Information Security Policy For

Organization Name

Town of Clyde Park

Organization Name

Enclosed are Town of Clyde Park information security policies. These policies have been developed to protect the information assets of Town of Clyde Park as well as its employees, partners, and customers. Adherence to these policies is mandatory. If you have any questions regarding any of the policies or your responsibilities in implementing them, please contact your supervisor.

Version 1.0

Approval Date: _____

Primary Contact: Stacy Mills Clerk/Treasu

TABLE OF CONTENTS

1. Introduction

The data that resides at Organization Name Town of Clyde Park is of great value to Organization Name Town of Clyde Park. Due to the increasing value of the data we collect, store, process, and share with our partners, it is a high priority for Organization Name Town of Clyde Park to protect such data.

The management of Organization Name Town of Clyde Park is committed to developing, adopting, and maintaining appropriate information security policies, standards, and procedures. This ensures integration of information security with Organization Name Town of Clyde Park 's mission, business strategy, risk posture, and in accordance with applicable regulatory guidelines. This will be accomplished by:

- Active Organization Name Town of Clyde Park board and management oversight.
- Effective management and monitoring of information security risks.
- Delineation of clear accountability for information security.
- Establishing appropriate organizational processes to ensure that information security risks are appropriately and regularly identified, monitored, and controlled.

This policy applies to all Organization Name Town of Clyde Park employees, contractors, service providers, and vendors. Additionally, this policy is supported by daily operational security procedures that have been developed in conjunction with it.

This policy is necessary to:

- Maintain Organization Name Town of Clyde Park compliance with applicable laws and standards.
- Protect Organization Name Town of Clyde Park from liability.
- Protect the confidentiality, integrity, and availability of Organization Name Town of Clyde Park
- information systems, data, and network resources.

Organization Name Town of Clyde Park 's information security policy represents the combined efforts of Organization Name Town of Clyde Park 's Information Services Department (IS), Human Resources Department (HR), Legal Department, and user communities.

Organization Name Town of Clyde Park may make changes to this policy at any time.

Reference: PCI DSS v3.2 requirements 12.4

Document Approval

Date of Last Review	Name and Title of Approver
04/22/2026	Stacy Mills Clerk/Treasurer

2. Definitions

Availability	Ensuring that information systems, data and network resources are available and ready for use when they are needed.
Confidentiality	The protection of data from unauthorized disclosure.
Contractor	Use standard Organization Name Town of Clyde Park definition
DMZ	Demilitarized zone; network added between a private and a public network to provide an additional layer of security.
Employee	Use standard Organization Name Town of Clyde Park definition
Emergency Change	An urgent or critical change that should occur outside of the Organization Name Town of Clyde Park 's formal change-management process.
Encryption	Process of converting data into an unintelligible form except to holders of a specific cryptographic key.

Information System	Information systems include, but are not limited to, laptop computers, workstations, servers, mainframe computers, routers, switches, cell phones, telephones, and fax machines.
Integrity	The accuracy, completeness, and validity of information.
Logical Controls	Controls that limit logical access to information systems and/or electronic data. For example, passwords, user accounts, and firewall rules.
Malicious software	Software designed to damage or disrupt information systems, data, or network resources.
Network Resource	Communication links and network bandwidth.
Physical Controls	Controls that are physically implemented. Example: surveillance cameras, motion alarms, door locks, and security guards.
Risk	The likelihood of a given threat causing a vulnerability, and the resulting impact of that adverse event on an organization.
Security Incident	Attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or services used or provided by _____.
Sensitive Areas	Any data center, server room, or area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale (POS) terminals are present, such as the cashier areas in a retail store.

Sensitive Data	Includes, but is not limited to: • Passwords • Social Security numbers • Credit card information • Protected Health Information (PHI) • Personally Identifiable Information (PII) • Bank account numbers • Tax ID numbers that are stored, processed, or transmitted on or by the Organization Name information systems or network resources
Strong Cryptography	A cryptographic algorithm or protocol that makes it very difficult for an unauthorized person to gain access to encrypted data.
Threat	A condition that may cause information or information-processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of Organization Name Town of Clyde Park.
Two Factor Authentication	The use of two independent mechanisms for authentication. (Example: a security token and a password).
User	Anyone who accesses Organization Name Town of Clyde Park information systems, data, or network resources.
Visitor	A vendor, guest of an employee, service personnel, or anyone who needs to enter a Organization Name Town of Clyde Park facility containing information systems, data, or network resources for a short duration, usually not more than one day.

3. Roles and Responsibilities

While responsibility for information security on a day-to-day basis is every Organization Name Town of Clyde employee's duty, specific guidance, direction, and authority for information security is the responsibility of Organization Name Clyde Park 's Chief Security Officer (CSO). The CSO has assigned the day-to-day responsibilities for information security to Organization Name Clyde Park 's Information Services (IS) Department. Accordingly, this Department will:

- Establish, document and distribute information security policies, standards and procedures.
- Monitor and analyze security alerts & information and distribute to appropriate Organization Name Clyde Park employees.
- Establish, document, and distribute security incident response and escalation procedures
- Administer user accounts, including additions, deletions, and modifications
- Monitor and control all access to sensitive data

Reference: PCI DSS v3.2 requirement 12.5 (12.5.1 – 12.5.5)

4. Risk Assessment

Organization Name Clyde Park must regularly identify, define, and prioritize risks to the confidentiality, integrity and availability of its information systems, network resources and data.

Organization Name Clyde Park must conduct an annual formal, documented risk assessment of its information systems, data and network resources. The assessment must identify and prioritize the threats and vulnerabilities to Organization Name Clyde Park 's information systems, data and network resources and define the likelihood and impact of risks.

The risk assessment must be used in conjunction with Organization Name Clyde Park 's risk management process to identify, select and implement appropriate and reasonable controls to protect the confidentiality, integrity and availability of Organization Name Clyde Park 's information systems, network resources and data.

Organization Name Clyde Park must conduct risk management on a regular basis and select and implement reasonable, appropriate and cost-effective controls to manage, mitigate or accept identified risks. All such controls must be commensurate with identified risks.

Annually, Clyde Park ’s Manager of Information Services must submit an information security risk management report to appropriate Clyde Park management. The report must identify the significant risks to Clyde Park information systems, data and network resources that have been identified during the past year, the risks that have been accepted and which risks have been mitigated.

Reference: PCI DSS v3.2 requirement 12.2

5. Network Security

Clyde Park must develop and implement formal, documented standards for its firewalls and routers. Such standards must include:

- A formal process for approving and testing all network connections and changes to Clyde Park firewall and router configurations.
- A current diagram(s) of Clyde Park ’s computer network. The diagram must show all connections to Clyde Park information systems that process, transmit or store sensitive data. Changes to the diagram(s) must be appropriately documented.
- Requirements for a firewall at each logical point where Clyde Park ’s network connects to the Internet and between any demilitarized zone (DMZ) and Clyde Park ’s internal network(s).
- A description of groups, roles and responsibilities for logical management of Clyde Park firewalls and routers.
- Documentation and business justification of all services, protocols and ports allowed by Clyde Park firewalls and routers, including documentation of security features implemented for insecure protocols (e.g. Telnet, FTP).
- A requirement to review Clyde Park firewall and router rule sets at least every six (6) months.

Clyde Park ’s firewalls must perform stateful inspection and must restrict connections between untrusted networks (i.e. the Internet) and Clyde Park information systems that process, transmit or store sensitive data. The firewalls must prohibit direct access from the Internet to such information systems, must restrict inbound and outbound traffic to that which is documented as necessary for organizational purposes and explicitly deny all other traffic.

Configuration files on Organization Name Clyde Park routers must be secured and regularly synchronized.

A firewall(s) must be installed between any wireless networks and Organization Name Clyde Park information systems that process, transmit or store sensitive data. Such firewalls must deny or control traffic from any wireless networks to these information systems.

Outbound traffic from Organization Name Clyde Park payment card applications must be sent to IP addresses within a Organization Name Clyde Park DMZ; such traffic must not be sent directly to the Internet. Inbound Internet traffic to Organization Name Clyde Park payment card applications must be limited to IP addresses within a Organization Name Clyde Park DMZ.

All Organization Name Clyde Park databases that store sensitive data must be placed in the Organization Name Clyde Park 's internal network(s) and be segregated from any Organization Name Clyde Park DMZ.

Personal firewall software must be installed and active on any mobile and/or Organization Name Clyde Park employee-owned computers with direct connectivity to the Internet that are used to access the Organization Name Clyde Park 's internal network. The personal firewall software must be configured to specific standards and prevent unauthorized users from altering or disabling it.

IP masquerading (e.g., port address translation [PAT] or network address translation [NAT]) must be used for information systems on Organization Name Clyde Park 's internal network(s).

Reference: PCI DSS v3.2 requirements 1.1, 1.2, 1.3, 1.4, 1.5

6. Information System Configuration

Organization Name Clyde Park must develop and implement formal, documented configuration standards for its information systems. Such standards must be consistent with system hardening best practices as defined by organizations such as SANS, NIST and CIS. At a minimum, the standards must require the following:

- One primary function for servers that process, transmit or store sensitive data (virtualization technologies are used, is only one primary function implemented per virtual system component or device)
- Disabling of unnecessary and/or insecure services and protocols
- Appropriate configuration of system security settings
- Removal of unnecessary functionality (e.g., scripts, Web servers, subsystems)
- Changing or removing vendor-supplied defaults (i.e., passwords, accounts, SNMP community strings)

For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:

- Encryption keys changed from default at installation and changed anytime anyone with knowledge of the keys leaves the company or changes positions
- Default SNMP community strings on wireless devices changed at installation
- Default passwords/passphrases on access points changed at installation
- Firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks

Organization Name
All remote logins that enable administrator access to Clyde Park information systems storing, transmitting or processing sensitive data must be encrypted.

Organization Name
Clyde Park must have a formal, documented process to identify newly discovered security vulnerabilities and update Organization Name Clyde Park configuration standards to address new vulnerabilities.

Reference: PCI DSS v3.2 requirements 2.1, 2.2, 2.3, 2.5 and 6.2

7. Data Retention and Disposal

Organization Name
Clyde Park must keep the storage of sensitive data to the minimum necessary required for business, legal and/or regulatory purposes. When no longer required for such purposes, sensitive data on Organization Name Clyde Park information systems or on Organization Name Clyde Park electronic and non-electronic media must be appropriately disposed of. The following disposal methods must be used:

- Non-electronic media must be cross-cut shredded, incinerated or pulped.
- Electronic media must be purged, degaussed, shredded or otherwise destroyed so that sensitive data cannot be reconstructed.

Organization Name
Sensitive data on Clyde Park electronic media and information systems must be securely and thoroughly erased before such items can be re-used.

Organization Name
Clyde Park information systems and electronic & non-electronic media that contain sensitive data must be inventoried and audited on a quarterly basis to ensure that the stored data does not exceed Organization Name Clyde Park 's data retention requirements.

After a payment card transaction is authorized, the following types of data must never be

stored in electronic or non-electronic form at a Organization Name Clyde Park facility:

- Magnetic stripe data
- CVC2/CVV2/CID/CAV2
- PIN/PIN Block

Unless otherwise authorized, credit card primary account numbers (PANs) on Organization Name Clyde Park information systems must be masked; the first six (6) and the last four (4) digits of the PAN are the maximum that can be displayed.

PANs stored electronically on Organization Name Clyde Park information systems or portable storage devices must be made unreadable. One of the following methods must be used:

- Strong one-way hash functions
- Truncation
- Index tokens and pads
- Strong cryptography

Cryptographic keys must be securely stored and comply with the following key management procedures:

- Generation of strong keys
- Maintenance of an inventory of encryption keys
- Secure key distribution
- Periodic key changes
- Destruction of old keys
- Split knowledge and dual control of keys
- Prevention of unauthorized substitution of keys
- Replacement of known or suspected compromised keys
- Revocation of old or invalid keys

Key custodians must sign a form specifying that they understand and accept their key-custodian responsibilities.

Reference: PCI DSS v3.2 requirements 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, and 9.8

8. Transmission of Data

If sensitive data must be sent over an open, public network (i.e., the Internet), strong cryptography such as TLS 1.2, or IPSEC must be used to encrypt the data.

Organization Name

If a Clyde Park wireless network is used to transmit sensitive data, strong encryption (i.e. WPA2 or IPSEC) must be used.

Strong cryptography must be used whenever sensitive data is sent via end-user messaging technologies (e.g., email, instant messaging, chat).

Reference: PCI DSS v3.2 requirements 4.1, 4.2

9. Malicious Software Protection

Organization Name

Clyde Park must deploy anti-virus software on its information systems commonly affected by malicious software. Such software must be capable of detecting, removing and protecting against malicious software including spyware and adware.

All Anti-virus signatures are to be kept current and the software must be kept actively running and capable of generating audit logs. Anti-virus software must be enabled for automatic updates and conduct periodic scans.

Reference: PCI DSS v3.2 requirements 5.1, 5.2, 5.3, 5.4.

10. Patch Management

Organization Name

Clyde Park must have a formal, documented process for regularly identifying and prioritizing relevant and necessary security and functional patches for its information systems and applications that process, transmit or store sensitive data.

Organization Name

Clyde Park may use a risk based approach for prioritizing security patch installations. All critical new security patches must be applied within one month of release.

This process includes:

- Using reputable outside sources for vulnerability information
- Assigning a risk ranking to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities

Reference: PCI DSS v3.2 requirements 6.1, 6.2

11. Change Control

Organization Name
Clyde Park must develop and implement a formal, documented change control process for information system and software configuration changes. The process must include:

- Identification and documentation of significant changes
- Assessment of the potential impact, including security implications, of significant changes
- Appropriate management approval of all changes
- Ability to terminate and recover from unsuccessful changes
- Testing procedures to ensure the change is functioning as intended
- Communication of completed change details to appropriate persons
- The updating of appropriate information system or software documentation upon the completion of a significant change
- Upon completion of a significant change, ensure all relevant PCI DSS requirements implemented on all new or changed systems and networks, and documentation updated as applicable

Only properly authorized persons may make an emergency change to Organization Name Clyde Park information systems, data or network resources. Such emergency changes must be appropriately documented and promptly submitted, after the change, to Organization Name Clyde Park 's normal change management process.

Reference: PCI DSS v3.2 requirements 6.4

12. Software Application Development

When Organization Name Clyde Park develops software applications that store, process or transmit sensitive data (" Organization Name Clyde Park developed applications"), such applications must be developed per a formal, documented software development life cycle and be based on information security best practices.

Security patches and system & software configuration changes on Organization Name Clyde Park developed applications must be tested before being deployed. Testing must include at least:

- Validation of all input
- Validation of proper error handling
- Validation of secure cryptographic storage
- Validation of secure communications
- Validation of proper role based access control

Organization Name
Clyde Park must have separate development, test and production environments for Organization Name
Clyde Park developed applications that process, transmit or store sensitive data. There must be clear separation of duties between the three environments. Real sensitive data must not be used or must be sanitized for testing or development of Organization Name
Clyde Park developed applications.

Test data and accounts must be removed before Organization Name
Clyde Park developed applications are placed into Organization Name
Clyde Park 's production environment. Custom code used in Organization Name
Clyde Park developed applications must be reviewed for vulnerabilities before the code is used in Organization Name
Clyde Park 's production environment.

Web applications developed by Organization Name
Clyde Park that process, transmit or store sensitive data (" Organization Name
Clyde Park developed Web applications") must be based on secure coding best practices such as the Open Web Application Security Project (OWASP) guidelines. Organization Name
Clyde Park developed Web applications must be protected against the following vulnerabilities:

- Malicious file execution
- Insecure direct object references
- Cross-site request forgery (CSRF)
- Information leakage
- Improper error handling
- Insecure cryptographic storage
- Insecure communications
- Inadequate authentication and session management
- Cross-site scripting (XSS) attacks
- Failure to restrict URL access
- Injection flaws

All Internet accessible Organization Name
Clyde Park Web applications that process, transmit or store sensitive data must be protected against known attacks by either: having an organization specializing in application security review the applications at least annually using manual or automated application vulnerability security assessment tools or methods or by installing a web-application firewall in front of the applications.

Reference: PCI DSS v3.2 requirements 6.3, 6.5, 6.6

13. Logical Access Control

Organization Name
Clyde Park employees, contractors, council members, service providers and vendors must not attempt to gain logical access to Clyde Park information systems, data or network resources for which they have not been given proper authorization.

Organization Name
Logical access to Clyde Park information systems and media containing sensitive data must be denied until specifically authorized by appropriate Clyde Park personnel.

Organization Name
Appropriate Clyde Park information system owners and/or data custodians or their designated delegates must define and approve logical access to Clyde Park information systems and media containing sensitive data.

Organization Name
Logical access to Clyde Park information systems and media must be provided only to those having a business need for specific access in order to accomplish a legitimate task and must be based on the principles of need to know and least possible privilege. All access to any database containing cardholder data (including access by applications, administrators, and all other users) restricted as follows:

- All user access to, user queries of, and user actions on (for example, move, copy, delete), the database through programmatic methods only (for example, through stored procedures)
- User direct access to or queries to databases restricted to database administrators
- Application IDs only able to be used by the applications (and not by individual users or other processes)

Organization Name
Clyde Park must have a formal, documented user management process which enables the controlled addition, change and termination of logical access rights on Clyde Park information systems, data and network resources. The process must be capable of granting different levels of access to Clyde Park data, information systems and network resources.

Organization Name
A unique user name must be used by all persons accessing Clyde Park information systems and media containing sensitive data. Along with the unique user name, one of the following authentication methods must be used:

- Password
- Token devices

- Biometrics

When other authentication mechanisms are used (for example, physical or logical security tokens, smart cards and certificates, etc.), the use of these mechanisms are assigned as follows:

- Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts
- Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access

Multi-factor authentication must be used by employees, contractors, service providers and vendors for remote access to Organization Name Clyde Park information systems and media containing sensitive data. Organization Name Clyde Park employees who telecommute must take all precautions necessary to secure any and all sensitive Organization Name Clyde Park data in their homes and prevent unauthorized access to any Organization Name Clyde Park information system or data.

Multi-factor authentication incorporated for all nonconsole access into the CDE for personnel with administrative access

Vendor maintenance ports on Organization Name Clyde Park information systems that contain sensitive data must be disabled until the specific time they are needed by the vendor. After appropriate use by the vendor, they must again be disabled.

Group, shared or generic accounts or passwords must not be used on Organization Name Clyde Park information systems that store, process or transmit sensitive data. The following requirements must be met for passwords on such systems:

- User passwords must be changed at least every 90 days.
- Passwords must be at least 7 characters long and include both numeric and alphabetic characters.
- First time passwords must be unique for each user and must be changed upon first use.
- Password reuse must be restricted to no more than once every 4 uses.
- Via the use of strong cryptography, all passwords must be unreadable during transmission and storage on all information systems that store, process or transmit sensitive data.
- User accounts must be locked after six failed login attempts. The lockout must be for at least 30 minutes or until authorized Organization Name Clyde Park personnel unlock the account.

- Organization Name Clyde Park employees must not use passwords that are also used for non-
- Organization Name Clyde Park accounts.

Activation of information system locking software or log off must occur when a user session on a Organization Name Clyde Park information system is inactive for more than 15 minutes.

User identity must be appropriately verified before any password, which enables access to a Organization Name Clyde Park information system or network resource, is reset.

User accounts that are inactive for more than 90 days on Organization Name Clyde Park information systems that store, process or transmit sensitive data must be disabled or removed.

At least every 6 months, appropriate Organization Name Clyde Park information system owners and/or data custodians or their designated delegates must review and verify logical access rights to Organization Name Clyde Park information systems and media containing sensitive data. Such rights must be revised as necessary. Inactive accounts over 90 days old must be either removed or disabled.

Organization Name Clyde Park employees and contractors experiencing a change in status (e.g. termination, position change) must have their logical access rights promptly reviewed, and if necessary, modified or revoked.

Reference: PCI DSS v3.2 requirements 7.1 (7.1.1 – 7.1.4), 7.2 (7.2.1 – 7.2.3) 7.3, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8

14. Physical Access Control

At least annually, Organization Name Clyde Park must identify all of its physical areas that must be protected from unauthorized physical access. The assessment must take into consideration areas where sensitive data is stored, processed, or transmitted as well as the location of any supporting assets or critical infrastructure.

Organization Name Clyde Park information systems and electronic & non-electronic media containing sensitive data must be located in physically secure areas (“limited access area”). Typically, such areas have a defined security perimeter such as a card controlled entry door or a staffed reception desk. Organization Name Clyde Park information systems located in unrestricted, public access areas must be physically secured to prevent theft.

Access to limited access areas must be denied until specifically authorized by appropriate Organization Name Clyde Park personnel. Such access must be provided only to those having a need for

specific access in order to accomplish a legitimate task and must be based on the principles of need to know and least possible privilege. Access privileges to limited access areas must be reviewed at least annually.

Cameras or other access control mechanisms must monitor the entry and exit points of Organization Name Clyde Park physical areas containing information systems that store, process or transmit sensitive data or electronic and non-electronic media containing sensitive data. Camera data must be stored for at least three (3) months unless otherwise restricted by law.

Organization Name Clyde Park must control and restrict physical entrance to publicly accessible network jacks; it must also restrict physical entrance to wireless access points (WAPs), gateways and handheld devices located at Organization Name Clyde Park facilities.

Backup media, both paper and electronic, that contains sensitive Organization Name Clyde Park data must be stored in a secure location. The location's security must be reviewed at least annually. An inventory of all such media must be conducted at least annually.

Organization Name Clyde Park electronic and non-electronic media containing sensitive data must be classified so that it can be identified as "confidential." Distribution of such media outside the Organization Name Clyde Park must be tracked and logged. Such media must only be distributed outside Organization Name Clyde Park via a delivery method that can be tracked.

Appropriate Organization Name Clyde Park management must approve the movement of any Clyde Park media containing sensitive data from a limited access area.

Organization Name Clyde Park must have a formal, documented process in place that clearly identifies and distinguishes between employees, contractors, and visitors.

Visitors to limited access areas must be formally authorized by an appropriate Organization Name Clyde Park employee to access such areas. Visitors to limited access areas must be given a physical token (i.e., a badge) that has an expiration date and that identifies a visitor as a non-employee. Visitors must return their physical token upon leaving a limited access area or at the expiration date.

Visitors must sign a visitor's log prior to being granted physical access to limited access areas. The log must document the visitor's name, the company represented, the authorizing Organization Name Clyde Park employee, and the date & time of entrance and departure. Unless otherwise restricted by law, visitor logs must be retained for at least three (3)

months.

Devices that capture payment card data via direct physical interaction with the card protected are against tampering and substitution as follows:

- An inventory of all devices is maintained that contains the device make and model, location, serial number, date installed, and date of device inspection (previous 18 months).
- Devices are periodically inspected to look for tampering or substitution
- Inventory is to be audited periodically to ensure accuracy

Reference: PCI DSS v3.2 requirements 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.9.1, and 9.10

15. Logging and Auditing

Appropriate logging and monitoring controls must be implemented on Clyde Park information systems, data and network resources.

Organization Name

Clyde Park must implement automated audit trails on its information systems that store, process or transmit sensitive data. The audit trails must be able to reconstruct the following events:

- Individual accesses to sensitive data
- Actions taken by any individual with root or administrative privileges
- Access to audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of audit logs
- Creation and deletion of system-level objects

For each of the above events, the following must be recorded:

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

Organization Name
Logs and audit trails on Clyde Park information systems that store, process or transmit sensitive data must be reviewed daily. Such logs and audit trails must be monitored by file integrity or change detection software. Log reviews must include intrusion detection and authentication, authorization and accounting (AAA) servers.

Organization Name
Information generated by logging and monitoring controls implemented on Clyde Park information systems, data and network resources must be protected from unauthorized access. Access to such information must be limited to only those individuals with a need-to-know. Such information must be promptly backed up to a centralized log server and/or media that is difficult to alter. Logs for Clyde Park external-facing technologies (i.e., firewalls, DNS, email) must be copied onto a log server on the Clyde Park 's internal network. Unless otherwise restricted by law, audit and log file information must be retained for at least one year.

Organization Name
Clyde Park information systems must have their system clocks and times synchronized with a master time source (e.g. network time protocol [NTP]). Internal Clyde Park time servers must not all receive time signals from external sources. Specific Internet time servers must be designated from which time updates will be accepted.

Reference: PCI DSS v3.2 requirements 10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.9

16. Information Security Testing

Organization Name
Clyde Park must annually, or after any significant changes to its information technology environment, perform internal and external penetration tests of its information systems that process, transmit or store sensitive data. The penetration tests must include both network, application layer tests, and validate network segmentation is in place and functioning correctly.

Organization Name
At least quarterly, a wireless analyzer must be used at Clyde Park facilities to identify all wireless devices in use or a wireless IDS/IPS must be deployed which is capable of identifying all wireless devices in use at Clyde Park facilities.

Organization Name
Clyde Park must use a PCI SSC certified Approved Scan Vendor (ASV) to conduct appropriate quarterly external vulnerability scans against all of its information systems that are Internet reachable. Clyde Park must also run quarterly internal vulnerability scans against all of its information systems that process, transmit or store sensitive data.

Issues identified on both the external and internal vulnerability scans must be fixed in accordance with Organization Name Clyde Park Patch Management policy and retested to ensure that the patch is in place and functioning properly.

Per its risk assessment, Organization Name Clyde Park must implement and maintain network IDS, host based IDS and/or IPSs to monitor all traffic to Organization Name Clyde Park information systems that process, transmit or store sensitive data.

Organization Name Clyde Park must deploy file integrity monitoring software on its information systems that process, transmit or store sensitive data. The software must perform critical file comparisons at least weekly.

Reference: PCI DSS v3.2 requirements 11.1, 11.2, 11.3, 11.4, 11.5, 11.6

17. Policy Distribution and Review

This policy must be published and distributed to all appropriate Organization Name Clyde Park employees, contractors, vendors, service providers and business partners.

This policy must be reviewed at least annually and revised as necessary.

Reference: PCI DSS v3.2 requirements 12.1

18. Employee Technologies

Employee technologies (i.e., remote-access technologies, wireless technologies, removable electronic media, laptops, PDAs) that access sensitive Organization Name Clyde Park data must only be used by employees and contractors if the following controls are in place:

- Appropriate Organization Name Clyde Park management approval for the use of the technologies
- Appropriate authentication is used
- A regularly updated inventory of devices, approved network locations for their use, and list of the persons authorized to access the devices
- Devices are labeled with owner name, contact information, and a description of the device's purpose
- Devices are appropriately used and placed in appropriate network locations
- Organization Name Clyde Park maintains a regularly updated list of approved devices

When payment card data on Organization Name Clyde Park information systems is remotely accessed, the data must not be copied, moved, or stored onto local hard drives or removable electronic media.

Remote access sessions to Organization Name Clyde Park information systems containing sensitive data must be disconnected after twenty (20) minutes of inactivity. Remote access technologies used by vendors to access Organization Name Clyde Park information systems containing sensitive data must be turned off when not in use by the vendors.

Reference: PCI DSS v3.2 requirements 12.3

19. Security Training and Awareness

Organization Name Clyde Park must ensure that employees and contractors are provided with sufficient training and supporting reference materials to enable them to appropriately protect Organization Name Clyde Park information systems, network resources, and data. Organization Name must provide information security awareness to its employees and contractors upon hire and then at least annually.

Organization Name Clyde Park must provide regular security information and awareness to its employees and contractors via methods such as log-in banners, posters, memos and periodic meetings. Such information and awareness must include, but is not limited to:

- Any significant revisions to Organization Name Clyde Park information security policies
- Any significant new Organization Name Clyde Park information security controls or processes
- Any significant changes to Organization Name Clyde Park information security controls or processes
- Any significant new security threats to Organization Name Clyde Park information systems, network resources, or data
- Information security best practices

Personal with access to POS devices are to be trained to be aware of attempted tampering or replacement of devices, to include the following:

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace or return devices without verification.
- Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).

- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel.

Employees must acknowledge, at least annually, that they have read and understood Organization Name Clyde Park 's information security policy.

Reference: PCI DSS v3.2 requirements 9.9.3, 12.6 (12.6.1 – 12.6.2), 12.7

20. Personnel Vetting

As determined necessary by Organization Name Clyde Park 's risk assessment, new Organization Name Clyde Park employees must be adequately vetted before being hired. Such vetting can include, but is not limited to, background checks, credit checks and/or personal references. Such vetting is especially important for positions that involve access to sensitive data.

New employees who will access sensitive data must sign a confidentiality (non-disclosure) agreement. This agreement must be regularly renewed.

Reference: PCI DSS v3.2 requirements 12.7

21. Service Provider Management

If Organization Name Clyde Park shares sensitive data with service providers, then Organization Name Clyde Park must develop and maintain a service provider management program that meets, at minimum, the following requirements:

- Maintenance of a list of service providers.
- Written acknowledgement from each service provider confirming they are responsible for the security of the sensitive data they possess or have access to.
- An established process for engaging service providers that includes proper due diligence prior to engagement.
- Development and maintenance of a program to monitor service providers' PCI DSS compliance.

Reference: PCI DSS v3.2 requirement 12.8

22. Security Incident Response

Organization Name
Clyde Park must have a formal, documented security incident response plan. The plan must include:

- Roles, responsibilities and communication strategies in the event of a security incident including notification of appropriate parties
- Specific incident response procedures
- Business recovery and continuity procedures
- Data back-up processes
- Legal requirements for reporting security incidents
- Coverage and responses for all critical Organization Name Clyde Park information systems
- Reference or inclusion of payment card brand incident response procedures
- Procedures for responding to alerts from intrusion detection (IDS), intrusion prevention (IPS) and/or file integrity monitoring systems

The security incident response plan must be tested annually and must designate specific personnel to be available on a 24/7/365 basis in order to respond promptly to information security alerts. The plan must be reviewed regularly and modified as necessary.

Organization Name
Clyde Park employees who are responsible for responding to security incidents must receive regular and appropriate training in security incident response processes.

Reference: PCI DSS v3.2 requirements 12.10

23. Compliance

Organization Name
Clyde Park employees and contractors must comply with all applicable parts of this security policy. Compliance is necessary to ensure the confidentiality, integrity and availability of Organization Name Clyde Park information systems, data and network resources.

Organization Name
Clyde Park employees and contractors who do not comply with all applicable Organization Name
Clyde Park security policies may be subject to disciplinary actions, up to and including termination of employment.

Third party persons (i.e. vendors, service providers) who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements.

Appendix A - Sample Policy Acknowledgment

Organization Name

I have received a copy of Clyde Park 's Information Security Policy and I have read and understand the policy. I agree to observe the terms and conditions of this policy.

Signed Name _____

Printed Name _____

Date _____

Appendix B – Terminal Inventory Worksheet

Device Name	Make/ Model	Location	Serial Number	Date Inspected	Inspector's Name
Sample One	*VeriFone vx 520*	*Store 3 -123 Main Street Anytown USA*	*5/20/20xx*	*2.14.2014*	*Tom Jones*

Appendix C – Terminal Inspection Checklist

Name of Inspector	
Inspector Signature	
Date of Inspection	

#	Inspection Criteria	Yes	No	Comment
1	Is the POS terminal and its PED in its designated location?			
2	Is the POS terminal's manufacturer name and/or model number correct?			
3	Is the POS terminal serial number correct? Merchants must maintain a record of all serial numbers along with model numbers assigned to each of its acceptance locations, by register lane if applicable?			
4	Is the number of POS terminals in use the same as the number of devices installed or assigned?			
5	Is the color and condition of the POS terminal as expected with no additional marks or scratches, especially around the seams or terminal window display?			
6	Are the manufacturer's security seals and labels present with no signs of peeling or tampering?			
7	Are the manufacturer's security markings and reference numbers as described?			

8	Is the number of connections to the POS terminal as expected, with the same type and color of cables, and with no loose wires or broken connectors?			
9	Is the number of connections entering the POS terminal as expected?			

Appendix D - Service Provider Summary Worksheet

#	Name of Service provider	Services Provided	PCI DSS Requirements Involved	Does Agreement Contain PCI DSS Language	Date of Last Review Completed
1	*Service Provider X*	*WebHosting*	*1.1,1.2,9.1-9.9, 11.2-11.3*	*Yes*	*11/15/20xx*
2					
3					
4					
5					
6					
7					
8					
9					
10					

Appendix E - Service Provider Checklist

Name of Service Provider:	
Name of Employee completing review:	
Employee Signature:	
Date Review Completed:	

#	Review Criteria	Yes	No	Comment
1	Is there a current contract in force with this service provider that requires them to store, process, and transmit cardholder data in a PCI DSS compliant Manner?			
2	Did the service provider provide references and have they been checked?			
3	Was an internet search conducted to see if the vendor has suffered a recent security incident or has pending litigation for non-performance of contract?			
4	Was a copy of the service providers SSAE 16 review provided?			

5	Which PCI DSS Requirements are being managed by this service provider:			
6	Requirement 1 - Install and maintain a firewall configuration to protect cardholder data			
7	Requirement 2 - Do not use vendor supplied default for system passwords and other security parameters			
8	Requirement 3 - Protect stored cardholder data			
9	Requirement 4 - Encrypt transmission of cardholder data over open (public) networks			
10	Requirement 5 - Protect all systems against malware and regularly update anti-virus software programs			
11	Requirement 6 - Develop and maintain secure systems and applications			
12	Requirement 7 - Restrict access to cardholder data by business need to know			
13	Requirement 8 - Identify and authenticate access to system components			
14	Requirement 9 - Restrict physical access to cardholder data			

15	Requirement 10 - Track and monitor all access to network resources and cardholder data			
16	Requirement 11 - Regularly test security systems and processes			
17	Requirement 12 - maintain a policy that addresses information security for all personnel			
18	Has this service provider provided an attestation of compliance that incudes services listed above?			
19	Has this service provider provided written acknowledgement that they are responsible for maintaining compliance for the services above?			