ANC Electronics & More

PCI DSS v4.0

Policies and Procedures

LAST REVISION DATE

2/7/2026

Provided By:

MegaplanIT Holdings, LLC

Developed For:

ANC Electronics & More

Table of Contents

Document Revision History

Revision Notes:	Revision By:	Revision Date:	Date Approved/ By Whom:
Initial creation	MegaplanIT Holdings, LLC	2/7/2026	2/4/2026| PCI

I. Introduction

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

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

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

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

Brief Explanation of Payment Card Industry (PCI) Compliance

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

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

II. Scope of Policies and Procedures

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

All system components that are owned, operated, maintained, and controlled by Encytro and are connected to the card-processing or data storage environment, as well as all other system components that interact with these systems, are in-scope for this policy. These system components include both physical and virtual servers, network devices (firewalls, routers, hubs, switches, repeaters, load balancers, etc.), as well as the operating systems and any applications that reside on them.

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

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

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

Requirement 1 – Install and Maintain Network Security Controls

Policy Statement:

Encytro is committed to protecting cardholder data by maintaining a secure network infrastructure. As part of this commitment, Encytro ensures that all network security controls are installed and maintained in accordance with PCI DSS v4.0 Requirement 1. Our network security controls are configured and maintained to protect cardholder data at all times. The purpose of this policy is to define the processes and mechanisms for installing and maintaining these controls.

Procedure:

1.1 Security policies and operational procedures

- All security policies and operational procedures identified in Requirement 1 are documented, reviewed annually, and communicated to all relevant parties.

- Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.

1.2 Network security controls

- Configuration standards for network security control rulesets are defined, implemented, and maintained.
- All changes to network connections and configurations of network security controls are approved and managed in accordance with the change control process defined at Requirement 6.5.1.
- An accurate network diagram and data-flow diagram is maintained that shows all connections between the CDE and other networks, including any wireless networks.
- All services, protocols, and ports allowed are identified, approved, and have a defined business need.
- Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure.
- Configurations of network security controls are reviewed at least once every six months to confirm they are relevant and effective.
- Configuration files for network security controls are secured from unauthorized access and kept consistent with active network configurations.

1.3 Network access to and from the cardholder data environment

- Inbound traffic to the CDE is restricted to only traffic that is necessary. All other traffic is specifically denied.
- Outbound traffic from the CDE is restricted to only traffic that is necessary. All other traffic is specifically denied.
- Network security controls are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that all wireless traffic from wireless networks into the CDE is denied by default. Only wireless traffic with an authorized business purpose is allowed into the CDE.

1.4 Network connections between trusted and untrusted networks

- Network security controls are implemented between trusted and untrusted networks.
- Inbound traffic from untrusted networks to trusted networks is restricted to communications with system components that are authorized to provide publicly accessible services, protocols, and ports (eg within a DMZ). Stateful responses to communications initiated by system components in a trusted network. All other traffic is denied.
- Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.
- System components that store cardholder data are not directly accessible from untrusted networks.

- The disclosure of internal IP addresses and routing information is limited to only authorized parties.

1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE

- Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE. (eg. personal firewall)
- Specific configuration settings are defined to prevent threats being introduced into the entity’s network.
- Security controls are actively running.
- Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.

Requirement 2 – Apply Secure Configurations to All System Components

Policy Statement:

Encytro is committed to ensuring that all system components are configured and managed securely to protect the confidentiality, integrity, and availability of cardholder data. This policy outlines the requirements for secure configuration and management of system components in compliance with PCI DSS v4.0 Requirement 2.

Procedure:

2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood

- All security policies and operational procedures identified in Requirement 2 are documented, reviewed annually, and communicated to all relevant parties.
- Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.

2.2 System components are configured and managed securely

- Configuration standards are developed, implemented, and maintained to cover all system components and address all known security vulnerabilities. The standards are consistent with industry-accepted system hardening standards or vendor hardening recommendations and updated as new vulnerability issues are identified.
- Vendor default accounts are managed by changing the default password per Requirement 8.3.6 or by removing or disabling the account if not used.
- Primary functions requiring different security levels are managed by isolating them from each other or securing them to the level required by the function with the highest security need.

- Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.
- Insecure services, protocols, or daemons are documented, and additional security features are implemented to reduce the risk of using them.
- System security parameters are configured to prevent misuse.
- All non-console administrative access is encrypted using strong cryptography.

2.3 Wireless environments are configured and managed securely

- For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or confirmed to be secure, including default wireless encryption keys, passwords on wireless access points, SNMP defaults, and any other security-related wireless vendor defaults.
- Wireless encryption keys are changed whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary, or whenever a key is suspected of or known to be compromised.

Requirement 3 – Protect Stored Account Data

Policy Statement:

Encytro is committed to protecting sensitive cardholder data in accordance with the Payment Card Industry Data Security Standard (PCI DSS) v4.0. This policy outlines the requirements for protecting cardholder data in storage, transmission, and processing.

Procedure:

3.1 Processes and mechanisms for protecting stored account data are defined and understood.

- All security policies and operational procedures identified in Requirement 3 are documented, reviewed annually, and communicated to all relevant parties.
- Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.

3.2 Storage of account data is kept to a minimum

- Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following
  - Coverage for all locations of stored account data
  - Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization.
  - Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.
  - Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.

  - Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
  - A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.

3.3 Sensitive authentication data (SAD) is not stored after authorization

- SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.
- The full contents of any track are not retained upon completion of the authorization process.
- The card verification code is not retained upon completion of the authorization process.
- The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.
- SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.
- Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is:
  - Limited to that which is needed for a legitimate issuing business need and is secured.
  - Encrypted using strong cryptography.

3.4 Access to displays of full PAN and ability to copy PAN is restricted

- PAN is masked when displayed (the BIN 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 BIN and last four digits of the PAN.
- When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.

3.5 Primary account number (PAN) is secured wherever it is stored

- PAN is rendered unreadable anywhere it is stored by using any of the following approaches:
  - One-way hashes based on strong cryptography of the entire PAN.
  - Truncation (hashing cannot be used to replace the truncated segment of PAN).
    - If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an

    environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN.
  - Index tokens.
  - Strong cryptography with associated key-management processes and procedures.
- Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.
- If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows:
  - On removable electronic media
  - OR
  - If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.
- If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows:
  - Logical access is managed separately and independently of native operating system authentication and access control mechanisms.
  - Decryption keys are not associated with user accounts.
  - Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.

3.6 Cryptographic keys used to protect stored account data are secured

- Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include:
  - Access to keys is restricted to the fewest number of custodians necessary.
  - Key-encrypting keys are at least as strong as the data-encrypting keys they protect.
  - Key-encrypting keys are stored separately from data-encrypting keys.
  - Keys are stored securely in the fewest possible locations and forms.
- Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes:
  - Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date.
  - Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.

  - Description of the key usage for each key.
  - Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.
- Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times:
  - Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key.
  - Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device.
  - As at least two full-length key components or key shares, in accordance with an industry-accepted method.
- Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.

3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented

- Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.
- Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.
- Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.
- Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following:
  - A defined cryptoperiod for each key type in use.
  - A process for key changes at the end of the defined cryptoperiod.
- Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when:
  - The key has reached the end of its defined cryptoperiod.
  - The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known.
  - The key is suspected of or known to be compromised.
  - Retired or replaced keys are not used for encryption operations.

- Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control.
- Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.
- Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.
- Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.

Requirement 4 – Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

Policy Statement:

Encytro is committed to protecting cardholder data during transmission over open, public networks. To achieve this, we implement strong cryptography and security protocols as outlined in PCI DSS v4.0 Requirement 4.

Procedure:

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented

- All security policies and operational procedures identified in Requirement 4 are documented, reviewed annually, and communicated to all relevant parties.
- Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.

4.2 PAN is protected with strong cryptography during transmission

- Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks:
  - Only trusted keys and certificates are accepted.
  - Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked.
  - The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.

  - The encryption strength is appropriate for the encryption methodology in use.
- An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.
- Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.
- PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.

Requirement 5 – Protect All Systems and Networks from Malicious Software

Policy Statement:

Encytro will implement processes and mechanisms to protect all systems and networks from malicious software and phishing attacks, in accordance with PCI DSS v4.0 Requirement 5. This includes deploying anti-malware solutions on all system components except for those identified as not at risk for malware, performing periodic scans, continuous behavioral analysis of systems or processes, and automatic scans of removable electronic media. In addition, processes and automated mechanisms will be in place to detect and protect personnel against phishing attacks.

Procedure:

5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood

- All security policies and operational procedures identified in Requirement 5 are documented, reviewed annually, and communicated to all relevant parties.
- Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.

5.2 Malicious software (malware) is prevented, or detected and addressed

- An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.
- The deployed anti-malware solution(s):
  - Detects all known types of malware.
  - Removes, blocks, or contains all known types of malware.
- Any system components that are not at risk for malware are evaluated periodically to include the following:
  - A documented list of all system components not at risk for malware.
  - Identification and evaluation of evolving malware threats for those system components.

  - Confirmation whether such system components continue to not require anti-malware protection.
- The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored

- The anti-malware solution(s) is kept current via automatic updates.
- The anti-malware solution(s):
  - Performs periodic scans and active or real-time scans.
  - OR
  - Performs continuous behavioral analysis of systems or processes.
- If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.
- For removable electronic media, the anti-malware solution(s):
  - Performs automatic scans of when the media is inserted, connected, or logically mounted,
  - OR
  - Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.
- Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.
- Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.

5.4 Anti-phishing mechanisms protect users against phishing attacks

- Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.

Requirement 6 – Develop and Maintain Secure Systems and Software

Policy Statement:

Encytro must establish, maintain, and adhere to policies and procedures that govern the secure development of all payment applications, including those developed in-house, commercial software purchased by the organization, and custom software developed by third parties. Encytro will implement secure coding practices throughout the software development lifecycle to ensure that all software developed and/or maintained by "Company" is free from common coding vulnerabilities that could result in unauthorized access to sensitive cardholder data.

Procedure:

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood

- All security policies and operational procedures identified in Requirement 6 are documented, reviewed annually, and communicated to all relevant parties.
- Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.

6.2 Bespoke and custom software are developed securely

- Bespoke and custom software are developed securely, as follows:
    - Based on industry standards and/or best practices for secure development.
    - In accordance with PCI DSS (for example, secure authentication and logging).
    - Incorporating consideration of information security issues during each stage of the software development lifecycle.
- Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:
    - On software security relevant to their job function and development languages.
    - Including secure software design and secure coding techniques.
    - Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.
- Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows:
    - Code reviews ensure code is developed according to secure coding guidelines.
    - Code reviews look for both existing and emerging software vulnerabilities.
    - Appropriate corrections are implemented prior to release.
- If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:
    - Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices.
    - Reviewed and approved by management prior to release.
- Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks

and related vulnerabilities in bespoke and custom software, including but not limited to the following:

  - Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.
  - Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.
  - Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.
  - Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).
  - Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.
  - Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

6.3 Security vulnerabilities are identified and addressed

- Security vulnerabilities are identified and managed as follows:
  - New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
  - Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
  - Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
  - Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.
- An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.
- All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:
  - Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.

  - All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).

6.4 Public-facing web applications are protected against attacks

- For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows:
  - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:
    - At least once every 12 months and after significant changes.
    - By an entity that specializes in application security.
    - Including, at a minimum, all common software attacks in Requirement 6.2.4.
    - All vulnerabilities are ranked in accordance with requirement 6.3.1.
    - All vulnerabilities are corrected.
    - The application is re-evaluated after the corrections
- OR
  - Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows:
    - Installed in front of public-facing web applications to detect and prevent web-based attacks.
    - Actively running and up to date as applicable.
    - Generating audit logs.
    - Configured to either block web-based attacks or generate an alert that is immediately investigated.
- For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:
  - Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.
  - Actively running and up to date as applicable.
  - Generating audit logs.
  - Configured to either block web-based attacks or generate an alert that is immediately investigated.
- All payment page scripts that are loaded and executed in the consumer’s browser are managed as follows:
  - A method is implemented to confirm that each script is authorized.
  - A method is implemented to assure the integrity of each script.

  - An inventory of all scripts is maintained with written justification as to why each is necessary.

6.5 Changes to all system components are managed securely

- Changes to all system components in the production environment are made according to established procedures that include:
  - Reason for, and description of, the change.
  - Documentation of security impact.
  - Documented change approval by authorized parties.
  - Testing to verify that the change does not adversely impact system security.
  - For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
  - Procedures to address failures and return to a secure state.
- Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.
- Pre-production environments are separated from production environments and the separation is enforced with access controls.
- Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
- Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.
- Test data and test accounts are removed from system components before the system goes into production.

Requirement 7 – Access Control

Policy Statement:

Encytro recognizes the critical importance of access control to protect sensitive data and maintain a secure environment. Access to systems and data must be restricted to authorized individuals only, and access controls must be in place to ensure that only those with a business need to access can gain entry.

Procedure:

7.1 – 7.3 Data and System Access

Encytro will ensure that the Access Control policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives:

- All security policies and operational procedures identified in Requirement 7 are documented, reviewed annually, and communicated to all relevant parties.
- Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.
- Access control model is defined and includes granting access:
  - Depending on business and access needs
  - System componets and data resocures that is based on users' job classification and functions
  - Least privileges requreied to preform a job function
- Access is assigned to users, including privileges users is based on job classificaiton, function, and lease privileges necessary to preform job responsibilities.
- Required privileges are approved by authorized personnel.
- All user accounts and related access privileges, including third-party/vendor accounts, are reviewed
  - At least once every six months
  - Accounts and access remin appropriate based on job funcitons
  - Management acknowledges that access reminas appropriate
- All application and system account and related access privileges are assigned and managed.
- All users access to query repositiories of stroed cardholder data is restricted via applications, programmatic methods, and allowed actions bases on user roles and least privileges.
- Only responsibiles administrator(s) can directly access or query repositories of stored CDH.
- Access control systems have a default *Deny All* setting.
- Security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

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

Categories of Information:

- **Public**: This classification relates to data assets that pose no adverse risk to the Encytro, and/or do not fit into the other categories below. Regardless, a user must receive approval from Encytro's Public Relations Department before distributing any Public data.

- **Private**: This classification relates to personal data assets that are intended for internal Encytro use only. Erroneous distribution of Private data could adversely impact Encytro. Private data often includes intellectual property, working designs, or policies and procedures.
- **Sensitive**: This classification relates to business-related data assets that are intended for internal Encytro use only. Erroneous distribution of Sensitive data could impact Encytro, stockholders, business partners, and customers. Sensitive data often includes audit reports and market research.
- **Confidential**: This classification relates to data assets that pose the most risk to Encytro, including passwords, bank account information, cardholder data, and encryption keys.

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

Access to network systems and data must be limited to those employees who have been properly authorized. As such, Encytro adheres to the concept of Role-Based Access Control (RBAC), which results in users being assigned privileges based on a job classification or function. Each user will be authorized to view a certain classification level. All access must be configured to authorize only the data each user needs for their specific position or business role. Every user must be authorized to access Encytro's systems. Authorization pertains to the user's business role and will only be authorized when necessary to fulfill said role.

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

This is the general workflow for requesting access to data:

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

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

Requirement 8 – User Identification and Authentication

Policy Statement:

Encytro is committed to maintaining the highest level of security and confidentiality of its information systems and data. As such, it is essential to implement and maintain effective user identification and authentication procedures to ensure that only authorized personnel have access to our systems and data.

Procedure:

8.1 – 8.3 Assign unique user IDs and require user authentication

- All security policies and operational procedures identified in Requirement 8 are documented, reviewed annually, and communicated to all relevant parties.
- Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.

Each authorized user will be given a unique account name. The user will create a secret password, utilizing the comprehensive password parameters put in place by Encytro. In addition, all Encytro systems must authenticate via passwords.

Authorized Encytro personnel will be responsible for the addition, deletion, and modification of user IDs and credentials. Inactive user accounts will be removed or disabled within 90 days of inactivity.

Encytro employees or third-party vendors must incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.

In addition, multi-factor authentication is required for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity’s network.

Two-factor authentication employs two of the three following authentication methods:

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

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

Authorized Encytro personnel will actively manage those IDs used by third-party vendors as follows:

- Vendor access will be enabled only during the time period needed and disabled when not in use.

- Vendor access will be intently monitored when in use by all appropriate means.

Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system componets

Invalid authentication attemps are limited by

- Locking out the user ID after no more than 10 attemps
- Lockout duration duration configuration to a minimum of 30 mintues or until the user's identiy is confirmed.

Password Policy

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

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

- Delete inactive users after a period of 90 days.
- Authenticate every account (meaning all users, systems, and applications) with a password.
- Require passwords of at least 12 characters, which include a combination of both numbers and letters.
- Identify every user by their unique account name:
- Mandate that a user account will be locked out of the system after 6 failed attempts to connect. The account will remain locked for at least 30 minutes or until a Systems Administrator unlocks it.
- Require that new passwords not be the same as the previous four passwords.
- Passwords must be changed every 90 days.
- Require that the system disconnect a user after an idle time of 15 minutes.

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

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

Passwords stored in any system components within the cardholder data environment or that are transmitted over the network must be rendered unreadable at all times using strong cryptography.

Any Encytro employees or vendors that have network access must have that access immediately revoked once their relationship with Encytro is severed for whatever reason.

8.4 MFA is implemented to secure access into the CDE

MFA (Multi-factor authentication) is required for all access to Encytro CDE, including remote network access from outside <Compnay> network and non-console access for personnel with administrative access. This applies to all users, administrators, third parties, and vendors.

8.5 MFS is configured to prevent misuse

MFA systems implemented include at least two authentication factors, with success required for access. These systems cannot be bypassed by any users unless authorized by management on an exception basis. Additionally, the MFA system must not be susceptible to replay attacks.

Requirement 9 – Physical Security

Policy Statement:

Encytro recognizes the critical importance of physical security to protect sensitive data and maintain a secure environment. Physical security controls must be implemented and maintained to ensure that access to system components and sensitive data is restricted to authorized individuals only.

Procedure:

9.1 Restricting physical access to cardholder data is defined and understood

- All security policies and operational procedures identified in Requirement 8 are documented, reviewed annually, and communicated to all relevant parties.
- Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.

9.2 – 9.3 Physical access controls handling visitors

Indivudual physical access to Encytro senstivie areas within the CDE is monitored with either video cameras or physical access control mechanisms.

Physical and logical controls are in place to restrict use of publicly accessible network jacks, while physical access to wireless access points, networking/communications hardware, and telecommunication lines is restricted within the facility. Additionally, access to consoles in sensitive areas is restricted by locking them when not in use.

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

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

The ID badge area, Encytro datacenter and other restricted areas must display a Visitor Log. Anyone accessing these areas must complete an entry in the log, and include:

Name, Date, Firm or Department, and the Name of the employee who authorized the access. This Visitor Log information must be stored for at least 3 months.

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

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

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

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

9.4 Store, inventory and secure media containing sensitive data securely

To ensure Encytro security of cardholder data, all media with such information is physically secured, and offline backups are stored in a secure location. The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months, and all media with cardholder data is classified according to its sensitivity. Media with cardholder data sent outside the facility is logged, sent by a secured courier or other tracked delivery method, and approved by management. To maintain accountability, inventory logs of all electronic media with cardholder data are maintained, and inventories are conducted at least once every 12 months.

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

Hardcopy Media

Hardcopy media are physical representations of media. Examples of hardcopy materials include paper reports, printer ribbons, fax transmissions, receipts etc. Storage of these materials is subject to the following guidelines:

- Removal of hardcopy materials from Encytro offices is prohibited.
- Removal of hardcopy materials from Encytro data centers or computer rooms is prohibited without prior approval from the Information Security Department.

- Any hardcopy material containing consumer data (confidential or sensitive) must be stored only at approved Encytro facilities/offices, and only for the minimum time necessary.
- Any hardcopy material containing confidential or sensitive material must be clearly labeled.
- All hardcopy media containing confidential or sensitive information must be securely stored in a locked container. Lockers, cabinets, storage bins and locked desks are acceptable, but must first be approved by the Information Security Department. These materials are never to be stored in an unlocked or insecure container.

Electronic Media

Electronic media are the bits and bytes contained in in electronic media devices. Examples of such devices include hard drives, RAM, ROM, CDs, DVDs, floppy disks, hard disks, USB thumb drives, backup tapes, etc. Any electronic media devices that store confidential or sensitive information must follow these guidelines:

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

Media Inventory

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

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

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

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

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

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

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

9.5 Media Device Protection and Training for Personnel

All devices that are capable of reading, storing, processing, and/or transmitting cardholder data must be rendered secure at all times to prevent unauthorized procurement of said devices. As such, Encytro has established the following procedures to ensure the safety and security of such devices.

Authorized personnel will maintain a list of all devices that read, store, process, and/or transmit cardholder data, which will include the following information:

- Make and model of device
- Physical address/location of device
- Any form of unique identification (e.g., serial number)

In addition, they will perform periodic inspections of these devices to ensure that they have not been tampered with or altered.

In the event that devices are added, removed, relocated, or decommissioned, the list of devices will be updated accordingly.

On an annual basis, Encytro will provide comprehensive security awareness training for personnel to be mindful of any attempted tampering or altering of media devices.

Requirement 10 – Logging and Auditing

Policy Statement:

Encytro recognizes the importance of effective logging and auditing practices to monitor and detect unauthorized access, data breaches, and other security incidents. To ensure that sensitive data is protected and security incidents are identified and responded to promptly, Encytro will implement and maintain a comprehensive Logging and Auditing policy that covers all systems and components that store, process, or transmit cardholder data.

Procedure:

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

- All security policies and operational procedures identified in Requirement 10 are documented, reviewed annually, and communicated to all relevant parties.
- Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.

10.2 Events Logged

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

- Invalid logical access attempts.
- All user access to cardholder data.
- Creation or deletion of system-level objects.
- All administrative actions utilizing user IDs with access above-and-beyond that of a general user (e.g., root, oracle, administrative privileges).
- Access or initialization of audit log files.
- Use of changes to identification and authentication mechanisms.
- Any increase or elevation of privileges.
- All changes, additions, or deletions to any account with root or administrative privileges.
- Any user or admin authentication attempts (either valid or invalid).

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

- Name of the affected data, system component or resource
- User ID
- Origination location of event
- Type of event
- Date and Time that event occurred
- Result of the event (success/failure)

10.3 Protect from unauthorized modification and destruction

Audit log files are protected to prevent modifications by individuals. Audit log files, including those for externalfacing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify. File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.

10.4 Review of Security Logs and Events

Encytro attests that the following items are to be reviewed by authorized personnel on a daily basis in order to identify any suspicious activities or irregularities:

- All security events
- Logs of all systems that store, process, or transmit cardholder data or sensitive authentication data
- Logs of all critical system components
- Logs of all servers and system components that perform security functions

In addition, authorized personnel will periodically review logs of all other system components and follow up on any suspicious activity or irregularities identified during the review process.

10.5 Audit Trails and Log Security

All event logs must be securely stored in a centralized location or on a storage device that is protected from unauthorized access. The logs will only be accessed and viewed by those individuals with a job-related need. Current audit trail files are to be protected from unauthorized modifications via access control mechanisms or segregation (physical and/or network). Wireless logs must be copied onto a log server housed on the internal LAN. Furthermore, the Information Security Department must establish a file integrity monitoring (FIM) system that will alert personnel in the event either unauthorized access to logs or modification of logs occurs.

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

10.6 Network Time Protocol (NTP)

The ability to compare log files from different systems and establish an exact sequence of events is vital for forensic analysis in the event of a breach. Therefore, time-synchronization technology is to be implemented and kept current in accordance with PCI DSS Requirement 6.1 and 6.2. All Encytro production systems, with the exception of Encytro's internal NTP servers, must be configured to utilize the internal NTP server for time synchronization purposes.

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

10.7 Review of Critical Security Control Systems

Encytro has established processes in place that aid in ensuring the timely detection and reporting of failures of critical security systems. These include, but are not limited to, the following:

- Firewalls
- IDS/IPS
- FIM

- Anti-virus
- Physical access controls
- Logical access controls
- Audit logging mechanisms
- Segmentation control

Encytro has established processes in place for responding to a security control failure. These include, but are not limited to, that include the following:

- Restoring security functions
- Identifying and documenting the duration (date and time start to end) of the security failure
- Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause
- Identifying and addressing any security issues that arose during the failure
- Performing a risk assessment to determine whether further actions are required as a result of the security failure
- Implementing controls to prevent cause of failure from reoccurring
- Resuming monitoring of security controls

When documenting security control failures, Encytro personnel will make sure to identify the root cause of the failure, the duration of the security failure (date and time start and end), and will provide details of the remediation required to address the root cause.

Requirement 11 – Regularly Test Security Systems and Processes

Policy Statement:

Encytro acknowledges the importance of regularly testing security systems and processes to identify vulnerabilities and ensure that all security controls are effective. To maintain the security of cardholder data and comply with PCI DSS Requirement 11, Encytro will implement and maintain a comprehensive security testing and vulnerability management program.

Procedure:

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

- All security policies and operational procedures identified in Requirement 11 are documented, reviewed annually, and communicated to all relevant parties.

- Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.

11.2 Scan for rogue wireless devices

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

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

11.3 Vulnerability Scans

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

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

If vulnerability scans uncover potential vulnerabilities, the appropriate Encytro personnel must be notified so remediation efforts may begin. Personnel must follow the Change Control Policy to correct high-level vulnerabilities. Additional scans must then be performed in order to confirm compliance with Encytro security standards. In the event that the vulnerability cannot be remediated or mitigated, personnel must document the reason why it cannot, and proceed accordingly with any other compensating control.

11.4 Vulnerability Penetration Testing

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

Network layer penetration tests must include all components that support network functions and operating systems. In addition, testing must include internally and externally accessible IPs.

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

http://www.owasp.org

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

- Insecure Configuration Management

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

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

If segmentation is used to isolate the cardholder environment, penetration testing must be performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods.

- The penetration testing covers all segmentation controls/methods in use.
- The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.
- The penetration testing must be performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).

11.5 Use Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS)

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

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

11.5 Detect and respond to changes on payment pages

To detect and prevent unauthorized modification, a change-and tamper-detection mechanism is deployed with several funtions. These functions include altering personnel to any unauthorized changes, additons, or deletions to the HTTP headers and payment page content as received by the consumer browers, evaluating the received HTTP header and payment page, and preforming these fucntions at least every seven days or periodically.

Requirement 12 – Maintain an Information Security Policy

Policy Statement:

Encytro recognizes that maintaining an effective information security policy is essential for protecting cardholder data and ensuring compliance with PCI DSS. To maintain the security of cardholder data and comply with PCI DSS Requirement 12, Encytro will implement and maintain a comprehensive Information Security Policy.

Procedure:

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

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

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

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

12.2 Acceptable Usage Policy (AUP)

Policy Applicability

The proper use of critical technologies by authorized individuals designated by Encytro will be clearly defined by their AUP. This policy must be followed by all users of critical Encytro technologies, whether employees, contractors or third parties. Exemptions may only be authorized with written approval from the Chief Security Officer.

These employee-facing technologies consist of system components as well as IT resources that are regarded as critical by any organization. Examples of such technologies include:

- Operating systems
- Network devices
- Databases
- Applications
- Wireless technologies
- Remote access technologies

- Removable electronic media
- Computers (desktops and/or laptops)
- Cell phones
- Internet use
- Email Use
- Social Media websites and applications

Encytro attests that this particular policy will be updated as needed in the future to reflect any new critical technologies and their intended uses.

Approval

Integration or use of critical technologies must be authorized by the Information Security Department, based on job function. The Information Security Department is responsible for maintaining a list of company-approved critical technologies. The list should identify the acceptable use and network locations for the technologies. Approvals must be documented in the Authorization Request Form.

Authentication

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

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

Device Inventory

The Information Security Department must maintain a list of the critical devices in use. The list of devices should include the following, at minimum:

- Device owner and contact information
- List of personnel authorized to use the
- The purpose/function of the device

Remote Access Technologies

Remote access technologies must be configured to disconnect after a specific period of inactivity. Remote access technologies for business partners should be activated only when needed by the vendors and business partners, with immediate deactivation after use.

Credit Card Data Access

For personnel accessing cardholder data via remote-access technologies, it is prohibited to copy, move, or store cardholder data onto local hard drives or removable electronic media unless explicitly authorized for a defined business need. Where there is an authorized business need, the data must be protected in accordance with all applicable PCI DSS Requirements

12.3 Annual Risk Assessment process

Encytro will engage in a risk assessment process that is performed at least annually and upon significant changes to their environment. This assessment process will identify critical assets, threats, and vulnerabilities, and will result in a formal, documented analysis of risk.

Typical risk factors include:

- Threat
- Vulnerability
- Impact
- Likelihood
- Predisposing Condition

SEE: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

12.5 Document and validate in scope systems

As part of Encytro commitment to comply with the Payment Card Industry Data Security Standard (PCI DSS), an up-to-date inventory of all system components that are in scope, including a description of their function and use, is maintained. The scope of our PCI DSS is documented and confirmed at least once every 12 months and whenever there is a significant change to our in-scope environment.

To validate the PCI DSS scope, all data flows for payment stages and acceptance channels are identified, data-flow diagrams are updated, and all locations where account data is stored, processed, and transmitted are identified. This includes locations outside the defined CDE, applications that process CHD, transmissions between systems and networks, and file backups.

Additionally, all system components within or connected to the CDE that could impact its security, and all segmentation controls in use, along with the environments from which the CDE is segmented, including justification for any out-of-scope environments, are identified.

It is also necessary to identify all connections from third-party entities with access to the CDE and to confirm that all identified data flows, account data, system components, segmentation controls, and connections from third parties are included in the scope. By completing these steps, compliance with the PCI DSS is maintained and the security of payment card data is ensured.

12.6 Formal security awareness program

The Encytro Chief Security Officer will oversee and the Information Security Department will execute security awareness training for all Encytro personnel. Initial training must be provided for personnel upon hire and periodic refresher training must occur annually at a minimum. The method of delivery as well as the topics can vary depending upon the audience. The Information Security Department will determine and approve training methods and topics. Where training is performed in a group setting, a sign-in sheet will be circulated for attendees to record their attendance. The Human Resources department will maintain a record of sign-in sheets.

12.7 Employee background checks

New hire candidates for positions requiring access to sensitive systems and applications involving credit card data, a background check will be ordered by the Human Resources Department. Furthermore, Encytro's Human Resources new hire process includes documentation that states what initiatives are conducted regarding background checks.

12.8 Third-party management – due care and due diligence

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

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

12.9 Documented acknowledgement of responsibility (Only applicable if Encytro is a service provider)

Encytro will provide in writing to customers, acknowledgement that they are responsible for the security of cardholder data that Encytro possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

12.10 Incident response plan

Incident Identification

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

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

- Unusual system behavior, such as unscheduled system reboots or abnormal errors in system log files/terminals).

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

Reporting and Incident Declaration Procedures

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

To maintain the integrity of both the incident investigation and recovery process, the Information Security Department’s personnel should be the sole investigating and remediating agent. However, when a possible security incident is noticed the employee should do the following as soon as possible:

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

Incident Severity Classification

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

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

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

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

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

Typical Response

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

- Level 1

Contain the Incident and Monitor for Changes.

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

- Level 2

Contain the Incident, Monitor for Changes and Warn Others.

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

made. If a Encytro employee is found to be the culprit, management should work with Human Resources to appropriately address the Acceptable Use violation.

- Level 3

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

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

Credit Card Companies – Special Response

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

1. The Information Security Department must first contain and/or eliminate the threat and avoid further exposure. A thorough investigation into the security breach must be performed within 24 hours of the incident. These steps should be taken to assist the investigation:
    a. Document all steps/actions taken.
    b. During the transfer of any materials or information related to the investigation, employees must utilize chain of custody techniques.
    c. Do not log on to the affected systems, change any passwords or otherwise access/alter the systems. Do not log on as ROOT.
    d. Do not turn the affected system off. It is important to isolate any compromised systems from the network. Isolation can be achieved by unplugging the network cable, deactivating switch ports or isolating the system to a contained environment (e.g., isolated VLAN). Disaster Recovery/Business Continuity procedures should be used to recover any lost or disabled business processes.
    e. Archive or store all logs and other electronic evidence.

   f. Change the wireless network SSID on the AP and other non-compromised machines (if applicable).
   g. Maintain vigilant to any additional threats and monitor all cardholder information systems.

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

- Visa

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

- Mastercard

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

- American Express

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

- Discover Card

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

- JCB

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

Root Cause Analysis and Lessons Learned

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

Plan Testing and Training

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

Automated Security System Notifications

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

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

12.11 Security review policies and procedures

Encytro attests that all applicable policies, procedures, and processes are reviewed at least quarterly to confirm that personnel are following Encytro security policies and operating procedures. These reviews must encompass the following processes:

- Daily log reviews
- Firewall rule-set reviews
- Applying configuration standards to new systems
- Responding to security alerts
- Change management processes

12.11.1 Maintenance of quarterly review documentation process

(Only applicable if Encytro is a service provider)

Encytro will maintain any documentation related to quarterly reviews confirming that personnel are following Encytro security policies and operating procedures. This documentation will contain the signature of designated Encytro personnel who is responsible for their PCI DSS compliance program.

Reviews must cover the following processes:

- Daily log reviews
- Firewall rule set reviews
- Applying configuration standards to new systems
- Responding to security alerts
- Change management processes

Additional requirement for service providers only: Maintain documentation of quarterly review process to include:

- Documenting results of the reviews.
- Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program

Appendix A – Periodic Operational Security Procedures

Task	Daily	Monthly	Quarterly	Bi-Annually	Annually
Policy and Procedures Review					X
Enterprise Risk Analysis					X
Security Awareness Training					X
Verify PCI DSS Compliance Status of Third Parties					X
Test Incident Response Plan					X
Employee Acknowledgement and Acceptance of Security Policies					X
Review Firewall Rule Sets				X	
Review System Access Controls				X	
Review Access Request Approvals and Audit Trail				X	

Audit Disposal of Data and Media (including Hardcopy)			X		
Audit Terminated Employees for System, Network, Application, Physical Access			X		
Incident Response Review and Training					X
Conduct Internal and External Vulnerability Scans			X		
Conduct Penetration Testing				6 Month Segmentation Test	X
Review all Logs	X				
Scan for Rogue Wireless Devices			X		
Install Critical Security Patches		X			
Disable Inactive Accounts			X		

Appendix B – System Configuration Record

<table>
<tr><th colspan="6">GENERAL SYSTEM INFORMATION</th></tr>
<tr><td colspan="2"><b>System Name:</b></td><td colspan="2"><b>System Purpose:</b></td><td colspan="2"><b>Build Date:</b></td></tr>
<tr><td colspan="3"><b>Build Engineer:</b></td><td colspan="3"><b>Comments:</b></td></tr>
<tr><th colspan="6">IP INFORMATION</th></tr>
<tr><td colspan="2"><b>IP Address:</b></td><td colspan="2"><b>Subnet Mask:</b></td><td colspan="2"><b>Default Gateway:</b></td></tr>
<tr><td colspan="2"><b>DNS/WINS Entries:</b></td><td colspan="2"><b>Domain:</b></td><td colspan="2"><b>Other Settings:</b></td></tr>
<tr><th colspan="6">OPERATING SYSTEM</th></tr>
<tr><td colspan="3"><b>Operating System:</b></td><td colspan="3"><b>Version:</b></td></tr>
<tr><td colspan="3"><b>Date Patched to:</b></td><td colspan="3"><b>Patch Exceptions:</b></td></tr>
</table>

System Hardened: ϒ Yes ϒ No	**Hardened by Which Standard:**

Hardening Exceptions:

Document Number: **Reason for Exception:**

______________________ ____

______________________ ____

APPLICATION (ATTACH ADDITIONAL SHEETS FOR OTHER ENTRIES)

Operating System and Applications:	**Version:**
Date Patched to:	**Patch Exceptions:**
System/Application Hardened: ϒ Yes ϒ No	**Hardened by Which Standard:**

Hardening Exceptions:

Document Number: **Reason for Exception:**

______________________ ____

______________________ ____

NOTES

Additional Comments / Notes:

Appendix C – Change Request Form

PART I (To be filled out by the Lead Requestor)

Type of Request: ϒ Initial Request ϒ Updated Request	**Office:** ANC Electronics N Services https://www.anc-electronics-n-services.net

Name (Last, First, MI): **Williams, Angela M**	**Phone Number:** **352-480-9856**	**Date:** 2/7/2026

Type of Change:

ϒ New Implementation ϒ Repair ϒ Removal ϒ Emergency ϒ Patch

ϒ Other: connecting several sites to allow customers to access all our services in one spot._

Description of Change:

We are building still but will have everything up and running by next month hopefully. Thank you for your patience in this change and look forward to doing business with you very soon.

Recurring Change: ϒ Yes, add to calendar ϒ No	**Requested Implementation Window:**

Systems Affected by Change:	**Users Affected by Change:**	**Documentation Attached:** ϒ Test Plan ϒ Back out Plan

Resources That May be Affected by Change: ϒ Customers ϒ Internal Dept. ϒ Other Explain: ________________________________	**Criticality of Change:** ϒ High ϒ Medium ϒ Low Explain: ______________________________

PART II (To be completed by Management)

Review Date:	**Review Participants:**
Test Plan Review: ϒ Acceptable ϒ Further Action is Required	**Back Out Plan Review:** ϒ Acceptable ϒ Further Action is Required
Resource Review: ϒ Acceptable ϒ Further Action is Required	**Schedule Review:** ϒ Acceptable ϒ Further Action is Required

Comments:			
Part III (To be completed by Management after approval)			
Approval Date:		**Approved Implementation Date:**	
Supervising Official Certification:			
Name:	**Phone:**	**Signature:**	**Date:**
______________________	_______________	_____________________	______________

Appendix D – Acceptable Use Policy

Overview

Encytro's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to its established culture of openness, trust and integrity. Encytro is committed to protecting its 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 Encytro. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Encytro 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 Encytro. These rules are in place to protect the employee and Encytro. Inappropriate use exposes Encytro to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Encytro business or interact with internal networks and business systems, whether owned or leased by Encytro, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Encytro and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Encytro policies and standards, and local laws and regulation.

This policy applies to employees, contractors, consultants, temporaries, and other workers at Encytro, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Encytro.

Policy

General Use and Ownership

Encytro proprietary information stored on electronic and computing devices whether owned or leased by Encytro, the employee or a third party, remains the sole property of Encytro. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Standard.

- You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Encytro proprietary information.
- You may access, use or share Encytro proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- 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.
- For security and network maintenance purposes, authorized individuals within Encytro may monitor equipment, systems and network traffic at any time.
- Encytro reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.

- System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.
- Postings by employees from a Encytro email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Encytro, unless posting is in the course of business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of 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 Encytro authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Encytro-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:

- 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 Encytro.
- 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 Encytro or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting Encytro business, even if you have authorized access, is prohibited.
- 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 export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- 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.
- Using a Encytro computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Encytro account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- 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.

- Port scanning or security scanning is expressly prohibited unless prior notification to Encytro is made.
- 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.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the Encytro network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- 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.
- Providing information about, or lists of, Encytro employees to parties outside Encytro.

Email and Communication Activities

- When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department.
- 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).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- 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.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Encytro's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Encytro or connected via Encytro's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Media

- Blogging by employees, whether using Encytro’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Encytro’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Encytro's policy, is not detrimental to Encytro's best interests, and does not interfere with an employee's regular work duties. Blogging from Encytro's systems is also subject to monitoring.

- Encytro's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Encytro confidential or proprietary information, trade secrets or any other material covered by Encytro's Confidential Information policy when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Encytro and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Encytro's *Non-Discrimination and Anti-Harassment* policy.
- Employees may also not attribute personal statements, opinions or beliefs to Encytro when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Encytro. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Encytro's trademarks, logos and any other Encytro intellectual property may also not be used in connection with any blogging activity

Policy Compliance

Compliance Measurement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by the Information Security team in advance.

Non-Compliance

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

02/04/2026

____
Date

Angela M. Williams
______________________________ ________________
Acknowledged and Agreed to by (Print Name) Employee ID

Angela Wi

____
Signature