monitoring vendor news sources, security personnel must monitor common industry vulnerability news groups and mailing lists for vulnerabilities and potential workarounds that may not yet be known or resolved by the vendor. Examples of outside news groups are:

- Security Focus
- Source
- Bug Traq
- Full Disclosure

Once a vulnerability is identified, the risk that vulnerability poses must be evaluated and ranked. This will allow the Grupo CSI Information Security department to address high priority risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.

Grupo CSI uses the Common Vulnerability Scoring System (CVSS) ver.2.0 calculator to determine the risk ranking for those vulnerabilities that are lacking a vendor-supplied patch classification. The following link provides access to the scoring calculator through NIST's website:

http://nvd.nist.gov/cvss.cfm?calculator&version=2

Grupo CSI System Configuration Standards must be updated to reflect all new vulnerabilities and the measures required to remediate them.

6.3 Software Development Lifecycle

It is important to consider the control measures and security checks that will be used throughout the software development life cycle. Proprietary software developed by Grupo CSI, whether internally or by a 3rd party, must utilize industry best practices for software development.

The following is a high level overview of the various security measures to be utilized during each phase of Grupo CSI's software development:

- **Requirements Analysis**: The developer is responsible for determining whether application requirements are sufficiently secure.

- **Design**: All application components must be developed in accordance with the latest data and network security trends.
- **Development**: The developer is responsible for considering vulnerabilities that might affect the application; such as privilege/access bypass and memory bound issues.
- **Code Review**: In order to better identify security issues, a second developer is responsible for conducting code reviews of all new or updated software.
- **QA Implementation**: It is important that the QA process does not hamper security controls or introduce new issues or vulnerabilities.
- **QA Testing**: The application's security features must be thoroughly tested, along with functional and efficiency testing.
- **Documentation**: Directions for correct security configurations must be included with all software feature guides and implementation/installation documentation.
- **Production Implementation**: It is important that the implementation process does not hamper security controls or introduce new issues or vulnerabilities.
- **Production Testing**: The application's security features must be thoroughly tested, along with functional and efficiency testing.
- **Maintenance**: New code must undergo the same reviewing/testing process as outlined above. Any future application maintenance must not hamper security controls or introduce new issues or vulnerabilities.

6.4 Change Management Policy

Any and all changes to Grupo CSI's network systems, devices and software configurations must adhere to the following Change Control Policy.

The department or staff member who proposed or implemented the change is required to complete and submit a Change Request Form to the Information Technology Department.

In order to review the change, the following information is mandatory:

- **Test Plan**: Develop a set of planned tests to determine if the change is effective and does not create additional risks or vulnerabilities within the network. Custom code changes must be tested for common coding vulnerabilities.
- **Back Out Procedures**: Develop a plan to revert the systems to their original configurations in case the change does not behave as expected.
- **Documentation of Impact**: This item must be completed if the change will affect internal or external customers in any way. Document how functionality will change for the customer, and include any applications and procedures that will differ from the existing system. Make a note of any upgrades or additional software the customer will be required to install/update.

Authorized approval must be obtained for any submitted Change Request Forms.

The proposed change must first be tested on an isolated network or QA environment that is not part of the overall network environment.

Using the approved Test Plan, ensure that the change will not adversely affect the network system in any way. Document any issues or potential problems and then create a new Change Request Form once those issues have been corrected. Follow the approved procedures to implement the successfully tested change. Ensure that back out procedures are prepared and ready for immediate invocation should an unforeseen issue arise during the change implementation.

For custom applications, a secure testing environment must be established that is separate from Grupo CSI's normal business environment. Access controls must be utilized to enforce the separation on any network that connects the testing environment to the business environment.

Actual cardholder data must not be used during software development/testing. Grupo CSI personnel must make every effort to use mock data and mock credit card numbers for testing purposes.

Once the testing process has been completed, all data (including custom accounts, usernames and passwords) must be deleted or disabled.

The Software Development Team must never have full time read/write access to business applications or data. Someone not part of the development team will be responsible for code promotion to the business environment. Developers may only assist in troubleshooting during an emergency, and will be issued a temporary, Emergency ID.

6.5 – 6.6 Develop and Test Web Applications Based on Secure Coding Guidelines

Any Grupo CSI applications that are considered web-based must be given special consideration. While these web-based applications must adhere to the same security measures outlined in the Development Life Cycle section, additional vulnerabilities must also be reviewed and tested.

Secure coding training is mandatory for all Grupo CSI developers, and their development process must consider the OWASP guidelines. These guidelines are available at the following website:

http://www.owasp.org

During the Code Review and Testing phase, the following vulnerabilities must be checked:

- Insecure Configuration Management
- Unvalidated Input
- Denial of Service
- Malicious Use of User IDs
- Insecure Storage
- Malicious Use of Account Credentials and Session Cookies
- Error Handling Flaws
- Cross-site Scripting
- SQL Injection and other Command Injection Flaws
- Buffer Overflows

On an annual basis, or whenever modifications have occurred, the web-based applications must undergo penetration testing performed by a 3rd party vendor. All custom code must be reviewed by an application security firm or have established an application layer firewall in front of web-facing applications.

Requirement 7 – Access Control

7.1 – 7.2 Data and System Access

All data assets stored on Grupo CSI systems must first be given a classification level by the creator or data manager. The classification level determines who can access the stored data.

Categories of Information:

- **Public**: This classification relates to data assets that pose no adverse risk to the Grupo CSI, and/or do not fit into the other categories below. Regardless, a user must receive approval from Grupo CSI's Public Relations Department before distributing any Public data.
- **Private**: This classification relates to personal data assets that are intended for internal Grupo CSI use only. Erroneous distribution of Private data could adversely impact Grupo CSI. Private data often includes intellectual property, working designs, or policies and procedures.
- **Sensitive**: This classification relates to business-related data assets that are intended for internal Grupo CSI use only. Erroneous distribution of Sensitive data could impact Grupo CSI, stockholders, business partners, and customers. Sensitive data often includes audit reports and market research.
- **Confidential**: This classification relates to data assets that pose the most risk to Grupo CSI, including passwords, bank account information, cardholder data, and encryption keys.

Grupo CSI systems must use an automated access control mechanism. Access controls must be configured and operational to track all access to data – including the user's identity, time and date, and a listing of the accessed data. This system of controls protects sensitive data and ensures that the information is not improperly distributed, copied, modified, or deleted.

Access to network systems and data must be limited to those employees who have been properly authorized. Each user will be authorized to view a certain classification level. All access must be configured to authorize only the data each user needs for their specific position or business role. Every user must be authorized to access Grupo CSI's systems. Authorization pertains to the user's business role and will only be authorized when necessary to fulfill said role.

For employees who require access to confidential, sensitive or private information, the data access request process must be followed. First, all requests must be approved by the Information Security Department. Second, the user must file a completed Authorization Request Form. Any employee who requests access to data above their normal security clearance must follow this procedure, as well as provide documentation that reports their access source and access time limits.

This is the general workflow for requesting access to data:

1. User's manager requests authorization by submitting an Authorization Request Form.
2. User's manager must approve the request based on the employee's role. The manager must make note of any additional access requirements before handing the request off to the Information Security Department.
3. The Information Security Department will coordinate with relevant department managers to ensure that the user is qualified to access to their data.
4. The Information Security Department will then hand the request off to the System Administrator.

5. The SysAdmin will create the user's account and forward that information to the Human Resources Department. Human Resources will then include these credentials within the user's employee file.

Requirement 8 – User Identification and Authentication

8.1 – 8.2 Assign unique user IDs and require user authentication

Each authorized user will be given a unique account name. The user will create a secret password, and all Grupo CSI systems must authenticate via passwords.

8.3 Remote access authentication requirements

Grupo CSI employees or 3rd party vendors who require remote, network-level access originating from outside the physical network must be required to provide two-factor authentication. Two-factor authentication employs two of the three following authentication methods:

- Something you know (example: password or passphrase)
- Something you have (example: soft or hard tokens, smart card or valid *and* unique digital certificate installed on user's workstation)
- Something you are (example: biometric)

It is not acceptable to employ one of these methods twice. For example, requiring a user to enter two different passwords does not constitute two-factor authentication.

8.5 Password policy

User-level access must include authentication measures, such as a password. Non-authenticated user IDs, shared IDs, and group IDs are not permitted.

Each Grupo CSI system must employ an automated access control process. This process will:

- Delete inactive users after a period of 90 days.
- Authenticate every account (meaning all users, systems, and applications) with a password.
- Require passwords of at least 7 characters, which include a combination of both numbers and letters.
- Identify every user by their unique account name:
- Mandate that a user account will be locked out of the system after 6 failed attempts to connect. The account will remain locked until a Systems Administrator unlocks it.
- Require that new passwords not be the same as the previous four passwords. Passwords must be changed every 90 days.
- Require that the system disconnect a user after an idle time of 15 minutes.

While this process applies to the authentication of all system users, any customer utilizing a Grupo CSI system must also adhere to these requirements.

Individuals granted network access for the first time and individuals requesting a password reset must be granted a unique password that must be changed after first use. Furthermore, for all non face-to-face password-reset requests, the System Administrator must verify the user's identity.

Any Grupo CSI employees or vendors that have network access must have that access immediately revoked once their relationship with Grupo CSI is severed for whatever reason. Vendor user accounts should only be enabled when needed. Furthermore, vendor access (both remote access and local access) must be monitored.

Requirement 9 – Physical Security

9.1 Monitor physical access to sensitive areas

Physical access controls must be established to protect hard copy, printed materials and electronic media used to store any Grupo CSI information.

- Access to physical network jacks, wireless access points and handheld devices must be restricted.
- Sensitive areas must be monitored by security cameras. The data collected must be stored for at least 3 months.
- Relevant facility controls must monitor and/or restrict access to any systems that store or process Grupo CSI information.

9.2 – 9.4 Handling visitors and ID badges

It is mandatory for all Grupo CSI employees, contractors and visitors to clearly display their ID badges at all times. Employees should be watchful for unknown persons or fellow employees not displaying an ID badge.

The badge distribution area should be kept in a physically secure environment, and monitored by the Information Security Department.

The ID badge area, Grupo CSI datacenter and other restricted areas must display a Visitor Log. Anyone accessing these areas must complete an entry in the log, and include: Name, Date, Firm or Department, and the Name of the employee who authorized the access. This Visitor Log information must be stored for at least 3 months.

Upon facility entry and completion of the Visitor Log, the receptionist will provide visitors with an ID badge containing no assigned access privileges. This type of ID badge is noticeably different than a regular employee ID badge. The receptionist will issue an expiration date of no longer than 1 day for each visitor ID badge.

For access to certain areas, employees may request a visitor badge be authorized. This request must be made to the Information Security Department 1 day prior to the scheduled visitation. Unescorted physical access to areas containing cardholder data is prohibited.

At the end of the visit, the receptionist will recover the temporary ID badge.

As part of the new employee orientation, Human Resources will distribute an Authorization Request Form and notify the Information Security Department. The new employee's direct supervisor should sign the form and return it to the Information Security Department. Once received, the Information Security Department will either approve or deny the request for a new ID badge. If approved, the Information Security Department will create and distribute the ID badge to the new employee. Whenever an employee is terminated, the Information Security Department must immediately disable badge access for said employee. Human Resources will be responsible for recovering the ID badge from the terminated employee.

9.5 – 9.9 Store, inventory and secure media containing sensitive data securely

All electronic media storage devices or hard copy materials containing sensitive or confidential information must be sufficiently protected by adequate physical access controls. Facility controls, such as locks and key passes, must be used to limit ease of access to systems storing sensitive or confidential information. As part of an annual risk assessment, the Information Security Department will review the security of all storage locations to ensure sensitive data is adequately protected.

Hardcopy Media

Examples of hardcopy materials include paper reports, fax transmissions, receipts etc. Storage of these materials is subject to the following guidelines:

- Removal of hardcopy materials from Grupo CSI offices is prohibited.
- Removal of hardcopy materials from Grupo CSI data centers or computer rooms is prohibited without prior approval from the Information Security Department.
- Any hardcopy material containing consumer data (confidential or sensitive) must be stored only at approved Grupo CSI facilities/offices, and only for the minimum time necessary.
- Any hardcopy material containing confidential or sensitive material must be clearly labeled.
- All hardcopy media containing confidential or sensitive information must be securely stored in a locked container. Lockers, cabinets, storage bins and locked desks are acceptable, but must first be approved by the Information Security Department. These materials are never to be stored in an unlocked or insecure container.

Electronic Media

Examples of electronic media includes CDs, DVDs, floppy disks, hard disks, USB thumb drives, backup tapes, etc. Any electronic media devices that store confidential or sensitive information must follow these guidelines:

- Confidential or sensitive information must not be copied to removable storage devices without prior consent from the Information Security Department.
- With the exception of computer system backups, no electronic media is to be removed from Grupo CSI facilities without prior consent from the Information Security Department.
- Any electronic media containing consumer data (confidential or sensitive) must be stored only at approved Grupo CSI facilities/offices, and only for the minimum time necessary.
- Any electronic media containing confidential or sensitive material must be clearly labeled and stored in a secure fashion.
- Incoming or outgoing media devices are to be delivered only via secured courier or other method approved by the Information Security Department.

Media Inventory

Any storage devices utilized for archival or backup purposes must be retained in a secure environment. Only Grupo CSI personnel and the contracted storage facility personnel should have access to the storage devices.

A Media Inventory Log must be kept in the same storage location as all hardcopy and electronic media used for data backups. On an annual basis, an inventory of all stored media and devices will be performed. Utilizing the Media Inventory Log, the Information Security Department will compare the list of in-use media with records kept at the approved storage facility.

A member of the Information Security Department must perform an annual inspection of this backup storage facility to ensure that the backups are secured and stored in a fireproof manner This check will ensure that all security controls are in place and operational.

A unique tracking code must be applied to any storage vessel or shipping container used for transporting backup media with sensitive or confidential information. These devices must be registered with the Information Security Department prior to the transfer.

Any storage device containing sensitive or confidential data must be identified as such prior to the transfer.

The Information Security Department must pre-approve potential media couriers and transport personnel.

During all media transfers, the personnel responsible will complete a Backup Media Transfer Log. The log must clearly indicate what media has been transferred, and by whom. The log must also include where the media is being transferred to, and a manager of the approved storage facility must sign the log upon receipt.

9.10 Data disposal policy

After sensitive or confidential data is no longer required for legal, regulatory or business needs it must be purged from Grupo CSI systems using a method described within this policy. This policy pertains to all data either stored in Grupo CSI systems, within temporary files or stored on external devices/drives.

All marked shred bins (for hardcopy materials) must be locked prior to shredding. Grupo CSI employees should cross-cut shred any hardcopy material containing confidential or sensitive information as soon as possible.

The Information Security Department must establish an automatic deletion process to be executed on cardholder information systems. This automatic process will occur on a nightly basis, and will remove any sensitive or confidential data that is no longer required or has exceeded its usefulness.

Data stored in files or directories containing reusable information must be removed using a wiping program approved by the Information Security Department.

External media storage devices containing confidential or sensitive data must be disposed of in a secure manner. This includes:

- **Hard Disks**: Perform a 7-pass binary wipe, degauss, or shred platter.
- **Floppy Disks**: Incinerate, shred, or melt.
- **Tape storage**: Degauss, incinerate, shred, or melt.
- **USB drives** (thumb drives), smart cards and digital media: Incinerate, or melt.
- **CDs and DVDs**: Destroy surface, incinerate, shred, or melt.

All confidential or sensitive data must be deleted or otherwise destroyed prior to any Grupo CSI computer equipment being shipped to a repair facility or other vendor for sale or trade-in.

Floppy drives, optical disks or other removable computer storage devices may not be donated to charity or recycled.

In the event that Grupo CSI outsources the disposal of media or computer equipment, only a bonded Disposal Vendor may be used. The vendor must provide a Certificate of Destruction to Grupo CSI.

Requirement 10 – Logging and Auditing

10.2 Events Logged

In order to reconstruct the following events, all system components must have an automated audit trail implemented.

- Invalid logical access attempts.
- All user access to cardholder data.
- Creation or deletion of system-level objects.
- All administrative actions utilizing user IDs with access above-and-beyond that of a general user (e.g., root, oracle, Admin group privilege).
- Access or initialization of audit log files.
- Any user or admin authentication attempts (either valid or invalid).

10.3 Event Log Structure

All system access event logs must contain the following minimum information:

- Name of the affected data, system component or resource.
- User ID.
- Origination location of event.
- Type of event.
- Date and Time that event occurred.
- Result of the event.

10.4 Network Time Protocol (NTP)

All Grupo CSI production systems, with the exception of Grupo CSI's internal NTP servers, must be configured to utilize the internal NTP server for time synchronization purposes.

Grupo CSI's internal NTP server will access time updates from the website "time.nist.gov". Access Control Lists (ACL) must be configured to limit those client systems allowed to retrieve time settings from the internal NTP server. The internal NTP system must, at all times, be running the latest version of the software.

10.5 Log Security

All event logs must be securely stored in a centralized location or on a storage device that is protected from unauthorized access. The logs will only be accessed and viewed on a "need to know" basis. Wireless logs must be copied onto a log server housed on the internal LAN. Furthermore, the Information Security Department must establish a file integrity monitoring (FIM) system that will alert personnel in the event either unauthorized access to logs or modification of logs occurs.

Logs must be retained for a minimum of one year with three months immediately available for analysis. If logs are archived on removable media and stored at an offsite location, attention should be paid to ensure that the most recent three months are kept onsite so that they can be readily analyzed should a security event occur.

Requirement 11 – Regularly Test Security Systems and Processes

11.1 Scan for rogue wireless devices

At least quarterly, the Information Security Department must scan for the presence of unauthorized wireless access points installed on the [Merchant DBA] network. Grupo CSI approved network analysis software must be used. Examples of acceptable software include BSD Airtools, Kismet, and Wireshark.

If an unauthorized wireless access point (example: wireless router or a wireless card installed on a server) is discovered, the incident response plan must be invoked. Rogue wireless devices are classified as a Level 2 severity under the Grupo CSI incident response plan.

11.2 Vulnerability Scans

On a quarterly basis, or after any significant change in the network, the Information Security Department must conduct internal network vulnerability scans. Significant changes might include firewall rule modifications, product upgrades, system component installations or changes in network topography.

ONLY a PCI ASV scan vendor is authorized to perform external network vulnerability scans. These ASV scans must occur, at a minimum, on a quarterly basis.

If vulnerability scans uncover potential vulnerabilities, the appropriate Grupo CSI personnel must be notified so remediation efforts may begin. Personnel must follow the Change Control Policy to correct high-level vulnerabilities. Additional scans must then be performed in order to confirm compliance with Grupo CSI security standards.

11.3 Vulnerability Penetration Testing

On an annual basis, or after any significant change to the network or after a significant application upgrade or modification, network and application layer penetration testing must be performed. Grupo CSI will utilize a 3rd party IT security firm for all penetration testing unless approval is granted by senior management to allow a qualified internal resource with organizational independence to perform the penetration testing.

Network layer penetration tests must include all components that support network functions and Operating Systems. In addition, testing must include internally and externally accessible IP's.

Application layer penetration tests must be performed internally and externally. At a minimum, testing must consider the top 10 OWASP vulnerabilities. These vulnerabilities are available at the following website:

http://www.owasp.org

During application layer penetration testing, the following vulnerabilities must be checked:

- Insecure Configuration Management
- Unvalidated Input
- Denial of Service

- Malicious Use of User IDs
- Insecure Storage
- Malicious Use of Account Credentials and Session Cookies
- Error Handling Flaws
- Cross-site Scripting
- SQL Injection and other Command Injection Flaws
- Buffer Overflows

If vulnerability penetration tests uncover potential vulnerabilities, the appropriate Grupo CSI personnel must be notified so remediation efforts may begin. Personnel must follow the Change Control Policy to correct high-level vulnerabilities. Additional scans must then be performed in order to confirm compliance with Grupo CSI security standards.

11.4 Use Intrusion Detection Systems (IDS's) and/or Intrusion Prevention Systems (IPS's)

An intrusion detection and/or prevention system must be installed, updated and configured per vendor guidelines to monitor all Grupo CSI networks and systems that fall within the payment card system scope. An IDS or IPS should be located at the perimeter (example: at the choke router) of the network zone where cardholder data is stored, processed and/or transmitted. In addition, an IDS/IPS should be located at any critical points within this trusted network zone. An example of a critical point would be a server containing a database where cardholder data is stored.

Any IDS/IPS systems must be configured to alert security personnel if an intrusion is detected. Security personnel will review the alert and determine if it is a false positive or a malicious event. If a malicious network intrusion is confirmed, security personnel must invoke the appropriate incident response plan.

Requirement 12 – Maintain an Information Security Policy

12.1 Establish, publish, maintain and disseminate an information security policy

The Information Security Department shall be responsible for maintaining the information security policy and ensuring that all personnel and relevant third parties receive a copy.

All users must read and understand Grupo CSI's Information Security Policies and Procedures document. By signing the Security Acknowledgement and Acceptable Use Policy, the user is declaring an understanding of policy prior to accessing Grupo CSI's network systems.

On an annual basis, the Chief Security Officer must ensure Grupo CSI data assets are sufficiently protected by coordinating a formal risk assessment. This assessment will identify any existing or new vulnerabilities. The information security policy will be updated as necessary to reflect any findings from the risk assessment.

12.3 Special technology use policy

Policy Applicability

This policy must be followed by all users of special Grupo CSI technologies, whether employees, contractors or third parties. Exemptions may only be authorized with written approval from the Chief Security Officer.

"Special technologies" refers to wireless networks, modem use and access, and any other employee-facing technologies used within the Grupo CSI computing environment. This particular policy will be updated in the future to reflect new special technologies and their intended uses.

Approval

Integration or use of special technologies must be authorized by the Information Security Department, based on job function. In regards to the general user, this applies to dial-in modem access, personal modem deployment, and wireless network access. Approvals must be documented in the Authorization Request Form.

Authentication

Wherever possible, user authentication mechanisms must be incorporated into Grupo CSI authentication systems. User authentication requirements must adhere to the strict policies and procedures as currently defined for passwords (complex passwords, password change process, etc.).

A strong two-factor authentication scheme (approved by the Information Security Department) must be used if a user is remotely accessing the Grupo CSI network using special technologies.

Device Inventory

The Information Security Department must pre-approve personal modems and wireless network interfaces and log these devices using the Special Technologies Device Inventory. Users of these technologies must also be approved by the Information Security Department, and noted on the Special Technologies User List. The following users must be documented:

- Vendors with dial-in modem access.
- Employees with dial-in modem access.

- Personal modem users.
- Wireless network users.

Device Identification
Each of these approved devices, including personal modems and wireless access points, must be labeled with the device owner, contact information and the device's purpose/business function.

Acceptable Use
The guidelines and restrictions listed in the Security Awareness and Acceptable Use Policy also apply to the acceptable use of Grupo CSI special technologies.

Permitted Locations
The placement/installation of wireless access points and dial-in modems must be authorized by the Information Security Department. Dial-in modems should be maintained in a location where they are free from tampering. Wireless access devices should be installed in the ceiling plenum. The use of these devices must be logged in the Special Technologies Device Inventory and the Special Technologies User List.

Approved Products
The Information Security Department must approve devices before they are installed onto the Grupo CSI network. The use of approved devices must be logged in the Special Technologies Device Inventory and the Special Technologies User List.

Session Disconnect
Modems (dial-in or modem banks) must be configured to automatically disconnect a user after 30 minutes of inactivity.

Vendor Connections
Any modem used solely by a third party vendor for maintenance or support must remain disconnected until required. The Information Security Department must approve the activation of these modems, or create a management procedure to handle the task. The modem must be disabled immediately upon completion of the task.

Credit Card Data Access
Special precautions must be taken to ensure the security of credit card data made available through a remote dial-in modem. It is forbidden to store cardholder data on local hard drives, floppy disks or other external storage media. During a connected session, the remote PC's cut/paste and Print functions must be disabled.

12.2, 12.4 – 12.5 Information security roles and responsibilities
Role of Chief Security Officer
The responsibilities of Grupo CSI's Chief Security Officer includes enforcing these policies and procedures, and working closely with the Chief Information Officer and business unit managers to identify additional areas of concern. Once identified, the Chief Security Officer works with Grupo CSI's management to coordinate the repairs or changes as needed.

Further responsibilities of the CSO include:

- An annual review of the Information Security policies and procedures document.

- This annual review helps to maintain the accuracy of the document and addresses any new or perceived threats.
- Performing an annual risk assessment that will identify new threats or vulnerabilities.
- Ensuring all third party vendors that stores or handles Grupo CSI's data assets is contractually obligated to comply with PCI DSS requirements. In addition, any connections to the third party vendors must be managed per the PCI DSS requirements.

Information Security Department Responsibilities

In order to successfully secure Grupo CSI's information systems, all departments must adhere to a consistent vision for information security. This challenge is met through the creation of an Information Security Department, which works with managers of each department to develop the standards, which will protect Grupo CSI assets.

The three main areas of focus for an Information Security Department are security awareness, education, and security planning.

More specific responsibilities include:

- Reviewing the policies and procedures annually. Creating and/or updating the Information Security Policies and Procedures Document as necessary.
- Restricting access to sensitive areas.
- Distributing and updating incident response plans and escalation procedures.
- Implementing/coordinating Information Security Policies when and were appropriate.
- Monitoring for security alerts and informing Grupo CSI management and other security personnel.
- Reviewing security logs on a daily basis, and reporting any discrepancies.

The Information Security Department approves user access based on the roles of each user. Any requests for network access must contain an approval (either written or in electronic form) from the Information Security Department.

Guided by a specific business unit's management, the Information Security Department will determine a user's access level based on their responsibilities and needs.

In order to determine that all access privileges are up-to-date and accurate, the Information Security Department will perform a bi-annual audit of all network authorizations by validating access rights for sample user populations. If access cannot be determined based on a defined business role, additional approvals must be collected by the Information Security Department before access is authorized. Contractor accounts, or any other extension authorizations, must also go through the Information Security Department.

In the event that access must be granted to correct an issue or resolve some other network problem, the Information Security Department may issue an Emergency ID. That process goes as follows:

- An Emergency ID request must be made through the Information Security Department, who will then notify all relevant departments and the proper System Administrator.
- Once work has been completed, the user must notify the Information Security Department so they can disable the ID.
- To avoid delaying access, an Emergency ID Request Form must be completed as soon as possible and filed by the Information Security Department.

System Administrator Responsibilities

Representing the direct link between Grupo CSI policies and the network, Grupo CSI System Administrators are vital to the upkeep of information security.

Their prime responsibilities include:

- Restricting physical access to wireless hot spots, network jacks, hand held devices and other network gateways.
- Managing user accounts and the authentication process.
- Applying Grupo CSI policies and procedures when and where appropriate.
- Assisting the Information Security Department in analyzing and controlling access to Grupo CSI data.

Additional areas of responsibility include:
Any requests for access must clearly state the role of the user and how that role is associated to the desired level of access. Any new accounts that are created by mirroring an existing user account are required to be audited against the request or roles determined to be appropriate for access.

A user's identity must be verified before any password resets are allowed by mail, telephone, or email.

When the System Administrator receives notice that access has been revoked, that access should immediately be disabled. To ensure that access for a terminated employee is revoked right away, written procedures should be in place. The System Administrator should suspend any users who are on an extended leave of absence or long-term disability. This employee status information can be validated by utilizing Grupo CSI's Human Resources systems.

After 60 days of inactivity, a User ID should be disabled. After 90 days of inactivity, the User ID should be removed from the system. Certain IDs, such as NT Admin or root, are exempt from this policy but require the System Administrator to file a written waiver with the Information Security Department. The waiver will include documentation detailing compensating controls around access to the accounts in question.

Any network or computer resource that is capable of displaying a sign-in message must display the following text at some point during the login process:

```
This system is for the use of authorized users only. Individuals
using this computer system without authority, or in excess of
their authority, are subject to having all of their activities on
this system monitored and recorded by system personnel. In the
course of monitoring individuals improperly using this system, or
in the course of system maintenance, the activities of authorized
users may also be monitored. Anyone using this system expressly
consents to such monitoring and is advised that if such monitoring
reveals possible criminal activity, system personnel may provide
the evidence of such monitoring to law enforcement officials.
```

- Audit logs must be enabled to record user activities (including administration). These audit logs must be stored for a minimum of one year, plus 90 days of online viewing availability.

- The user must change any passwords set up by the System Administrator during their first login. System Administrator passwords must also be unique and follow the password policy.
- Prior to performing a password reset, the System Administrator must validate the identity of the requester.
- Any authorized contractor accounts should be set to expire at the end of the contract. Any necessary extensions may be requested through the Information Security Department. These temporary accounts should be monitored carefully.
- Accounts for terminated employees and users who no longer have a need for their level of access should immediately be disabled.
- When Grupo CSI does business with a remote vendor, their access to the system should only be authorized when needed to perform remote functions.
- Ensure authentication for access to all systems, with a focus on access to databases containing cardholder or other highly sensitive data.

Human Resources

The Human Resources Department plays an important role in Grupo CSI's information security. This is due to their direct relationship with employees (both current and former).

As related to information security, the following duties are the responsibility of Human Resources:

- Distribute this Information Security Policies and Procedures Document to all Grupo CSI employees, contractors, vendors and partners.
- Work with the Information Security Department to formulate sanctions and other disciplinary actions involving violations of security policies.
- Work with the Information Security Department to distribute security information awareness and education materials to employees.
- Perform background checks on those employees with access to network systems and critical data. Checks include background, criminal, pre-employment, credit history and references.
- Coordinate employee terminations with Access Management personnel.

Users

All users of Grupo CSI resources, computers and network systems must understand the importance of information security. In doing so, they will recognize their own crucial role in safeguarding critical data and maintaining Grupo CSI systems.

These specific responsibilities apply to all Grupo CSI information system users:

- Assist Grupo CSI in meeting its business goals by understanding that their actions have real consequences. Users must act accordingly, especially when it pertains to information security policy.
- Avoid distributing classified or sensitive information.
- Maintain an understanding of current information security policies.

12.6 Security awareness program

The Grupo CSI Chief Security Officer will oversee and the Information Security Department will execute security awareness training for all Grupo CSI personnel. Initial training must be provided for personnel upon hire and periodic refresher training must occur annually at a minimum. The method of delivery as well as the topics can vary depending upon the audience. The Information

Security Department will determine and approve training methods and topics. Where training is performed in a group setting, a sign-in sheet will be circulated for attendees to record their attendance. The Human Resources department will maintain a record of sign-in sheets.

12.7 Employee background checks

New hire candidates for positions requiring access to sensitive systems and applications involving credit card data, a background check will be ordered by the Human Resources Department.

12.8 Third-party information sharing – due care and due diligence

The Information Security Department shall maintain a list of service providers with whom Grupo CSI shares credit card data. Grupo CSI must exercise due care in maintaining written agreements between Grupo CSI and any service providers. Such agreements must include language where the service provider acknowledges their responsibility to secure credit card data where they are involved in the storing, processing and/or transmitting of this data.

In addition, Grupo CSI must exercise due diligence prior to engaging service providers. Service providers should be vetted thoroughly prior to establishing a formal relationship. Part of this process should include checking references and professional accreditations. Preference will be given to service providers who have undergone and passed the rigors of a PCI DSS Level One Audit. Once a service provider is engaged, Grupo CSI must monitor the service providers' PCI DSS compliance status annually. This process will require Grupo CSI to request a copy of the service providers' Attestation of Compliance on an annual basis.

12.9 Incident response plan

Incident Identification

Employees share the responsibility of detecting and reporting security incidents. It is mandatory for all employees to assist the incident response procedures by managing their personal area of responsibility. The types of security incidents that an employee might likely encounter in their daily work routine includes:

- Security event notifications (e.g., natural disaster alerts, file integrity alerts, intrusion detection alarms, physical security alarms).
- Fraud, such as inaccurate database information or inaccurate logs/records.
- Theft or unauthorized access (e.g., surveillance/CCTV evidence of a break-in, missing items, unauthorized logins, broken locks).
- Unusual system behavior, such as unscheduled system reboots or abnormal errors in system log files/terminals).

Every employee should possess a working knowledge of these possible incident identifiers, as well as the appropriate team member to notify. All employees must report incidents per the guidelines in 14.3 (Reporting and Incident Declaration Procedures), unless they are otherwise occupied with a separate aspect of the incident response plan.

Reporting and Incident Declaration Procedures

When an employee reports a possible incident, the Information Security Department should be notified – especially if it deals with a critical component of Grupo CSI's business environment. The Information Security Department can best assess whether a reported issue is really a security incident or not.

To maintain the integrity of both the incident investigation and recovery process, the Information Security Department's personnel should be the sole investigating and remediating agent. However,

when a possible security incident is noticed the employee should do the following as soon as possible:

- If the possible security incident involves a Grupo CSI computer system:
  - DO NOT alter or modify the computer system. The computer should be left powered on, with all software/programs left running.
  - DO NOT power down or restart the computer.
  - IMMEDIATELY disconnect the Ethernet/network connector from the back of the computer (if applicable).
- Report the Incident:
  - Contact the Information Security Department and report the incident.
  - DO NOT communicate this incident to other employees, with the exception of supervisors and the Information Security Department.
  - DO NOT contact the police. If necessary, communication with law enforcement will be coordinated by the Information Security Department.
  - While waiting for the investigation to begin, employees should document any pertinent information that will aid in responding to the matter. The documentation should include date, time, and the nature of the incident.

Incident Severity Classification

After a possible security incident is reported, the Information Security Department must determine if the incident requires a formal response.

For incidents that do not require a formal response, the Information Security Department will notify the appropriate IT personnel who will perform any necessary support services that may be necessary.

The Information Security Department should determine the appropriate response based on the following:

- **Level 1**: This level corresponds with ONE instance of potentially hazardous activity, such as an unexpected performance peak, unauthorized telnet, or corrected virus detection.
- **Level 2**: This level corresponds with either a second Level 1 attack, or ONE instance of an obvious attempt to access unauthorized information/systems. This could be an attempted download of password files/credentials, attempt to access a restricted area or unauthorized vulnerability scan.
- **Level 3**: This level corresponds with either a second Level 2 attack or an actual security breach (or serious attempt). Denial of service attacks, multi-pronged attacks, virus infections of a critical system, broken locks, stolen documents, successful unauthorized access to critical systems are all Level 3 incidents.

Note: A Level 1-type attack that focuses on systems storing sensitive or confidential information should be classified as Level 2.

Typical Response

The stages of a typical response are: identification, severity classification, containment, eradication, recovery, and an analysis of the root cause. Finally, an overall improvement of security controls should transpire as a result of the findings. Once an incident has been identified and classified, the Information Security Department will be responsible to take the following actions:

Level 1

Contain the Incident and Monitor for Changes.

1. Whenever possible, document the user, IP address and domain of intruder.
2. Block the intruder's access via approved technology controls.
3. Monitor for future breach attempts originating from the documented user or IP address.

Level 2

Contain the Incident, Monitor for Changes and Warn Others.

1. Document and securely store any information associated with the incident.
2. Block the intruder's access via approved technology controls.
3. Attempt to track down the connection's origin.
4. If possible, contact the ISP and gather information regarding the incident or suspected intruder.
5. Perform research as to the possible ramifications surrounding the chosen method of attack. If applicable, re-evaluate and re-classify the severity level rating (adhering to the Level 3 guidelines for containment, eradication and recovery).
6. Once the source is identified, notify the malicious user that Grupo CSI has knowledge of their activities. Warn them of future recriminations if another attempt is ever made. If a Grupo CSI employee is found to be the culprit, management should work with Human Resources to appropriately address the Acceptable Use violation.

Level 3

Contain the Incident, Eradicate the Issue, Recover and perform Root Cause Analysis.

1. For any incident involving cardholder data or systems, a notification must be issued to the Acquirer and any related card associations.
2. Contain the incident/intruder by unplugging the network cables, applying restrictive ACLs, deactivating the user's ID, isolating the switch port, or terminating the user's session and ability to change passwords.
3. Document and securely store any information associated with the incident via offline methods. If necessary, the Information Security Department will work with legal and Grupo CSI management to employ forensic specialists.
4. Continually update management on the progress of each step.
5. Delete or eliminate the intruder's access path and any associated vulnerabilities.
6. Perform research to determine the connection's origin.
7. If possible, contact the ISP and gather information regarding the incident or suspected intruder.
8. Perform research as to the possible ramifications surrounding the chosen method of attack.

Credit Card Companies – Special Response

The Information Security Department must follow this procedure for any security incident that involves a potential compromise of credit card information or personal cardholder data.

1. The Information Security Department must first contain and/or eliminate the threat and avoid further exposure. A thorough investigation into the security breach must be performed within 24 hours of the incident. These steps should be taken to assist the investigation:

a. Document all steps/actions taken.
b. During the transfer of any materials or information related to the investigation, employees must utilize chain of custody techniques.
c. Do not log on to the affected systems, change any passwords or otherwise access/alter the systems. Do not log on as ROOT.
d. Do not turn the affected system off. It is important to isolate any compromised systems from the network. Isolation can be achieved by unplugging the network cable, deactivating switch ports or isolating the system to a contained environment (e.g., isolated VLAN). Disaster Recovery/Business Continuity procedures should be used to recover any lost or disabled business processes.
e. Archive or store all logs and other electronic evidence.
f. Change the wireless network SSID on the AP and other non-compromised machines (if applicable).
g. Maintain vigilant to any additional threats and monitor all cardholder information systems.

2. Alert all relevant parties. The following should be notified:
   a. U.S. Secret Service (if VISA payment data has been compromised).
   b. Local FBI Office.
   c. Merchant Bank.
   d. If not already involved, the Incident Response and Forensic Teams.
3. Specific cards have additional procedures. Follow these procedures for any cards that Grupo CSI accepts:

Visa
Within 10 business days, the VISA Fraud Control Group must be provided with all the compromised VISA accounts. The VISA Fraud Control Group will advise on how to securely transmit any account numbers. For assistance, call (650) 432-2978. VISA will distribute the compromised account details to issuers and will ensure the continued confidentiality of non-public and entity information.

Mastercard
Contact Grupo CSI's merchant bank to obtain details on how to handle a compromise involving Mastercard cardholder data. The merchant bank can assist with contacting Mastercard at (636) 722-4100.

American Express
Contact Grupo CSI's American Express representative or call 1-800-528-4800.

Discover Card
Contact Grupo CSI's Discover Card representative or call 1-800-347-3083.

JCB
Contact Grupo CSI's JCB representative or call 1-213-896-3718.

Root Cause Analysis and Lessons Learned

To determine the root cause of the security incident, the Information Security Department and all affected departments/employees will meet within one week of the incident to review results of the investigation. During this review, the effectiveness of the Incident Response Plan will be evaluated. Additionally, security controls will be reviewed to determine their effectiveness. Updates to the Incident Response Plan, security controls and other policies and procedures will be made accordingly.

Plan Testing and Training

On an annual basis, the current plan will be tested by means of a "mock incident." The Information Security Department will facilitate and plan the incident at their discretion. All procedures outlined above must be followed, including the follow-up session. This test will involve any and all Grupo CSI employees who have an active role in the Incident Response Plan.

Automated Security System Notifications

Automated intrusion detection systems, such as detection sensors and file integrity monitoring (FIM) systems, should be configured to automatically alert the Information Security Department of any potential threats. FIM solutions should be used to protect logs as well as any system-level objects. System-level objects are anything on a system component that is required for its operation, including but not limited to application executable and configuration files, system configuration files, static and shared libraries and DLL's, system executables, device drivers and device configuration files and added third-party components.

One Information Security Department Engineer must be "on call" 24 hours a day to respond and initiate the Incident Response Plan.