EDUARDO CABIDE LLC

Information Security Policies and Procedures

0. REVISION HISTORY 1
1. INTRODUCTION AND SCOPE 7
1.1. Introduction 7
1.2. Regulatory Compliance 7
1.3. Scope of Compliance 7
2. POLICY ROLES AND RESPONSIBILITIES 8
2.1. Policy Applicability 8
2.2. Role of Chief Technical Officer 8
2.3. Information Security Team 11
2.4. System Administrators 12
2.5. Users 12
3. IT CHANGE CONTROL POLICY 13
3.1. Policy Applicability 13
3.2. Change Request Submittal 13
3.3. Change Request Approval 14
3.4. Change Testing 14
3.5. Change Implementation 15
4. DATA CLASSIFICATION AND CONTROL POLICY 15
4.1. Policy Applicability 15
4.2. Data Classification 15
4.3. Data Access 17
4.4. Physical Security 18
4.5. User Authentication 19
4.6. Account and Access Management 22
5. DATA RETENTION AND DISPOSAL POLICY 25
5.1. Policy Applicability 25
5.2. Retention Requirements 25

5.3. Disposal Requirements 27
5.4. Disposal Process 27
6. PAPER AND ELECTRONIC MEDIA POLICIES 29
6.1. Policy Applicability 29
6.2. Storage 29
6.3. Inventory 32
6.4. Destruction 32
7. FIREWALL AND ROUTER SECURITY ADMINISTRATION POLICY 33
7.1. Policy Applicability 33
7.2. Device Management Responsibilities 33
7.3. Firewall, Router and Network Configuration Changes 34
7.4. Allowed Services 35
7.5. Allowed Network Connection Paths and Configuration Requirements 36
7.6. Configuration Review 37
7.7. Personal Firewalls 37
8. SYSTEM CONFIGURATION POLICY 38
8.1. Policy Applicability 38
8.2. System Build and Deployment 38
8.3. Vulnerability Identification and System Updates 44
9. ANTI-VIRUS POLICY 48
9.1. Software Configuration 48
9.2. Signature Updates 49
9.3. Software Logging 49
10. BACKUP POLICY 50
10.1. Location 50
10.2. Transport 50
10.3. Audit 51

11. ENCRYPTION POLICY 52
11.1. Policy applicability 52
11.2. Encryption Key Management 52
12. SPECIAL TECHNOLOGIES USAGE POLICY 57
12.1. Policy Applicability 57
12.2. Approval 57
12.3. Authentication 57
12.4. Device Inventory 58
12.5. Device Identification 58
12.6. Acceptable Use 59
12.7. Permitted Locations 59
12.8. Approved Products 59
13. SOFTWARE DEVELOPMENT POLICY 61
13.1. Development Environment 61
13.2. Secure Software Development Procedures 62
14. INCIDENT RESPONSE PLAN AND PROCEDURES 67
14.1. Incident Identification 67
14.2. Reporting and Incident Declaration Procedures 67
14.3. Incident Severity Classification 68
14.4. Incident Response 69
14.5. Plan Testing and Training 73
14.6. Automated Security System Notifications 74
15. EMPLOYEE IDENTIFICATION POLICY 74
15.1. Employee Requirements 74
15.2. Facilities 74
16. LOGGING CONTROLS POLICY 75
16.1. Events Logged 75

16.2. Event Log Structure 76
16.3. Log Security 77
Appendix A – Security Awareness and Acceptable Use Policy 78
Appendix B – Authorization Request Form 83
Appendix C – Change Request Form **Error! Bookmark not defined.**
Appendix D – Media Inventory Log **Error! Bookmark not defined.**
Appendix E – Permitted Network Services and Protocols **Error! Bookmark not defined.**
Appendix F – System Configuration Standards **Error! Bookmark not defined.**
F.1 Windows Systems **Error! Bookmark not defined.**
F.2 UNIX Systems **Error! Bookmark not defined.**
F.3 Network Devices **Error! Bookmark not defined.**
Appendix G – System Configuration Record **Error! Bookmark not defined.**
Appendix H – Backup Media Transfer Log **Error! Bookmark not defined.**
Appendix I – Encryption Key Custodianship Form **Error! Bookmark not defined.**
Appendix J – Encryption Key Management Log **Error! Bookmark not defined.**
Appendix K – Special Technologies Device Inventory **Error! Bookmark not defined.**
Appendix L – Special Technologies User List **Error! Bookmark not defined.**
Appendix M – Periodic Operational Security Procedures **Error! Bookmark not defined.**
Appendix N – MANAGEMENT of connected entities **Error! Bookmark not defined.**
N.1 Connection Standards **Error! Bookmark not defined.**
N.2 Connection Process **Error! Bookmark not defined.**
Appendix O: MANAGEMENT OF CONNECTED ENTITIES FORM **Error! Bookmark not defined.**
Appendix P: NEW EMPLOYEE CARD **Error! Bookmark not defined.**

0. REVISION HISTORY

Changes	By	Date
<<Add change description>>	<<Add change author>>	<<Add change date>>

0. INTRODUCTION AND SCOPE

0.1. Introduction

This document explains EDUARDO CABIDE LLC’s information security requirements for all employees.

EDUARDO CABIDE LLC’s management has committed to these policies to protect information utilized by

EDUARDO CABOODE LLC in attaining its business goals. All employees are required to adhere to the policies described within this document.

0.2. Regulatory Compliance

The Payment Card Industry Data Security Standard (PCI DSS) Program is a mandated set of security standards that were created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding credit cardholder information for all credit card brands.

In September of 2006, a group of five leading payment brands including American Express,

Discover Financial Services, JCB, MasterCard Worldwide and Visa International jointly announced formation of the PCI Security Standards Council, an independent council established to manage ongoing evolution of the PCI standard. Concurrent with the announcement, the council released version 1.1 of the PCI standard.

PCI DSS requirements apply to organizations where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their Cardholder Data Environment (CDE). Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party by the applicable PCI DSS requirements.

During the normal course of compliance and reporting activities EDUARDO CABIDE LLC will ensure that proper scoping of compliant PCI operations and reporting are in effect.

0.3. Scope of Compliance

This Information Security Policy applies to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication

data. “System components” include network devices, servers, computing devices, and applications. Examples of system components include but are not limited to the following:

- Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- Applications include all purchased and custom applications, including internal and external (for example, Internet) applications.
- Any other component or device located within or connected to the CDE.
- Support systems (e.g. Active Directory, PC’s performing support functions such as system administration, etc.)

1. POLICY ROLES AND RESPONSIBILITIES

1.1. Policy Applicability

All employees, contractors, vendors and third parties that use, maintain or handle EDUARDO CABIDE LLC information assets must follow this policy.

1.2. Role of Chief Technical Officer

The Chief Technical Officer is responsible for coordinating and overseeing EDUARDO CABIDE LLC’s compliance with policies and procedures regarding the confidentiality, integrity and security of its information assets.

The Chief Technical Officer will work closely with the other EDUARDO CABIDE LLC managers and staff involved in securing the company’s information assets to enforce established policies, identify areas of concern, and implement appropriate changes as needed. Specific responsibilities of the

Chief Technical Officer include:

- Make high-level decisions pertaining to the information security policies and their content. Approve exceptions to these policies in advance on a case-by-case basis.
- On an annual basis, coordinate a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks
- At least annually review the Information Security policies and procedures to maintain adequacy considering emergent business requirements or security threats.
- Make sure that third parties, with whom company information is shared, are contractually required to adhere to the PCI DSS requirements and to acknowledge that they are responsible for the security of the company information which they process.
- Assure that connections to third parties are managed by PCI requirements via the relationship procedures described in Management of Connected Entities (Appendix O)
- Complete tasks as required by the Periodic Operational Security Procedures (Appendix N).
- Disseminating EDUARDO CABIDE LLC information security policies and acceptable use guidance, and other user policies to all relevant system users, including vendors, contractors and business partners.
- Ensure background checks are carried out on potential employees who will have access to systems, networks, or data, for example background, pre-employment, criminal, or reference checks.
- Work with the Information Security Team on disseminating security awareness information to system users.
- Work with the Information Security Team to administer sanctions and disciplinary action relative to violations of Information Security Policy.
- Notify Access Management personnel when any employee is terminated Maintain all Security Awareness and Acceptable Use (Appendix A) and Authorization Request Forms (Appendix B) in employee files.

PCI Requirements Reference:

2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.

12.1.1 The information security policy is reviewed at least annually and updated as the environment changes.

12.4 Ensure the security policy and procedures clearly define information security responsibilities for all personnel.

Audit Procedure 12.5 Examine information security policies and procedures to verify:

- The formal assignment of information security to a Chief Security Officer (Note that for EDUARDO CABIDE LLC the Chief Security Officer's role will be carried out by the Chief Technical Officer) or other security-knowledgeable member of management.

- The following information security responsibilities are specifically and formally assigned.

12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:

12.8.1 Maintain a list of service providers including a description of the service provided.

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:

12.8.1 Maintain a list of service providers including a description of the service provided.

12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.

12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.

12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

8.1.3 Immediately revoke access for any terminated users

12.5.1 Creating and distributing security policies and procedures is formally assigned.

12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

12.6.1 Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions).

12.7 Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment.

1.3. Information Security Team

Successfully securing EDUARDO CABIDE LLC information systems requires that the various individuals and groups consistently adhere to a shared vision for security. The Information Security Team works with system managers, administrators and users to develop security policies, standards and procedures to help protect the assets of EDUARDO CABIDE LLC.

The Information Security Team is dedicated to security planning, education and awareness. Specific responsibilities of the Information Security Team:

- Create new information, security policies and procedures when needs arise. Maintain and update existing information security policies and procedures. Review the policy on an annual basis and assist management with the approval process.
- Act as a central coordinating department for implementation of the Information Security Policies.
- Maintain and distribute incident response and escalation procedures.
- Monitor and analyze security alerts and distribute information to appropriate information security, technical and business unit management personnel.
- Review logs daily. Follow up on any exceptions identified.
- Restrict and monitor access to sensitive areas. Ensure appropriate physical controls are in place where sensitive cardholder information is present.
- Complete tasks as required by the Periodic Operational Security Procedures (Appendix N).

PCI Requirements Reference:

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.

12.2 Develop daily operational security procedures that are consistent with requirements in this specification (e.g., user account maintenance procedures, log review procedures)

12.5 Assign to an individual or team the following information security management responsibilities:

12.5.1 Establish, document, and distribute security policies and procedures.

12.5.2 Monitor and analyze security alerts and information and distribute to appropriate personnel.

12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.

12.5.4 Administer user accounts, including additions, deletions, and modifications.

12.5.5 Monitor and control all access to data.

1.4. System Administrators

EDUARDO CABIDE LLC System Administrators are the direct link between information security policies and the network, systems and data. System Administrator responsibilities include:

- Applying EDUARDO CABIDE LLC information security policies and procedures as applicable to all information assets.
- Administering user account and authentication management.
- Assisting the Information Security Team with monitoring and controlling all access to EDUARDO CABIDE LLC data.
- Maintain an up-to-date network diagram including wireless networks.
- Restrict physical access to publicly accessible network jacks, wireless access points, gateways and handheld devices.
- Completing tasks as required by Periodic Operational Security Procedures (Appendix N).

PCI Requirements Reference:

1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks

12.5.4 Administer user accounts, including additions, deletions, and modifications.

12.5.5 Monitor and control all access to data.

1.5. Users

Each user of EDUARDO CABIDE LLC computing and information resources must realize the fundamental importance of information resources and recognize their responsibility for the safekeeping of those resources. Users must guard against abuse that disrupts or threaten the viability of all systems. The following are the specific responsibilities of all EDUARDO CABIDE LLC information system users:

- Understand what the consequences of their actions are regarding computing security practices and act accordingly. Embrace the “Security is everyone’s responsibility” philosophy to assist EDUARDO CABIDE LLC in meeting its business goals.
- Maintain awareness of the contents of the information security policies.
- Read and sign the EDUARDO CABIDE LLC Security Awareness and Acceptable Use Policy (Appendix A)
- Classify confidential and sensitive information that is received unclassified. Limit the distribution of this information accordingly.

PCI Requirements Reference:

12.4.a Verify that information security policies clearly define information security responsibilities for all personnel.

12.4.b Interview a sample of responsible personnel to verify they understand the security policies.

12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.

2. IT CHANGE CONTROL POLICY

2.1. Policy Applicability

All proposed changes to EDUARDO CABIDE LLC network devices, systems and application configurations must follow this policy.

2.2. Change Request Submittal

The party responsible that will be implementing the change must complete and submit a

Change Request Form to the COO. A model form is shown in Appendix C illustrating the minimum data to be captured electronically or on hard copy. This form will not be reviewed without the following information completed, at a minimum:

- Resources Affected by Change (customers) – If a change could impact the functionality of customers, internal or external, this item must be completed. This documentation must include changes to features, applications and procedures that will be different from the existing system. Included in this documentation are some upgrades that the customer needs to perform to the operating system or other required 3rd party software or hardware.

- Back out Procedures – If the change does not go as intended a plan must be in place that describes the process of reverting the environment to its original configuration.
- Test Plan - A set of planned tests must be developed to verify that the change accomplished what it was supposed to do and does not adversely affect other system components or create a weakness in the security posture of the environment. This plan may be specific to each change.

Completion of the relevant details in the EDUARDO CABIDE LLC issue tracking system is equivalent to completion of the change request form.

PCI Requirements Reference:

Audit Procedure 6.4.5.1 Verify that documentation of customer impact is included in the change control documentation for each sampled change

Audit Procedure 6.4.5.4 Verify that back-out procedures are prepared for each sampled change.

2.3. Change Request Approval

After all planning and documentation is complete all management and concerned parties must sign off on the Change Request Form.

This can be achieved verbally in the weekly IT Development meeting.

PCI Requirements Reference:

Audit Procedure 6.4.5.2 Verify that documented approval by authorized parties is present for each sampled change.

2.4. Change Testing

Prior to introduction into the production network or systems all changes must first be tested on a QA or test network isolated from the production environment.

The documented test plan must be followed to ensure no adverse security effects on the network, systems or applications. Any discrepancies should be documented and a new Change Request Form generated once all issues have been resolved.

PCI Requirements Reference:

Audit Procedure 6.4.5.3.a Verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.

Audit Procedure 6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.

2.5. Change Implementation

All changes must be implemented according to the procedures that were tested successfully. Any discrepancies between expected results and actual results that impact the network, systems, applications, business requirements or support procedures must result in the immediate invocation of the documented back out procedures.

3. DATA CLASSIFICATION AND CONTROL POLICY

3.1. Policy Applicability

All data stored and accessed on EDUARDO CABIDE LLC information systems, whether managed by employees or by a third party, must follow this policy. Policy exemptions will be permitted only if approved in advance and in writing by the COO.

3.2. Data Classification

3.2.1. Introduction

All data stored on EDUARDO CABIDE LLC computing resources must be assigned a classification level by the information owner or creator. This level is used to determine which users are permitted to access the data.

3.2.2. EDUARDO CABIDE LLC Internal Information Categories

Confidential - applies to the most sensitive business information which is intended strictly for use within EDUARDO CABIDE LLC. Unauthorized disclosure could seriously and adversely impact the company, stockholders, business partners, and/or its customers.

Confidential information includes:

- Passwords
- Encryption keys
- Cardholder information

- Bank account information
- Intellectual property

Sensitive - Applies to less sensitive business information which is intended for use within EDUARDO CABIDE LLC. Unauthorized disclosure could adversely impact the company, its stockholders, its business partners, and/or its customers.

Sensitive information includes:

- Internal market research
- Audit reports, etc.

Private - Applies to personal information which is intended for use within EDUARDO CABIDE LLC.

- Unauthorized disclosure could adversely impact on the company and/or its employees.
- Examples of Private information include policies and procedures, procedure metrics, human resources information, etc.

Public - Applies to all other information which does not clearly fit into any of the above three classifications. Unauthorized disclosure isn't expected to seriously or adversely impact the company. Any release of this information must be authorized by the COO or CEO.

Public information includes:

PCI Data – The class of credit card and transaction data identified for protection under the Payment Card Industry (PCI) Data Security Standard (DSS). These data are specified in the Requirements and Security Assessment Procedures (RSAP) Version 2.0. 2 types of data are defined: Cardholder Data which may be stored after transaction authorization and Sensitive Authentication Data which may not be stored after transaction authorization.

- **Card Holder Data** – Applies to credit card data taken as payment for services. Data elements as specified in the PCI Security Audit Procedures version 1.1 are
    - Primary Account Number (PAN)
    - Card holder Name
    - Service Code
    - Expiration Date

- **Sensitive Authentication Data** – Applies to credit card data required for authentication and processing of credit card transactions as specified in the
    - PCI Requirements and Security Assessment Procedures 2.0 are
    - Full Magnetic Stripe
    - CVC2/CVV2/CID
    - PIN/PIN Block

3.3. Data Access

All confidential or sensitive data must be protected via access controls to ensure that data is not improperly disclosed, modified, deleted or rendered unavailable. The access controls must track all access to such data and identify who and when the data was accessed (See Section 15 Logging Controls Policy for more details). All access to systems must be configured to deny all but what information a particular user needs to access per their business role.

Access to systems or applications handling confidential, sensitive or private information must follow the data access request process. All requests require approval from the Information Security Team and a valid Authorization Request Form (Appendix B - A model form is shown illustrating the minimum data to be captured electronically or on hard copies. Access to data exceeding the employee's authorized role must also follow the data access request process and must include documented limits around such access (e.g. access source, access time limits, etc.). All access creation, modification and deletion request records must be retained for a period of 6 months following access termination.

3.3.1. Data Access Request Process

The following generally describes the workflow used by EDUARDO CABIDE LLC for requesting new access:

1. The user's manager will request or grant (as appropriate) authorization for access to confidential data via the New Employee Card (Appendix P).
2. The user's manager must approve the request for access based on the employee's role, identify any additional access requirements and submit the request to a member of the Information Security Team for approval.
3. If the access requested requires privileges above the employee's role a member of the Information Security Team will engage additional system owners or management to confirm.

4. The Information Security Team will forward the approved request to the System Administrator for account creation.
5. The System Administrator will create the user account(s) requested. Once the accounts have been created, the System Administrator must forward the request form to the COO for inclusion in the Users employee records and notify the Information Security Team that the request has been completed.

Requests for change of access must be submitted by the user's manager utilizing the last version of the New Employee Card (Appendix P). Business units are expected to capture this data in such a form that a clear audit trail is always available for review on file and the workflow shall be the same as above.

Direction regarding removal of an employee's access shall follow the same workflow above. When an employee leaves the business, a note will be added to their New Employee Card to confirm that access has been removed.

PCI Requirements Reference:

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

3.4. Physical Security

Hard copy materials and electronic media containing sensitive or confidential information must be protected by appropriate physical access controls.

- Cameras must be used to monitor server closets and data centers where systems reside that store sensitive, confidential, and cardholder data. The data collected must be stored for at least 3 months unless otherwise restricted by law.
- Appropriate facility controls must be used to limit and monitor physical access to systems that store confidential or sensitive data.
- Visitor logs and physical audit trails of access to these systems must be collected and kept at least 3 months unless otherwise restricted by law.
- Physical access must be restricted to publicly accessible network jacks, wireless access points and handheld devices.

PCI Requirements Reference:

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.

9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks.

9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.

3.5. User Authentication

3.5.1. Users

Each user's access privileges shall be authorized according to business need. User access to computer resources shall be provided only when necessary to perform tasks related to EDUARDO CABIDE LLC business.

The use of non-authenticated (e.g., no password) User IDs or User IDs not associated with a single identified user are prohibited. Shared or group user IDs are never permitted for user-level access. Every user must use a unique user account and a personal secret password for access to EDUARDO CABIDE LLC information systems and networks. Systems and applications must authenticate using a password or token entry.

All users must acknowledge understanding of the EDUARDO CABIDE LLC Information Security Policies by reading and signing the EDUARDO CABIDE LLC Security Acknowledgment and Acceptable Use Policy (Appendix A) prior to being allowed to access EDUARDO CABIDE LLC information systems and networks.

PCI Requirements Reference:

7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.

8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:

8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.

8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

8.1.3 Immediately revoke access for any terminated users.

8.1.4 Remove/disable inactive user accounts within 90 days.

8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:

- Enabled only during the period needed and disabled when not in use.
- Monitored when in use.

8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.

8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

8.4 Document and communicate authentication policies and procedures to all users including:

- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised.

8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

- All user access to, user queries of, and user actions on databases are through programmatic methods.
- Only database administrators can directly access or query databases.
- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

10.1 Implement audit trails to link all access to system components to each individual user.

3.5.2. Systems Access Controls

Each computer system should have an automated or procedural access control process. The process must:

- The user ID shall consist of at least 7 characters.
- User ID’s will be unique for each user

- Authenticate every user ID, system account and application account with a password.
- Require all passwords to be at least 7 characters in length.
- Require complex passwords, consisting of numeric, alphabetic & special characters with a mixture of both upper- and lower-case ones.
- Require that new passwords cannot be the same as the four previously used passwords.
- Lock out accounts after not more than six invalid logon attempts.
- Require that once a user account is locked out it remains locked for a minimum of 30 minutes or until the System Administrator resets the account.
- Require system/session idle time out of 15 minutes.
- Require passwords to be reset at least every ninety (90) days. Note: Job/Service user IDs may be exempt from this requirement with management approval. Administrative user ID's (e.g. root, Oracle, Administrator) must comply.
- Remove or disable inactive user accounts over 90 days old.
- Educate employees as part of induction and awareness programs & require the use of company approved password vault utilities to prevent disclosure of written password.
- Authentication credentials such as passwords must be protected from eavesdropping when transmitted over both trusted and untrusted networks (i.e. internal and external ones) by means of implementing industry approved encryption or hashing algorithms.
- Authentication credentials must be protected from disclosure/theft when stored by implementing industry approved encryption or hashing algorithms. These requirements apply to both internally developed or 3rd party applications, operating systems, devices or solutions.

The requirements above are for authenticating all system users.

PCI Requirements Reference:

8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:

8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.

8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

8.1.3 Immediately revoke access for any terminated users.

8.1.4 Remove/disable inactive user accounts within 90 days.

8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:

- Enabled only during the period needed and disabled when not in use.
- Monitored when in use.

8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.

8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.

8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

3.6. Account and Access Management

3.6.1. Information Security Team Responsibilities

The Information Security Team will approve access authorization according to the role and responsibilities of information system users. Each request for access must contain written and/or electronic evidence of approval by the Information Security Team.

Information Security, in conjunction with business unit management, will determine the default access levels that will be granted per a user's role. The Information Security Team will perform a bi-annual audit of computer resource authorizations to confirm that access privileges are appropriate. The audit will consist of validating access rights for sample user populations.

The Information Security Team must collect additional approvals for all access that is not associated with a defined access role. Extension authorizations for contractor accounts must go through the Information Security Team to provide an audit trail. An Emergency ID will be established when access is needed to diagnose and/or correct a problem.

- The request to create the Emergency ID must be made via the Information Security Team which will notify the appropriate system administration team.
- The requestor must inform the Information Security Team upon completion of the work so that the ID can be disabled.
- The Information Security Team will ensure that the Emergency ID Request Form is completed as soon as practical (the completion of this form should NOT delay providing access). The completed form must be filed by the Information Security Team

3.6.2. System Administrator Responsibilities

Account creation requests must specify access either explicitly or via a “role” that has been mapped to the required access. New accounts created by mirroring existing user accounts must be audited against the explicit request or roles for appropriate access rights. If a user requests a password reset via phone, email, web or other non-face-to-face method, that user’s identity must be verified before the password is reset Either through a request filed by his line manager or by presenting him/herself to the relevant system administrator.

Access should be removed immediately upon notification that access is no longer required.

Written procedures must be in place to ensure that access privileges of terminated or transferred users are revoked as soon as possible. Whenever possible users who are on leave-of-absence or extended disability should be suspended from the system.

User IDs shall be disabled after sixty (60) days of inactivity. After an additional thirty (30) days, disabled user IDs must be purged. These requirements may not apply to certain specialized accounts (e.g., NT Admin, root). In those instances, the System Administrator must provide a written waiver to the Information Security Team and document the compensating controls around access to the accounts.

All computer resources capable of displaying a custom sign-on or similar message must display the following message as part of the login process:

“This system is for the use of authorized users only. Individuals using this computer system without authority, or more than their authority, are subject to having all their activities on this system monitored and recorded by system personnel. While monitoring individuals improperly using this system, or during 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 evidence of such monitoring to law enforcement officials.

- System Administrators must enable audit logs to record user and administrative activities. Audit logs must be archived for a minimum of one year with ninety (90) days available for on-line viewing and analysis.
- Passwords set by System Administrators must be changed immediately upon the user’s next login. System Administrators must set initial passwords that are unique and compliant with the password rules.

- System Administrators must validate the identity of the user before performing a password reset. Business units must create local policies for positively validating user identities.
- Contractor accounts must have Information Security Team approval and must automatically expire at the end of the contract date. Extensions must be requested through the Information Security Team. System Administrators must monitor these accounts carefully while they are in use.
- Access must be immediately revoked for terminated users and for user access that is no longer required.
- Vendor accounts used for remote maintenance must only be enabled during the time that access is needed.
- Ensure that all systems and especially access to any databases containing cardholder information is authenticated (e.g., users, applications, administrators, etc.).

PCI Requirements Reference:

8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.

8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.

8.1.3 Immediately revoke access for any terminated users.

8.1.4 Remove/disable inactive user accounts within 90 days.

8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.

8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user and change immediately after the first use.

8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:

- Enabled only during the period needed and disabled when not in use.
- Monitored when in use**.**

8.5 Do does not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

- Generic user IDs are disabled or removed.
- Shared user IDs do not exist for system administration and other critical functions.

- Shared and generic user IDs are not used to administer any system components.

8.2.4 Change user passwords/passphrases at least once every 90 days.

8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:

- All user access to, user queries of, and user actions on databases are through programmatic methods.

- Only database administrators can directly access or query databases.

- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

10.1 Implement audit trails to link all access to system components to each individual user.

4. DATA RETENTION AND DISPOSAL POLICY

4.1. Policy Applicability

All data deemed sensitive or confidential by the Information Security Team which is stored on EDUARDO CABIDE LLC networks and systems must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Technical Officer.

4.2. Retention Requirements

All sensitive and confidential data, regardless of storage location, will be retained only as long as required for legal, regulatory and business requirements. The specific retention length will be established by the Data Owner under advisement from the General Counsel.

Sample Data Types and Data Retention

Data Type	Data Retention Period
Confidential	10 years
Sensitive	7 years
Private	5 years
Public	3 years
PCI Data (Card Holder Data)	7 years after end of business relationship with customer

PCI Data (Sensitive Authentication Data) *	Never stored beyond authorization of payment transaction

*As a special case, card holder data used for single transactions may be kept for up to 120 days.

As EDUARDO CABIDE LLC act on behalf of an issuer, card holder data utilized for transactions will be retained for the lifetime of the customer's account with EDUARDO CABIDE LLC. Once a customer's account is disabled or terminated, all the card holder data for that customer will be purged after 7 years of the termination using an approved destruction method.

Sensitive Authentication Data, including track, CVV2 and PIN information, will be retained only until completion of the authorization of a transaction. Storage of cardholder authorization data post-authorization is forbidden.

Business units will create local policies for the retention of all other company information.

All system and network audit logs must be retained for one year with 90 days minimum kept available for online view and analysis.

PCI Requirements Reference:

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
- Specific retention requirements for cardholder data
- Processes to secure deletion of data when no longer needed
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

3.2 Does not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.

3.2.1 Does not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

3.2.2 Does not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.

3.2.3 Does not store the personal identification number (PIN) or the encrypted PIN block after authorization.

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

4.3. Disposal Requirements

All confidential or sensitive electronic data, when no longer needed for legal, regulatory or business requirements, must be removed from EDUARDO CABIDE LLC systems using an approved method documented in this policy. This requirement includes all data stored in systems, temporary files or contained in the storage media.

PCI Requirements Reference:

9.8 Destroy media when it is no longer needed for business or legal reasons

4.4. Disposal Process

A programmatic (automatic) process will be executed on cardholder information systems nightly to remove all sensitive and confidential data that exceeds business retention requirements.

Other applicable data stored in files and directories where the containing media will be reused must be deleted securely by a “wiping” utility approved by the Information Security Department.

Media containing confidential or sensitive data that should no longer be retained must be disposed of in a secure and safe manner as noted below:

- Hard disks: sanitize (7-pass binary wipe), degauss or shred platter.
- Floppy disks: disintegrate, incinerate, pulverize, shred or melt.
- Tape media: degauss, shred, incinerate, pulverize or melt.
- USB “thumb/flash” drives, smart cards, and digital media: incinerate, pulverize or melt.
- Optical disks (CDs and DVDs): destroy optical surface, incinerate, pulverize, shred or melt.
- RSA Encryption Keys: keys must be revoked and the revoked key published to any online key repositories where the previously valid key is stored.

- Before computer or communications equipment can be sent to a vendor for trade-in, service or disposal, all confidential or sensitive information must be destroyed or concealed according to the approved methods in this policy.
- Removable computer storage media such as floppy, optical disks or magnetic tapes may not be donated to charity or otherwise recycled.
- Outsourced destruction of media containing confidential or sensitive information must use a bonded Disposal Vendor that provides a “Certificate of Destruction”.

PCI Requirements Reference:

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
- Specific retention requirements for cardholder data
- Processes to secure deletion of data when no longer needed
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

3.1.a Examine the data retention and disposal policies, procedures and processes to verify they include the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements.
- Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons).
- Processes for secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons.
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.

3.1.b Interview personnel to verify that:

- All locations of stored cardholder data are included in the data retention and disposal processes.

- Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data.

- The quarterly automatic or manual process is performed for all locations of cardholder data.

3.1.c For a sample of system components that store cardholder data:

- Examine files and system records to verify that the data stored does not exceed the requirements defined in the data retention policy

- Observe the deletion mechanism to verify data is deleted securely.

9.8 Destroy media when it is no longer needed for business or legal reasons as follows:

9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.

9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

5. PAPER AND ELECTRONIC MEDIA POLICIES

5.1. Policy Applicability

All employees handling hardcopy or electronic media must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Operating Officer.

5.2. Storage

5.2.1. Physical Security

Hard copy materials and electronic media containing sensitive or confidential information must be protected by appropriate physical access controls.

- Camera must be used to monitor sensitive areas. The data collected must be stored for at least 3 months unless otherwise restricted by law.

- Appropriate facility controls must be used to limit and monitor physical access to systems that store confidential or sensitive data.

- Visitor logs and physical audit trails of access to these systems must be collected and kept at least 3 months unless otherwise restricted by law.

PCI Requirements Reference:

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

9.1.1 Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.

9.4 Implement procedures to identify and authorize visitors.

Procedures should include the following:

9.4.1 Visitors are authorized before entering, and always escorted within, areas where cardholder data is processed or maintained.

9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.

9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.

9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.

Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log.

Retain this log for a minimum of three months, otherwise restricted by law.

9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.

5.2.2. Hardcopy Media

Hard copy materials containing sensitive or confidential information (e.g., paper receipts,

paper reports, faxes, etc.) are subject to the following storage guidelines:

- At no time are printed reports containing confidential or sensitive information to be removed from any EDUARDO CABDE LLC secure office environment.
- At no time is printed material containing confidential or sensitive information to be removed from any EDUARDO CABIDE LLC data center or computer room without prior authorization from the Information Security Team.

- Printed reports containing confidential or sensitive data are to be physically retained, stored or archived only within secure EDUARDO CABIDE LLC office environments, and only for the minimum time deemed necessary for their use.
- All hardcopy material containing confidential or sensitive information should be clearly labeled as such.
- All confidential or sensitive hardcopy media must be stored in a secure and locked container (e.g. locker, cabinet, desk, storage bin) which has been approved by the Information Security Team.
- Confidential or sensitive hardcopy material is never to be stored in unlocked or insecure containers or open workspaces.

5.2.3. Electronic Media

Electronic media containing sensitive or confidential information (e.g., CD, DVD, floppy disk,

hard disk, tape, etc.) is subject to the following storage guidelines:

- Confidential or sensitive information must never be copied onto removable media without authorization from the Information Security Team.
- At no time is electronic media containing confidential or sensitive information to be removed from any EDUARDO CABDE LLC secure office environment except for computer system backups.
- At no time is electronic media containing confidential or sensitive information to be removed from any EDUARDO CABIDE LLC data center or computer room without prior authorization from the Information Security Team.
- Electronic media containing confidential or sensitive data are to be physically retained, stored or archived only within secure EDUARDO CABIDE LLC office environments, and only for the minimum time deemed necessary for their use.
- All electronic media containing confidential or sensitive information should be clearly labeled as such.
- All removable, confidential or sensitive electronic media must be stored securely.
- All media must be sent or delivered by a secured courier or other delivery methods that can be accurately tracked and that have been approved by the Information Security Team.

PCI Requirements Reference:

9.5 Physically secure all media.

9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.

9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:

9.6.1 Classify media so the sensitivity of the data can be determined.

9.6.2 Send the media by secured courier or other delivery methods that can be accurately tracked

9.6.3 Ensure management approves all media that is moved from a secure area (including when media is distributed to individuals).

5.3. Inventory

A Media Inventory Log (Appendix D A model form is shown illustrating the minimum data to be captured electronically or on hard copy). All stored electronic and hard-copy media containing confidential or sensitive information must be inventoried annually by the Information Security Team. At this time, the security controls on the storage mechanism will be checked. Upon completion of the inventory the log will be updated.

PCI Requirements Reference:

Audit Procedure 9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.

5.4. Destruction

All hardcopy shred bins must always remain locked (until shredding). Employees should make every effort to immediately crosscut shred any printed material containing confidential or sensitive information.

Electronic media must be destroyed as outlined in the Data Retention and Disposal Policy.

PCI Requirements Reference:

9.10 Destroy media when it is no longer needed for business or legal reasons as follows:

9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.

9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed – for example purge, degauss, shred, or otherwise destroy).

6. FIREWALL AND ROUTER SECURITY ADMINISTRATION POLICY

6.1. Policy Applicability

All firewalls and routers on EDUARDO CABIDE LLC networks, whether managed by employees or by third parties, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Technical Officer.

6.2. Device Management Responsibilities

Management of all EDUARDO CABIDE LLC firewalls and routers shall be a combined effort of the System Administrator, the Network Operations Center and the Information Security Team.

The following subsections detail the responsibilities for these groups.

6.2.1. System Administrator

- Assure that changes to firewall hardware or software or security rules are approved by the Information Security Team and follow all change control policies and procedures.
- Document all firewall security rules utilizing Appendix E, Permitted Network Services and Protocols (A model form is shown illustrating the minimum data to be captured electronically or on hard copy).
- Following every change, review and update network diagrams to assure they accurately describe all connections to confidential or sensitive information and critical network protection mechanisms (e.g., firewalls, IDS/IPS, Anti-virus systems, access control systems, etc.).
- Enable appropriate logging on all security systems and perform active daily monitoring of the logs that report security events.
- Provide the Network Operations Center with read-only access to logs related to the critical systems health and performance.
- Provide the Network Operations Center and Information Security Team with read-only access to security event logs.
- Report on network security incidents to the Information Security Team immediately upon discovery.
- Coordinate an appropriate response with the Information Security Team to mitigate security events.
- Ensure that router configuration files are secured and synchronized properly.

6.2.2. Network Operations Center

- Monitor system and application specific alerts on critical systems (e.g., interface up/down, firewall demon failing, system reboots, etc.)

- Notify the appropriate parties in the event of a security system failure or security event.

6.2.3. Information Security Team

- Assure that security rules applied to the firewalls are sufficient to protect EDUARDO CABIDE LLC networks and corporate assets from external attacks and unauthorized access.
- Assure that security rules applied to the firewalls are sufficient to prevent internal security events from leaving the EDUARDO CABIDE LLC network.
- Review all firewall and router security rule change requests for policy compliance prior to submission through the change management process.
- Ensure that all protocols/services allowed through the firewalls are properly documented
- Avoid the use of risky protocols. If business or technological constraints justify their use, ensure the risky protocol employed has undergone a risk assessment which specifies compensating controls as well as documents the identified constraints.
- Actively monitor firewall security events to identify internal or external security incidents.
- Coordinate an appropriate response with the System Administrator to mitigate security events.

PCI Requirements Reference:

1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.

1.1.4.a Examine the firewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.

1.1.4.b Verify that the current network diagram is consistent with the firewall configuration standards.

1.1.4.c Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams.

1.2.2 Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration

6.3. Firewall, Router and Network Configuration Changes

Because firewalls support critical EDUARDO CABIDE LLC information systems activities, they are production systems.

All firewall changes must be approved by the Information Security Team and must be adequately tested following production standards as defined in the Change Control Policy.

These changes include, but are not limited to:

- Firewall rule additions, deletions, and modifications.
- Firewall or router software or system modifications.
- Firewall or router software or system upgrades, patches, or hot fixes.

PCI Requirements Reference:

1.1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:

1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all:

- Network connections and
- Changes to firewall and router configurations

1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.

1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.

6.4. Allowed Services

Every connectivity path and service that is not specifically permitted by this policy, with supporting documents issued by the Information Security Team, must be blocked by EDUARDO CABIDE LLC firewalls. The list of currently approved paths and services, with justifications, is listed in Appendix E, Permitted Network Services and Protocols.

PCI Requirements Reference:

1.1.6.a Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each.

1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.

1.1.6.c Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.

1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment and specifically deny all other traffic.

6.5. Allowed Network Connection Paths and Configuration Requirements

All Internet-based inbound traffic is only permitted into a firewall segmented demilitarized zone (DMZ) network. In all cases, this traffic should be limited to only ports necessary for EDUARDO CABIDE LLC's business requirements. Perimeter routers should not be configured with a route to internal address space except for the DMZ. Internal IP addresses must be hidden utilizing Network Address Translation (NAT) or Port Address Translation (PAT). Anti-spoofing technologies must be configured on perimeter devices, denying or rejecting all traffic with a:

- Source IP address matching internally allocated or EDUARDO CABIDE LLC owned address space.
- Source IP address matching RFC 1918 address space.
- Destination IP address matching RFC 1918 address space.

Outbound traffic from internal production systems must only be allowed to the EDUARDO CABIDE LLC DMZ network. Additionally, this traffic should be restricted to only required protocols and services.

Databases must be located on an internal network which is segmented from the EDUARDO CABIDE LLC DMZ network. Inbound connections to internal production payment systems, and originating from EDUARDO CABIDE LLC wireless networks, are not permitted. The use of a stateful packet inspection firewall must be utilized for Internet and wireless segmentation to only allow established connections into or out of each network segment. VLAN's with compliant ACL's may be used for cardholder environment segmentation so long as the VLAN switch is compliant with PCI and hardened to prevent all currently identified switch exploits (e.g. ARP cache flood). If VLAN's are used for segmenting all requirements for firewalls apply (e.g. deny all but business necessary traffic, change control, etc.).

PCI Requirements Reference:

1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.

1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)

1.3.4 Does allow unauthorized outbound traffic from the cardholder data environment to the Internet.

1.3.5 Permit only “established” connections into the network.

1.3.6 Place system components that store cardholder data (such as database) in an internal network zone, segregated from the DMZ and other untrusted networks.

1.3.7 Does not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to:

- Network Address Translation (NAT)
- Placing servers containing cardholder data behind proxy servers/firewalls
- Removal or filtering of route advertisements for private networks that employ registered addressing
- Internal use of RFC1918 address space instead of registered addresses.

6.6. Configuration Review

At least quarterly, the Information Security Team must thoroughly review each firewall rule set and record results of the review. The review must include the removal, when merited, of unused or unnecessary access paths. All proposed changes identified because of this review must go through the current change control process prior to implementation.

PCI Requirements Reference:

1.1.7 Requirement to review firewall and router rule sets at least every six months.

6.7. Personal Firewalls

All mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees) that are used to access the EDUARDO CABIDE LLC network must have personal

firewall software installed and activated. All such software must have a non-user alterable configuration as dictated by the Information Security Team.

PCI Requirements Reference:

1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include:

- Specific configuration settings are defined.
- Personal firewall (or equivalent functionality) is actively running.
- Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.

7. SYSTEM CONFIGURATION POLICY

7.1. Policy Applicability

All servers and network devices on EDUARDO CABIDE LLC networks, whether managed by employees or by third parties, must be built and deployed in accordance with this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Technical Officer.

7.2. System Build and Deployment

7.2.1. System Purpose

All computing systems should be designated for a single primary purpose where possible

(e.g., web servers, database servers, and DNS should be implemented on separate servers). No multi-purpose systems may, under any circumstances, store, transmit, or process confidential or sensitive data unless required by vendor documentation (e.g., SAP, Peoplesoft, ipAngel, Cisco Pix with add-ons, etc.).

PCI Requirements Reference:

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)

Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.

7.2.2. System Configuration Standards

All systems, prior to deployment in the production environment must conform to the

System Configuration Standards (Appendix G- a model form is shown illustrating the minimum data to be captured electronically or on hard copy). A valid business justification and risk assessment must exist for all deviations from EDUARDO CABIDE LLC published configuration standards. Deviations require written approval by the Information Security Team and must be noted on the System Configuration Record for the system.

7.2.3. System Configuration Records

A System Configuration Record (Appendix G - a model form is shown illustrating the minimum data to be captured electronically or on hard copy. This form must be updated with any future modifications to system configurations.

7.2.4. System Configuration Process

All new system deployments will follow the following high-level procedure:

1. Install operating system.
2. Update all operating system software with vendor recommendations.
3. Configure operating system parameters and secure the system according to the system configuration build documentation described in Appendix G (A model form is shown illustrating the minimum data to be captured electronically or on hard copy. Install applications and software:
    a. Install system specific applications and software according to System Configuration Record (if this is a replacement for an existing system).
    b. Install applications and software necessary for the systems purpose.
    c. Configure Network Time Protocol (NTP).
4. Update all application software by vendor recommendations.
5. Configure application parameters according to build document (application hardening).
6. Enable logging per Logging Controls (Section 15).
7. For systems containing confidential or sensitive information, deploy file integrity monitoring (FIM) software to alert personnel to unauthorized modification of critical system or content files. Configure FIM to perform critical file comparisons at least weekly.

8. Complete system specific System Configuration Record and maintain on file.

PCI Requirements Reference:

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

Sources of industry-accepted system hardening standards may include, but are not limited to:

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

2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)

2.2.2 Enable only necessary services, protocols, diamonds, etc., as required for the function of the system.

2.2.3 Implement additional security features for any required services, protocols, or demons that are insecure.

2.2.4 Configure system security parameters to prevent misuse.

2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).

7.2.5. Standard Software

The following list must be considered standard installed software on all applicable systems. A valid business justification and risk assessment must exist for all deviations from EDUARDO CABIDE LLC published configuration standards. Any such deviations require written approval by the Information Security Team and noted on the System Configuration Record for the system (see below).

- File servers, mail servers, and Windows-based systems
- Anti-Virus software
- Critical production systems
- File Integrity software
- Notebooks/Laptops
- Personal Firewall software
- VPN Client software
- PGP Desktop with Whole Disk Encryption enabled

PCI Requirements Reference:

1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include:

- Specific configuration settings are defined.
- Personal firewall (or equivalent functionality) is actively running.
- Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.

5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

7.2.6. Network Time Protocol (NTP)

Except for the internal EDUARDO CABIDE LLC NTP server(s), all EDUARDO CABIDE LLC production systems must be configured to use two of the internal NTP servers to maintain time synchronization with other systems in the environment.

The internal EDUARDO CABIDE LLC NTP server(s) will be configured to request time updates from the Internet site time.nist.gov & uk.pool.ntp.org. Client systems able to retrieve time settings from the NTP server will be limited through Access Control Lists (ACL).

The NTP system will always be running the latest available version of the software.

PCI Requirements Reference:

Audit Procedures 10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).

10.4.1.a Examine the process for acquiring, distributing and storing the correct time within the organization to verify that:

- Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.

- Where there is more than one designated time server, the time servers peer with one another to keep accurate time,

- Systems receive time information only from designated central time servers(s).

10.4.1.b Observe the time-related system-parameter settings for a sample of system components to verify:

- Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.

- Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time.

- Systems receive time only from designated central time server(s).

7.2.7. Cardholder Data Information Processing Application

All EDUARDO CABIDE LLC applications, dealing with the processing or retrieval of cardholder information, must be configured in a manner which masks or truncates displayed credit card numbers if possible. If the application is designed for a specific purpose in which the full credit card number must be displayed approval must be given by the Information Security Team during the Requirements Phase as described in section 12 Software Development Policy. In all cases displaying full or masked card numbers must be limited to the fewest number of users possible.

PCI Requirements Reference:

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.

7.2.8. Credit Card Storage Applications

All EDUARDO CABIDE LLC applications, dealing with the storage of cardholder information, must be configured in a manner which does not retain prohibited cardholder data, such as full track data, card-validation codes, card not present values (CV2, CID, etc.), pins or pin blocks. Storage devices on a network must be on an internal network segregated from the DMZ. All access to networked storage devices must have its authentication and communication encrypted. The PAN must be rendered unreadable through one of the following:

- Strong one-way hash functions (hashed indexes) with salt
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key management processes and procedures

PCI Requirements Reference:

1.3.6 Place system components that store cardholder data (such as database) in an internal network zone, segregated from the DMZ and other untrusted networks.

3.2.1 Does not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:

- The cardholder's name
- Primary account number (PAN)
- Expiration date
- Service code to minimize risk, store only these data elements as needed for business.

3.2.2 Does not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.

3.2.3 Does not store the personal identification number (PIN) or the encrypted PIN block after authorization.

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and logs) by using any of the following approaches:

- One-way hashes based on strong cryptography, (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures.

The MINIMUM account information that must be rendered unreadable is the PAN.

If for some reason, a company is unable to encrypt cardholder data, refer to PCI DSS Appendix B: "Compensating Controls for Encryption of Stored Data."

7.3. Vulnerability Identification and System Updates

7.3.1. Vulnerability Identification

Members of the Information Security Team must be informed of information security issues and vulnerabilities applicable to EDUARDO CABIDE LLC computing systems. When security issues are identified, the Information Security Team is responsible for notifying appropriate personnel, including system and network administrators.

The primary method for identifying new threats as they arise will be through vendor and security specific Internet mailing lists. Although not complete, the following lists should be subscribed to as well as other vendor lists applicable to EDUARDO CABIDE LLC specific software packages and systems:

- Common Vulnerability Scoring System (CVSS-SIG) - http://www.first.org/cvss/
- Common Vulnerabilities and Exposures -CVE - http://cve.mitre.org/
- National Vulnerability Database - NVD - http://nvd.nist.gov/
- Pecunia - http://secunia.com/advisories/
- Verisign iDefense - http://www.verisigninc.com/en_US/products-and-services/network-intelligence-availability/idefense/index.xhtml
- TippingPoint Zero Day Initiative ZDI - http://www.zerodayinitiative.com/advisories/upcoming/
- Symanted DeepSight Alert Services - https://tms.symantec.com/
- Cisco Security InstallShield Alert Manager Service - http://www.cisco.com/en/US/products/ps6834/serv_group_home.html

- IBM ISS XForce - http://www-935.ibm.com/services/us/iss/xforce/
- VUPEN - http://www.vupen.com/english/research.php
- McAfee Threat Intelligence Services (MTIS) - http://www.mcafee.com/us/mcafee-labs/technology/threat-intelligence-services.aspx
- Bugtraq -http://seclists.org/bugtraq/
- Full Disclosure - http://seclists.org/fulldisclosure/

EDUARDO CABIDE LLC System Configuration Standards (Appendix F - a model form is shown illustrating the minimum data to be captured electronically or on hard copy) must be updated to reflect measures required for protection from any newly discovered vulnerability.

PCI Requirements Reference:

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

Sources of industry-accepted system hardening standards may include, but are not limited to:

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

6.1.a Examine policies and procedures to verify that processes are defined for the following:

- To identify new security vulnerabilities
- To assign a risk ranking to vulnerabilities that includes identification of all “high risk” and “critical” vulnerabilities.
- To use reputable outside sources for security vulnerability information.

7.3.2. Vulnerability Risk Ranking

The risk ranking process at EDUARDO CABIDE LLC must consider the possible risks to the cardholder data environment (CDE) to determine which are the most significant to a specific system or component and implement prioritized deployment. Determining which risks to address and the optimum strategy for mitigating said risks is the responsibility of the Information Security Team. The vulnerability risk ranking

process is based on the Common Vulnerability Scoring System (CVSS) under the custodial care of the Forum of Incident Response and Security Teams (FIRST): http://www.first.org/cvss/

The vulnerability scanning solutions utilized by EDUARDO CABIDE LLC (QualysGuard PCI and Tenable Network Security's Nessus) include within their reports a CVSS Base Score. It is the responsibility of the IT Security Team to use the NIST CVSS v2.0 calculator as described within the EDUARDO CABIDE LLC Vulnerability Risk Ranking Procedure v1.0 to provide contextualized scoring to the EDUARDO CABIDE LLC CDE by defining the Temporal and Environmental Metrics.

PCI Requirements Reference:

6.2 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.

Note: Risk rankings should be based on industry's best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.

7.3.3. Vulnerability Testing

The Information Security Team is responsible for conducting internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades). This process includes identifying any unauthorized wireless devices on the network.

Additional external vulnerability scans must be performed by a scan vendor approved by the payment card industry at least quarterly. Penetration tests at both the application and network layer must be performed annually or after any significant change in the network. Networks and systems that fall under payment card system scope must also be monitored by an intrusion detection/prevention system that

alerts personnel of potential compromises. All confirmed and potential vulnerabilities identified through vulnerability scans and penetration tests will be communicated to appropriate personnel within EDUARDO CABIDE LLC for assessment and remediation. All high-level vulnerabilities must be corrected utilizing the Change Control EDUARDO CABIDE LLC Policy. Follow up scans must be performed to confirm compliance with EDUARDO CABIDE LLC security standards as well as the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures

The Chief Technical Officer must coordinate an annual formal risk assessment process that identifies any existing or new threats and vulnerabilities to ensure EDUARDO CABIDE LLC assets are adequately protected.

PCI Requirements Reference:

11.1 Implement processes to test the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades).

11.3 Implement a methodology for penetration testing that includes the following:

- Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
- Includes coverage for the entire CDE perimeter and critical systems
- Includes testing from both inside and outside the network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5
- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- Specifies retention of penetration testing results and remediation activities results.

11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.

Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

12.1.2 Implement a risk-assessment process that:

- Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),
- Identifies critical assets, threats, and vulnerabilities, and
- Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.

7.3.4. Security Patch Deployment

All security patches, hot-fixes and service packs identified by the Information Security

Team or system administrators must be applied to applicable systems within (30) days of vendor release. With any change to the environment, changes to the management process must be followed.

PCI Requirements Reference:

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month and addressing less critical devices and systems within three months.

8. ANTI-VIRUS POLICY

8.1. Software Configuration

All applicable systems must be configured with Information Security Team approved anti-virus/anti-spyware/anti-adware/anti-rootkit software. The software must be configured to scan in real-time, log anti-virus events with routing to a central logging solution, and end-users must not be able to configure or disable the software. The software must be configured to perform weekly scans. The preferred

deployment scenario should use a central management console, if the number of systems and utilized solution justify that.

PCI Requirements Reference:

5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers). Note: Systems commonly affected by viruses typically do not include UNIX based operating systems or mainframes.

5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

8.2. Signature Updates

All systems with anti-virus software must be configured to update virus signatures on at least a daily basis.

PCI Requirements Reference:

5.2 Ensure that all anti-virus mechanisms are maintained as follows:

- Are kept current,
- Perform periodic scans
- Generate audit logs which are retained by PCI DSS Requirement 10.7.

8.3. Software Logging

Anti-virus software must alert the Information Security Team in real-time to the detection of a virus. The Information Security Team will determine what steps to take based on the Incident Response Policy. Retention of Anti-Virus software logs will be in accordance with the Data Retention and Disposal Policy.

PCI Requirements Reference:

Audit Procedure 5.2.a Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date.

5.2.b Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are:

- Configured to perform automatic updates, and

- Configured to perform periodic scans.

5.2.c Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that:

- The anti-virus software and definitions are current.
- Periodic scans are performed.

5.2.d Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that:

- Anti-virus software log generation is enabled, and
- Logs are retained in accordance with PCI DSS Requirement 10.7.

9. BACKUP POLICY

9.1. Location

The backup media for each system is relocated to a secure off-site storage area.

The off-site storage location must be visited annually by management or a member of the

Information Security Team to confirm that it is physically secure and fireproof.

PCI Requirements Reference:

9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.

9.2. Transport

Offline storage media utilized for archival, or back-up purposes must be handled and retained in a secure environment such that only EDUARDO CABIDE LLC personnel and contracted storage facility personnel have access to the archival media. All media couriers and transport mechanisms must be approved by the Information Security Team.

Positive log-out and log-in of archive media will take place during all archive media transfers. All media that is transferred from one location to another should be logged as being transferred, by whom, where, and was it properly received, with signature from management. The Backup Media Transfer Log is in Appendix H (A model form is shown illustrating the minimum data to be captured electronically or on hard copy. All media containing confidential or sensitive data must be classified and identifiable as such prior to transfer as detailed in the Data Classification and Control Policy.

PCI Requirements Reference:

9.6.1 Classify media so the sensitivity of the data can be determined.

9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.

9.6.3 Ensure management approves all media that is moved from a secure area (including when media is distributed to individuals).

9.3. Audit

All media used will be classified as confidential or sensitive and assigned a unique tracking number or similar feature that uniquely identifies the media. All media must be registered with the Information Security Team for tracking prior to use.

Annual inventories of all stored media will take place. The Information Security Team will compare their list of in-use media with records at the storage facility using the Media Inventory Log (Appendix D A model form is shown illustrating the minimum data to be captured electronically or on hard copy.

PCI Requirements Reference:

9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.

10.5 Media Destruction

All media that is no longer needed or has reached an end-of-life must be destroyed or rendered unreadable so that no data may be extracted. Information on acceptable destruction techniques is detailed in the Data Retention and Disposal policy.

PCI Requirements Reference:

9.8 Destroy media when it is no longer needed for business or legal reasons as follows:

9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.

9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

10. ENCRYPTION POLICY

10.1. Policy applicability

This policy documents encryption standards that must be applied to all applicable mechanisms and systems on EDUARDO CABIDE LLC networks and data repositories, whether managed by employees or by third parties. This policy also applies to the management of encryption keys which may be shared with customers to exchange confidential information. Documentation provided to customers who have a need to exchange encryption keys with EDUARDO CABIDE LLC must include these guidelines. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Technical Officer.

10.2. Encryption Key Management

Keys must be generated, accessed, distributed and stored in a controlled and secure manner.

10.2.1. Key Access

Access to encryption key components will only be granted to those custodians specifically requiring access due to job function. All access may only be granted by the Chief Technical Officer and those requiring access must have so noted on their Authorization Request Form (Appendix B -a model form is shown illustrating the minimum data to be captured electronically or on hard copy. Additionally, these users must sign the Encryption Key Custodianship Form (Appendix I) A model form is shown illustrating the minimum data to be captured electronically or on hard copy. These forms will be held in the employee's Human Resources file.

PCI Requirements Reference:

3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.

3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.

10.2.2. Split Knowledge and Dual Control

Two custodians authorized by the Information Security Team, are required to collaborate to perform any symmetric key action (such as key generation or loading the key). Additionally, no single custodian may know or have access to all pieces of a symmetric data encryption key.

PCI Requirements Reference:

3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key).

***Note**: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*

***Note:** Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*

10.2.3. Key Generation

- Only strong encryption keys are to be used. Creation of encryption keys must be accomplished using a random or pseudo-random number generation algorithm.

Generating encryption keys must be accomplished by two custodians authorized by the Information Security Team. Each custodian will generate one clear text piece that will be used to create the encryption key. To prevent unauthorized substitution of keys physical and logical access to the key generating procedures and mechanisms must be secured.

PCI Requirements Reference:

3.6.1 Generation of strong cryptographic keys.

3.6.7 Prevention of unauthorized substitution of cryptographic keys.

10.2.4. Key Distribution

Only custodians authorized by the Information Security Team are allowed to retrieve key components from secure storage or distribute keys. Custodians must document all such actions in the Encryption Key Management Log (Appendix J) A model form is shown illustrating the minimum data to be captured electronically or on hard copy. The encryption keys must be placed in secure packaging prior to being returned to storage.

PCI Requirements Reference:

3.6.2 Secure cryptographic key distribution.

10.2.5. Key Storage

All data encryption keys must be stored encrypted and in a secure location. Key-encrypting keys must be stored separately from data-encrypting keys within applicable applications.

Clear-text backups of encryption key components must be stored separately in tamper-evident packaging in a secure location.

PCI Requirements Reference:

3.5.4 Store cryptographic keys securely in the fewest possible locations and forms.

Note: *This requirement also applies to key-encrypting keys used to protect data-encrypting keys-such key-encrypting keys must be at least as strong as the data-encrypting key.*

3.6.3 Secure cryptographic key storage.

10.2.6. Key Changes and Destruction

An encryption key change is the process of generating a new key, and should the circumstances dictate, decrypting the current production data and re-encrypting the confidential data with the new key. All data encryption keys must be changed when circumstances dictate a change to maintain encryption or key integrity as well as according to the following cryptoperiods based on the type of encryption algorithm and key length.

Protocol	Key size (bits)	Crypto period
RSA	4096	10 years
RSA	2048	5 years
AES	256	10 years
AES	128	6 months

The following dictates additional conditions when a key change is required:

- Regular Rotation: Keys must be changed to a minimum of 1 time per year.

- Suspicious Activity: This change is driven by any activity related to the key process which raises concern regarding the security of the existing key.
- Resource Change: Keys must be changed if a resource with knowledge of the keys terminates employment or assumes a new job role that no longer requires access to an encryption process.
- Technical Requirement: Keys must be changed if the key in place has become questionable due to a technical issue such as corruption or instability.
- Encryption keys are no longer in service to be disposed of in accordance with the process outlined in the Data Retention and Disposal Policy.

PCI Requirements Reference:

3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).

***Note**: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*

3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.

10.2.7. Transmission over Un-trusted Networks

Confidential and sensitive information must be encrypted during transmission over networks in which it is easy and common for the data to be intercepted, modified or diverted, some examples of strong encryption that is acceptable are:

- Transport Layer Security (TLS)
- Internet Protocol Security (IPSEC)
- Secure Shell (SSH)
- Secure FTP and FTP over SSL (SFTP & FTP-S)

Since these protocols support various encryption algorithms and key lengths (including known to be weak or compromised ones) it is imperative that the implementation and configuration of components using these protocols follow best practices based on industry standards.

PCI Requirements Reference:

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use.

10.2.8. Email Transmission of Confidential Information

Confidential and sensitive information is never to be sent unencrypted through email or other messaging technologies. Employees, with valid business justification, must be issued relevant for the messaging technology encryption software by the Information Security Team.

PCI Requirements Reference:

4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).

10.2.9. Encryption of Wireless Networks

All wireless networks in use at EDUARDO CABIDE LLC facilities must be protected through secure data encryption; the current minimum standards are WPA2. Wired Equivalent Privacy (WEP) is expressly prohibited. Under no circumstances should the encryption strength be configured to be less than the equivalent of 128 bits symmetric key encryption. Wireless encryption keys will be changed every ninety (90) days or whenever an administrator with knowledge of the keys is terminated.

PCI Requirements Reference:

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

11. SPECIAL TECHNOLOGIES USAGE POLICY

11.1. Policy Applicability

All users of special technologies deployed on EDUARDO CABIDE LLC networks, whether employees or contractors, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Technical Officer. Currently, “special technologies” refers to modem use, modem or VPN access, wireless networks and other employee-facing technologies within the EDUARDO CABIDE LLC computing environment. This policy will be modified in the future to include any new “special technologies” used.

PCI Requirements Reference:

12.3 Develop usage policies for critical technologies and define proper use of these technologies.

Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.

Ensure these usage policies require the following:

11.2. Approval

The Information Security Team must explicitly approve any use or deployment of special technologies by job function role or on an individual basis. For general user application, this includes remote VPN access and wireless network access. These approvals must be documented on the user’s Authorization Request Form (Appendix B A model form is shown illustrating the minimum data to be captured electronically or on hard copy.

PCI Requirements Reference:

12.3.1 Explicit approval by authorized parties.

11.3. Authentication

User authentication mechanisms, where possible, must be integrated into the current EDUARDO CABIDE LLC authentication systems. All devices must be authenticated at a minimum with username and password or other authentication items (for example, token) Under no circumstances may the user authentication requirements be less strict than currently defined policies and procedures (e.g., complex password change interval, etc.).

All remote access to the EDUARDO CABIDE LLC network using these technologies must be authenticated via a strong two-factor authentication scheme approved by the Information Security Team.

PCI Requirements Reference:

8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.

Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.

11.4. Device Inventory

All approved user devices (personal modems and wireless network interfaces) must be noted on the Special Technologies Device Inventory (Appendix K A model form is shown illustrating the minimum data to be captured electronically or on hard copy. All approved users of these technologies must be noted on the Special Technologies User List (Appendix L A model form is shown illustrating the minimum data to be captured electronically or on hard copy. Users that must be documented include:

- Wireless network users
- Employees with VPN access
- Vendors with remote/VPN access

PCI Requirements Reference:

12.3.3 A list of all such devices and personnel with accesst

11.5. Device Identification

All personal modems and wireless access points must be labeled with the device owner, contact information and device purpose.

PCI Requirements Reference:

12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)

11.6.Acceptable Use

Acceptable use of EDUARDO CABIDE LLC special technologies is subject to the same guidelines and restrictions put forth in the Security Awareness and Acceptable Use Policy (Appendix A).

PCI Requirements Reference:

12.3.5 Acceptable uses for technology.

11.7.Permitted Locations

The Information Security Team must authorize the placement of any wireless access points and dial-in modems. Dial-in modems are typically limited to the data center. Wireless access points are normally placed in the ceiling plenum to protect them from tampering. The use of these devices must be logged according to the Special Technologies Device Inventory (Appendix K A model form is shown illustrating the minimum data to be captured electronically or on hard copy) and Special Technologies User List (Appendix L A model form is shown illustrating the minimum data to be captured electronically or on hard copy.

PCI Requirements Reference:

12.3.6 Acceptable network locations for the technologies.

11.8.Approved Products

Only the Information Security Team-approved devices may be deployed into the EDUARDO CABIDE LLC network. The use of these devices must be logged according to the Special Technologies Device Inventory (Appendix K) and Special Technologies User List (Appendix L A model is shown illustrating the minimum data to be captured electronically or on hard copy.

PCI Requirements Reference:

12.3.7 A list of company-approved products.

12.9 Session Disconnect

All dial-in modems, modem banks and VPN concentrators/termination points (for client and not site-to-site connectivity) must be configured to automatically disconnect sessions after thirty (30) minutes of inactivity.

PCI Requirements Reference:

12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity

12.10 Vendor Connections

VPN connections and other remote-access technologies, systems and accounts used solely for the purpose of vendor maintenance and support must remain disconnected and/or disabled until required. Activating these remotes access paths requires approval from the Information Security Team or established problem management procedures and they must be disabled immediately after use.

PCI Requirements Reference:

12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.

12.11 Cardholder Data Access

If any cardholder data is available through remote-access connections special precautions must be taken. The following are prohibited:

- Storage of the company information onto local hard drives, floppy disks, and other media is prohibited.
- Cut, paste, and print functions of remote PCs is prohibited for the duration of the connection.

PCI Requirements Reference:

12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.

Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.

12. SOFTWARE DEVELOPMENT POLICY

12.1. Development Environment

All new software must be tested in a test/development environment separate from the production environment. If the network is connected to the production EDUARDO CABIDE LLC network, access controls must be in place to enforce the separation.

Production card holder data will not be used for testing and development purposes without being sanitized. Test personnel should make every effort to use mock data only for testing on non-production systems and software. If it is determined that production card holder data must be used in testing, the Security Council must review and approve the business justification, the testing window will have as short a duration as possible, all PCI controls must be enforced on the systems under test, and the Security Council must be notified of test results, and verification that production data has been scrubbed after close of testing window.

All test data, custom application accounts, usernames and passwords must be removed at the conclusion of testing, and in all cases before software becomes active. All code promotion to the production environment will be accomplished by the System Administrators. Under no circumstances will the Development Department have full time read/write access to production applications or data. Under emergency situations developers may assist in troubleshooting utilizing an Emergency ID described in section *3.6.1 Information Security Team Responsibilities.*

PCI Requirements Reference:

6.4.5 Change control procedures must include the following:

6.4.5.1 Documentation of impact.

6.4.5.2 Documented change approval by authorized parties.

6.4.5.3 Functionality testing to verify that the change does not adversely impact on the security of the system.

6.4.5.4 Back-out procedures.

6.4.1 Separate development/test environments from production environments and enforce separation with access controls.

6.4.2 Separation of duties between development/test and production environments

6.4.3 Production data (live PANs) are not used for testing or development.

6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.

12.2. Secure Software Development Procedures

12.2.1. Development Lifecycle

Internal and 3rd party development of proprietary software must utilize industry recognized best practices for software development such as described at http://www.oracle.com/technetwork/java/seccodeguide-139067.html Security checks and control measures must be considered throughout the development life cycle.

The high-level overview of the security measures taking place within each phase of the EDUARDO CABIDE LLC development process are as follows:

- Requirements Analysis – developers should determine whether application requirements are inherently insecure.
- Design – application components must be planned in a manner consistent with data and network security.
- Development – developers must consider all application vulnerabilities (i.e.: memory bound issues, privilege and access bypass, etc.).
- QA Implementation - implementation must not compromise security controls already in place or introduce new vulnerabilities.
- QA Testing - in addition to functional and efficient testing, all security features of the application must be tested.
- Documentation – all application feature and implementation documentation must include direction on proper security configurations.
- Production Implementation – implementation must not compromise security controls already in place or introduce new vulnerabilities.
- Production Testing – in addition to functional and efficiency testing, all security features of the application must be tested.
- Maintenance – all future application maintenance should not compromise security controls already in place or introduce new vulnerabilities. Any new code must be reviewed and tested as detailed above.

PCI Requirements Reference:

6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:

- In accordance with PCI DSS (for example, secure authentication and logging)
- Based on industry standards and/or best practices.
- Incorporating information security throughout the software-development life cycle

6.3.2 Review custom code prior to release to production or customers to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:

- Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices.
- Code reviews ensure code is developed according to secure coding guidelines
- Appropriate corrections are implemented prior to release.
- Code-review results are reviewed and approved by management prior to release.

***Note**: This requirement for code reviews applies to all custom code (both internal and public facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*

12.2.2. Internally Developed Applications

In addition to the Development Life-Cycle security measures that take place throughout the application development life cycle, special care should be given to EDUARDO CABIDE LLC applications that are web-based. All EDUARDO CABIDE LLC developers will receive training on secure coding practices. All development must be done taking the OWASP guidelines into account, located at http://www.owasp.org. Specifically, the following vulnerabilities must be considered and checked for during the Code Review and Testing phases:

- Unvalidated Input
- Malicious Use of User IDs
- Malicious Use of Account Credentials and Session Cookies
- Cross-Site Scripting
- Cross-site request forgery
- Buffer Overflows
- SQL Injection and other Command Injection Flaws

- Error Handling Flaws
- Insecure Cryptographic Storage
- Denial of Service
- Insecure Configuration Management
- Insecure Direct Object references

Annually, and whenever significant modifications have taken place, all web-based applications will be put through an application-specific penetration test. All custom codes are to be reviewed by an organization that specializes in application security or an application layer firewall in front of web-facing applications.

PCI Requirements Reference:

6.5 Address common coding vulnerabilities in software-development processes as follows:

- Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.
- Develop applications based on secure coding guidelines.

Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry's best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.

6.5.1 Injection flaws, particularly SQL injections. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.

***Note**: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with the industry's best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*

6.5.2 Buffer overflows

***Note**: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with the industry's best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*

6.5.3 Insecure cryptographic storage.

Note: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with the industry's best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.

6.5.4 Insecure communications.

Note: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with the industry's best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.

6.5.5 Improper error handling.

Note: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with the industry's best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.

6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).

***Note**: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with the industry's best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*

6.5.7 Cross-site scripting (XSS)

***Note**: Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external).*

***Note**: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with the industry's best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*

6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).

***Note**: Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external).*

***Note**: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with the industry's best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*

6.5.9 Cross-site request forgery (CSRF)

***Note**: Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external).*

***Note**: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with the industry's best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*

6.5.10 Broken authentication and session management.

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.

- Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

***Note**: "An organization that specializes in application security" can be either a third-party company or an internal organization, if the reviewers specialize in application security and can demonstrate independence from the development team.*

12.2.3. Cardholder Data and Processing Applications

All EDUARDO CABIDE LLC proprietary or custom applications dealing with the processing or retrieval of cardholder information must be configured in a manner which masks or truncates the displayed credit card number. If cardholder information is to be masked only the first 6 and any other 4 digits may remain displayed. If the application is designed for a specific purpose in which the full credit card number must be displayed, approval must be given by the Information Security Team.

PCI Requirements Reference:

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.

Note: This requirement does not supersede stricter requirements in place for displays of cardholder data, for example, legal or payment card brand requirements for point-of-sale (POS) receipts.

13. INCIDENT RESPONSE PLAN AND PROCEDURES

13.1. Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees are responsible for assisting in the incident response procedures within their areas of knowledge, expertise, and responsibility. Some examples of security incidents that an employee might recognize in their day-to-day activities include, but are not limited to:

- Theft, damage, or unauthorized access (e.g., unauthorized logins, papers missing from their desk, broken locks, missing log files, alerts from security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – Inaccurate information within databases, logs, files, or paper records
- Abnormal system behavior (e.g., unscheduled system reboot, unexpected messages, abnormal errors in system log files or on terminals)
- Security event notifications (e.g., file integrity alerts, intrusion detection alarms, physical security alarms such as fire alarms, environmental alarms, natural disaster alerts)

All employees, regardless of job responsibilities, should be aware of the potential incident identifiers and who to notify in these situations. In all cases, every employee should report incidents via the instructions under 13.2 Incident Reporting, unless they are assigned other activities within the incident response plan.

13.2. Reporting and Incident Declaration Procedures

The Information Security Team should be notified immediately of any suspected or confirmed security incidents involving EDUARDO CABIDE LLC computing assets, particularly critical systems. If it is unclear whether a situation should be considered a security incident, the Team should be contacted to evaluate it.

Apart from the steps outlined below, it is imperative that any investigative or corrective action be taken only by Information Security Team personnel or under the oversight of Information Security Team personnel, to assure the integrity of the investigation and recovery process. When faced with a potential situation, you should do the following:

- If the incident involves a compromised computer system.
- Do not alter the state of the computer system.
- The computer system should remain on, and all currently running computer programs should be left as it is. Do not shut down the computer or restart the computer.

- Immediately disconnect the computer from the network by removing the network cable from the back of the computer.
- Reporting the security incident.
- Contact the Information Security Team to report any suspected or actual incidents.
- No one should communicate with anyone outside of their supervisor(s) or the
- Information Security Team about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Information Security Team.
- Document any information you know while waiting for the Information Security Team to respond to the incident. This must include date, time, and the nature of the incident, if known. Any information you can provide will aid in responding in an appropriate manner.

PCI Requirements Reference:

12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:

- Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum
- Specific incident response procedures
- Business recovery and continuity procedures
- Data backup processes
- Analysis of legal requirements for reporting compromises
- Coverage and responses of all critical system components
- Reference or inclusion of incident response procedures from the payment brands.

13.3. Incident Severity Classification

The Information Security Team will first attempt to determine if the security incident justifies a formal incident response.

In cases where a security incident does not require an incident response, the situation will be forwarded to the appropriate area of IT to ensure that all technological support services required are rendered.

The following descriptions should be used to determine what response the Information Security Department will take.

- Level 1 - One instance of potentially unfriendly activity (e.g., finger, unauthorized telnet, port scan, corrected virus detection, unexpected performance peak, etc.).
- Level 2 - One instance of a clear attempt to obtain unauthorized information or access (e.g., attempted download of secure password files, attempt to access restricted areas, single computer successful virus infection on a non-critical system, unauthorized vulnerability scan, etc.) or a second Level 1 attack.
- Level 3 - Serious attempt or actual breach of security (e.g., multi-pronged attack, denial of service attempt, virus infection of a critical system or the network, successful buffer/stack overflow, successful unauthorized access to sensitive or critical data or systems, broken lock, stolen papers, etc.) or a second Level 2 attack.
- Any Level 1 type incident occurring against systems storing sensitive or confidential data or originating from unauthorized internal systems is classified as a Level 2.

13.4. Incident Response

13.4.1. Typical Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls. The following actions should be taken by the Information

Security Department once an incident has been identified and classified.

13.4.1.1. Level 1

Contain and Monitor

1. If possible, record the user, IP address and domain of intruder.
2. Utilize approved technology controls to temporarily or permanently block the intruder’s access.
3. Maintain vigilance for future break-in attempts from this user or IP address.

13.4.1.2. Level 2

Contain, Monitor and Warn

1. Collect and protect information associated with the intrusion.
2. Utilize approved technology controls to temporarily or permanently block the intruder’s access.

3. Research the origin of the connection.
4. Contact the ISP and ask for more information regarding the attempt and intruder.
5. Research potential risks related to intrusion method attempted and re-evaluated for higher classification and incident containment, eradication, and recovery as described for Level 3 incident classifications.
6. Upon identification, inform malicious users of our knowledge of their actions and warn of future recrimination if attempt is repeated. If an employee is the malicious user, management should work with Human Resources to address the Acceptable Use violation appropriately.

13.4.1.3. Level 3

Contain, Eradicate, Recover and perform Root Cause Analysis

1. If the incident involved credit card systems, the Acquirer and applicable card associations must be notified. See section 13.2 for more details.
2. Contain the intrusion and decide what action to take. Consider unplugging the network cables, applying highly restrictive ACL's, deactivating or isolating the switch port, deactivating the user ID, terminating the user's session/change password etc.
3. Collect and protect information associated with the intrusion via offline methods. If forensic investigation is required, the Information Security Team will work with legal and management to identify appropriate forensic specialists.
4. Notify management of the situation and maintain notification of progress at each following step.
5. Eliminate the intruder's means of access and any related vulnerabilities.
6. Research the origin of the connection.
7. Contact ISP and ask for more information regarding attempt and intruder, reminding them of their responsibility to assist in this regard.
8. Research potential risks related to, or damage caused by intrusion method used.

13.4.2. Cardholder Data Compromise – Special Response & Notification Procedures

For any incidents involving potential compromises of credit card information, the Information Security Team will use the following procedure:

1. Contain and limit the exposure. Conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:
    a. Log all actions taken (e.g., bound notebook, video camera, etc.).

b. Utilize chain of custody techniques during all transfers of equipment and information related to the incident.

c. Do not access or alter compromised systems (e.g., do not log on or change passwords; do not log in as ROOT).

d. Do not turn off the compromised machine. Instead, isolate compromised systems from the network (e.g., unplug the network cable, deactivate switch port, isolate to contained environment e.g. isolated VLAN). Utilize Disaster Recovery / Business continuity procedures to recover business processes.

e. Preserve logs and electronic evidence.

f. If you use a wireless network, change SSID on the AP and other machines that may be using this connection (apart from any systems believed to be compromised).

g. Be on high alert and monitor all cardholder information systems.

2. Alert all necessary parties. Be sure to notify:

   a. Internal or External Incident Response or Forensics Team, if they are not already involved

   b. Merchant bank

   c. U.S. Secret Service (if PCI payment data is compromised)

3. Follow appropriate procedures for each card association which EDUARDO CABIDE utilizes for credit card services.

Visa

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact (650) 432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if Compromised" documentation for additional activities that must be performed. That documentation can be found at http://www.visaeurope.com/en/businesses__retailers/payment_security/idoc.ashx?docid=9dadfd15-c66b-4c63-abd2-faa2f71a1ef9&version=-1

MasterCard

Contact your merchant bank for specific details on what to do following a compromise.

Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf

American Express

Contact your relationship manager or call the support line on 1-800-528-4800 for further guidance.

Discover Card

Contact your relationship manager or call the support line at 1-800-347-3083 for further guidance.

JCB

Contact your relationship manager or call the support line on 1 213 896-3718 for further guidance.

PCI Requirements Reference:

Audit Procedure 12.10.1a Verify that the incident response plan includes:

- Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum
- Specific incident response procedures
- Business recovery and continuity procedures
- Data backup processes
- Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database)
- Coverage and responses for all critical system components
- Reference or inclusion of incident response procedures from the payment brands.

12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:

- Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum
- Specific incident response procedures
- Business recovery and continuity procedures
- Data backup processes

- Analysis of legal requirements for reporting compromises
- Coverage and responses of all critical system components
- Reference or inclusion of incident response procedures from the payment brands

13.4.3. Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Information Security Team and all affected parties will meet to review the results of the investigation conducted under step 1, section 13.4.2 of this document to determine the root cause of the compromise and evaluate the effectiveness of the Incident Response Plan. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient must be updated accordingly.

PCI Requirements Reference:

Audit Procedure 12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

13.5. Plan To Test and Training

At least once a year, a mock-incident will be initiated to facilitate testing of the current plan.

The exact incident scenario to be tested will be at the discretion of the Information Security Team. Once complete, a follow-up session, as detailed above, will be held.

All EDUARDO CABIDE LLC employees that could have an active role within incident response will be part of the test process. Training regarding incident response responsibilities should be performed regularly to ensure employees' readiness for test and actual incidents.

PCI Requirements Reference:

12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.

12.9.4 Provide appropriate training to staff with security breach response responsibilities.

13.6. Automated Security System Notifications

All automated intrusion detection systems within the EDUARDO CABIDEL LLC environment, including intrusion detection sensors and file integrity checking systems, will be configured to automatically notify the Information Security Team of any potential compromises or attacks.

An engineer with the Information Security Team must be available on a 24/7 basis to initiate the incident response plan if warranted.

PCI Requirements Reference:

Audit Procedure 12.10.5 Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems are covered in the incident response plan.

Audit Procedure 12.10.3 Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.

14. EMPLOYEE IDENTIFICATION POLICY

14.1. Employee Requirements

Visitors to EDUARDO CABIDE LLC's shared office facility must always clearly display their ID badges. It is every employee's responsibility to watch for unknown people or employees not displaying badges.

PCI Requirements Reference:

9.2. Develop procedures to easily distinguish between onsite personnel and visitors, to include:

- Identifying onsite personnel and visitors (for example, assigning badges)
- Changes to access requirements
- Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).

14.2. Facilities

Cardholder data will not be accessible from EDUARDO CABIDE LLC's office facilities and storage of such information will be held by PCI DSS compliant infrastructure.

PCI Requirements Reference:

9.2.a Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.

- Verify procedures include the following:
- Identifying onsite personnel and visitors (for example, assigning badges),
- Changing access requirements, and
- Revoking terminated onsite personnel and expired visitor identification (such as ID badges)

9.4 Implement procedures to identify and authorize visitors.

Procedures should include the following:

9.4.1 Visitors are authorized before entering, and always escorted within, areas where cardholder data is processed or maintained.

9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.

9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.

9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.

Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log.

Retain this log for a minimum of three months, otherwise restricted by law.

9.3 Control physical access for onsite personnel to sensitive areas as follows:

- Access must be authorized and based on individual job function.
- Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.

15. LOGGING CONTROLS POLICY

15.1. Events Logged

Automated audit trails must be implemented for all system components to reconstruct the following events:

- All user access to company information.

- All administrative actions utilizing user IDs with significant privileges above a general user (e.g. root, user IDs with Administrator group privilege, oracle, etc.)
- Access or initialization of audit log files
- Any user or administrator authentication attempts (both valid and invalid)
- Creation or deletion of system-level objects.
- Invalid logical access attempts

PCI Requirements Reference:

10.2.1 All individual user accesses to cardholder data

10.2.2 All actions taken by any individual with root or administrative privileges

10.2.3 Access to all audit trails

10.2.4 Invalid logical access attempts

10.2 5 Use of and changes to identification and authentication mechanisms, including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges

10.2.6 Initialization, stopping, or pausing of the audit logs

10.2.7 Creation and deletion of system-level objects.

15.2. Event Log Structure

All system access event logs must contain at least the following information.

- User Identification
- Type of event
- Date and time of event
- Result of the event
- Originating location of the event
- The name of the affected data, system component or resource

PCI Requirements Reference:

10.3 Record at least the following audit trail entries for all system components for each event:

10.3.1 User identification

10.3.2 Type of event

10.3.3 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource.

15.3.Log Security

All event logs must be collected in a centralized location or media that is difficult to alter and protected from unauthorized access. The viewing of such logs is to occur on a need only basis. The logs will be further protected by a file integrity monitoring system that alerts the Information Security Team upon unauthorized access. Wireless logs must be copied onto a log server on the internal LAN.

PCI Requirements Reference:

10.5 Secure audit trails so they cannot be altered.

10.5.1 Limit viewing of audit trails to those with a job-related need

10.5.2 Protect audit trail files from unauthorized modifications

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.

10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

APPENDIX A – SECURITY AWARENESS AND ACCEPTABLE USE POLICY

Error! Unknown document property name. Security Awareness and Acceptable Use Policy

Overview

The intention for publishing a security awareness and acceptable use policy is not to impose restrictions that are contrary to the established culture of openness, trust and integrity. **Error! An unknown document property name.** is committed to protecting all employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of **Error! Unknown document property name.**. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations.

Effective security is a team effort involving the participation and support of every **Error! Unknown document property name.** employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at **Error! Unknown document property name.**. These rules are in place to protect the employees and **Error! Unknown document property name.**. Inappropriate use exposes **Error! Unknown document property name.** to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees, contractors, consultants, temporary employees, and all other workers at **Error! Unknown document property name.**, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by **Error! Unknown document property name.**.

Policy

General Use and Ownership

1. While network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of **Error! Unknown document property name.**. Because of the need to protect the network, management cannot guarantee the confidentiality of employee's personal information stored on any network device belonging to **Error! Unknown document property name.**.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. IT recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within **Error! An unknown document property name.** may monitor equipment, systems and network traffic at any time.
5. **Error! The Unknown document property name.** reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to credit card information, company private, corporate strategies, competitor sensitivity, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. The system and user level passwords should be changed every 90 days.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.

4. Employees should secure their workstations by logging off or lock (control-alt-delete for Windows users) when the host will be unattended.

5. Use encryption of information in compliance with Information Technologies' Security Policies.

6. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the corporate security standards, including personal firewalls.

7. Postings by employees from an **Error! Unknown document property name.** email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of **Error! Unknown document property name.**, unless posting is during business duties.

8. All hosts used by the employee that are connected to the **Error! Unknown document property name.** Internet/Intranet/Extranet, whether owned by the employee or **Error! Unknown document property name.**, shall be continually executing approved virus-scanning software with a current virus database.

9. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of **Error! Unknown document property name.** authorized to engage in any activity that is illegal under local, national or international law while utilizing **Error! Unknown document property name.**-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by **Error! Unknown document property name.**.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which **Error! Unknown document property name.** or the end user does not have an active license is strictly prohibited. The use of any recording device such as, but not limited to, digital cameras, video cameras, and cell phone cameras, within the premises of all **Error! An unknown document property name.** properties is prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to the export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a **Error! Unknown document property name.** computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
7. Making fraudulent offers of products, items, or services originating from any **Error! Unknown document property name.** account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, **Error! Unknown document property name.** employees to parties outside **Error! Unknown document property name.**.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within name's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by **Error! Unknown document property name.** or connected via name's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

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

Definitions

Spam Unauthorized and/or unsolicited electronic mass mailings.

Employee/Contractor/Third Party Signature

Date

Printed Name

Date of Security Awareness Training

HORIZATION REQUEST FORM

PART I (To be filled out by the Requestor or Requestor's Supervisor)