2018.1

PCI Data Security Standards Policy

Responsible Executive: Chief Executive Officer, Golden Communications, Inc.

Issued: June 1, 2018

Last Updated: June 26, 2018

Policy Statement

Golden Communications, Inc. [GoldenComm] is committed to developing and maintaining appropriate information security policies, standards, and procedures to ensure adherence with GoldenComm's mission, business strategy, risk posture, and applicable regulatory guidelines. This policy focuses on safeguarding data as it pertains to the Payment Card Industry Data Security Standard (PCI DSS).

Reason for Policy

This policy is necessary in order to maintain GoldenComm's compliance with applicable laws and standards, to protect GoldenComm from liability, and to protect the confidentiality, integrity, and availability of GoldenComm's information systems, data, and network resources.

Entities Affected by this Policy

This policy applies to all GoldenComm employees, contractors, service providers, and vendors. Additionally, this policy is supported by operational security processes and procedures that have been developed in conjunction with this policy.

Who Should Read this Policy

All employees, contractors, service providers, and vendors of GoldenComm who are processing credit card transactions either in electronic or paper form. This also applies to any of the above mentioned that may access services or systems deemed to be part of the cardholder data environment (CDE).

Web Address of this Policy

https://www.goldencomm.com/private/PCI-DSS-Policy

Contacts

Direct any questions about this policy, *2018.1 – PCI Data Security Standards Policy*, to Casey Deveau, Information Technology Security Manager, using one of the methods below:

Phone: 949-574-5500

Email: cdeveau@goldencomm.com

Contents

1. Information Security Policy

GoldenComm is committed to developing, adopting, and maintaining appropriate information security policies, standards, and procedures to ensure integration of information security with GoldenComm's mission, business strategy, risk posture, and in accordance with applicable regulatory guidelines.

This will be accomplished by active executive and management oversight, effective management and monitoring of information security risks, delineation of clear accountability for information security, and establishing appropriate organizational processes to ensure that information security risks are appropriately and regularly identified, monitored, and controlled.

This policy applies to all GoldenComm employees, contractors, service providers, and vendors. Additionally, this policy is supported by operational security procedures that have been developed in conjunction with this policy.

This policy is necessary in order to maintain GoldenComm's compliance with applicable laws and standards, to protect GoldenComm from liability, and to protect the confidentiality, integrity, and availability of GoldenComm's information systems, data, and network resources.

This policy focuses on safeguarding data as it pertains to the Payment Card Industry Data Security Standard (PCI DSS).

1.01 Roles and Responsibilities

Relevant PCI DSS 3.2 Requirements: 12.4, 12.5 (12.5.1 – 12.5.5)

Securing the cardholder data environment at GoldenComm involves many teams within the organization as well as external vendors and contractors.. This section identifies general roles and responsibilities as it pertains to building, configuring, implementing, and maintaining GoldenComm's cardholder data environment.

- **Chief Executive Officer**

  The Chief Executive Officer, Jason Lavin (JL), provides oversight to the policies and standards in accordance with applicable laws and standards to help the organization secure GoldenComm's data and information systems. The Chief Executive Officer is responsible for establishing an appropriate level of visibility for these policies and information risk to the organization.

- **Chief Technology Officer**

  The Chief Technology Officer, Andrew Nguyen (AN), is responsible for complying with security policies within the organization. The Chief Technology Officer manages and monitors information systems that support GoldenComm's information security infrastructure, and is responsible for maintaining awareness of the security of the resources managed by working with the Special Operations Team, and assures that security related activities are well documented and completed in a consistent and auditable manner. The Chief Technical Officer is responsible for periodic reevaluation of current operational methods to identify possible areas for improvement in security. The Chief Technology Officer will evaluate security risks to new and existing systems with the Information Technology Security Manager in accordance with this policy. The Chief Technology Officer must assure that appropriate security controls are implemented commensurate with the acceptable level of risk.

- **Information Technology Security Manager**

  The Information Technology Security Manager, Casey Deveau (CD), is responsible for developing and implementing strategy for security and compliance within the organization and serves as a liaison for regulatory compliance in the organization. The Information Technology Security Manager develops policies, standards, and guidelines for securing information systems. In addition, the Information Technology Security Manager conducts risk assessments and analysis in accordance with applicable laws and standards to help the organization secure GoldenComm's data and information systems. Risk findings, including non-compliant and vulnerable systems, may be reported to the The Chief Technology Officer. The Information Technology Security Manager reserves the right to restrict access to vulnerable systems. It is the Information Technology Security Manager's responsibility to ensure that corrective action plans are completed and information system integrity is not compromised.

- **Administrators of Cardholder Data Environment**

  Individuals who manage GoldenComm's cardholder data environment are responsible for complying with policies that govern the security of the resources they manage. The Information Technology Security Manager will establish protocols with the Systems Administrators to ensure that appropriate security controls are implemented as specified in this document and related technical hardening guidelines. Systems Administrators provide information to the Information Technology Security Manager to facilitate risk assessment activities, and are responsible for implementing corrective actions as recommended. In addition, System Administrators are responsible for maintaining sufficient documentation about system configuration, maintenance, and overall management of information systems.

Individuals who provide access to GoldenComm's cardholder data environment are responsible for ensuring the appropriate training and authorization requests have been completed prior to providing access. In addition, such individuals are responsible for conducting periodic access reviews as it pertains to audit and regulatory requirements.

- **Department Leads**

  Department Leads are responsible for ensuring that all individuals review and comply with the requirements set forth in this policy. In addition, these individuals are responsible for helping to maintain an adequate inventory of all equipment and serve as a point of contact for the Special Operations Team as it pertains to processing credit card transactions.

- **Payment Card Processors**

  All individuals responsible for handling and processing credit card payments on behalf of GoldenComm or its affiliated entities are required to review, understand, and acknowledge the requirements set forth in this policy.

1.02 Policy Development and Maintenance

Relevant PCI DSS 3.2 Requirements: 12.1 (12.1.1), 12.3 (12.3.1 – 12.3.10)

This policy must be published and distributed to all appropriate GoldenComm employees, contractors, vendors, service providers, and business partners.

This policy must be reviewed at least annually and revised as necessary. It must also be reviewed and revised at a time of major change to the cardholder data environment or update to the PCI DSS standards.

The following acceptable use controls must be followed to ensure proper usage of the cardholder data environment:

- Access to the systems and resources in the cardholder data environment require explicit approval and authorization by the Information Technology Security Manager. Such authorization must be in accordance with the individual's job responsibilities, and the individual must complete the appropriate training administered by the Department Leads.

- All individuals accessing systems within the cardholder data environment must use their own uniquely assigned ID and password. No individual should access the cardholder data environment through the use of a shared or generic ID. Passwords or active sessions to any system must never be shared with another individual.

- The Special Operations Team must maintain an inventory of all assigned credit card swipe devices and other electronic payment systems in use at various department and office locations. All deployed devices should be tagged in the asset management system.

- All individuals with access to the cardholder data environment must be maintained in a centralized repository. If a credit card swipe device is individually assigned, this relationship must also be maintained in the asset inventory. One individual should be designated as the appropriate contact person in order for maintenance and reconciliation of the device inventory.

- Any deployment of new products for the use of processing credit card transactions must be reviewed, assessed, and approved by the Special Operations Team.

- Cardholder data should not be copied or removed from the cardholder data environment (all data must be contained within the secure environment). Access controls must be in place to prohibit such action by any authorized individual, including access from a remote location.

1.03 Service Providers and Incident Response

Relevant PCI DSS 3.2 Requirements: 12.8 (12.8.1 – 12.8.5), 12.9, 12.10 (12.10.1 – 12.10.6)

A list of known service providers and a description of the service provided should be maintained centrally and reviewed for accuracy on an annual basis. The Chief Technology Officer and the Special Operations team will work together to maintain this list.

The list of service providers should be reviewed on an annual basis, or at time of a significant change, to confirm that the providers are compliant with all PCI DSS standards.

The list of service providers should contain a mapping or listing of relevant PCI DSS standards that pertain to each service provider so it is clear which standards pertain to the service provider versus those which pertain to GoldenComm.

Effective with the issuance of this policy and for all newly signed or renewed agreements, all contracts and agreements with service providers must include provisions or acknowledgement that the service providers are responsible for the security of cardholder data they either possess or otherwise store, process or transmit on behalf of GoldenComm, or to the extent that the service providers could impact the security of GoldenComm's cardholder data environment.

A risk assessment should be conducted for any new service providers that will be responsible for possessing, storing, or processing cardholder data on behalf of GoldenComm. At the minimum, members of the Chief Technology Manager and the Information Technology Security Manager should be involved to adequately assess and vet the provider. The risk assessment should include a review of the service providers' policies that demonstrate their commitment to comply with PCI DSS standards.

GoldenComm's Security & Privacy Incident Response Plan must be tested annually and include reporting requirements in the event of a suspected incident or breach involving cardholder data. The GoldenComm Security & Privacy Incident Response Plan includes appropriate provisions for reporting and escalating incidents pertaining to the cardholder data environment and is the authoritative plan as it pertains to this policy document.

2. Secure Network and Systems

2.01 Firewall Configuration

Relevant PCI DSS 3.2 Requirements: 1.1 (1.1.1 – 1.1.7), 1.2 (1.2.1 – 1.2.3), 1.3 (1.3.1 – 1.3.7), 1.4 – 1.5

GoldenComm 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 GoldenComm's firewall and router configurations
- A current network diagram that identifies all connections between GoldenComm's cardholder data environment and other networks, including any wireless networks
- A current diagram that shows all GoldenComm's cardholder data flows across systems and networks; the diagram must be kept current and updated as needed upon changes to the environment
- Requirements for a firewall at each internet connection and between any demilitarized zone (DMZ) and any internal network zone
- A description of groups, roles, and responsibilities for management of GoldenComm's network components
- Documentation and business justification for use of all services, protocols, and ports allowed by GoldenComm's firewalls and routers, including documentation of security features implemented for those protocols considered to be insecure (e.g., FTP, Telnet, POP3, IMAP, and SNMP v1 and v2, TLS)
- A requirement to review GoldenComm's firewall and router rule sets at least every six (6) months

GoldenComm's firewall and router configurations must restrict connections between untrusted networks and any system components in the cardholder data environment. Such configurations must:

- Restrict inbound traffic to only that which is necessary for GoldenComm's cardholder data environment, and specifically deny all other traffic
- Secure and synchronize configuration files across routers and firewalls
- Configure perimeter firewalls between all wireless networks and GoldenComm's cardholder data environment, to deny or— if traffic is necessary for business purposes—permit only authorized traffic between the wireless environment and GoldenComm's cardholder data environment
- Prohibit direct public access between the internet and any system component in GoldenComm's cardholder data environment, such that
    1. A DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports
    2. Inbound public internet traffic is limited to IP addresses within the DMZ
    3. Direct connections inbound between the internet and GoldenComm's cardholder data environment are not allowed
    4. Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering GoldenComm's network

5. Unauthorized outbound traffic from GoldenComm's cardholder data environment to the internet is not allowed
6. A stateful inspection (or dynamic packet filtering) firewall is implemented to allow only "established" connections into GoldenComm's network
7. System components storing GoldenComm cardholder data should be placed in one of GoldenComm's internal network zones and should be segregated from GoldenComm's DMZ and any other untrusted networks
8. Private GoldenComm IP addresses and other internal routing information are not disclosed to unauthorized parties (e.g., masquerading via implementation of NAT, proxies, etc.)
9. Personal host-based firewalls or equivalent software are installed on any device or computer containing, storing, accessing, or transmitting GoldenComm data over the internet; these firewalls need to be configured to prevent unauthorized users from altering or disabling the firewall

---

GoldenComm hosted systems and services that are accepting credit card transactions are in-scope of the greater cardholder data environment. In order to comply with the above requirements to secure the cardholder data environment, any/all remote access to the CDE must leverage an authorized Secure Encrypted VPN connection with Multi Factor authentication. In cases of legacy integrations or non-compliance, a remediation plan must be established and agreed upon by the GoldenComm entity to implement a approved Secure VPN solution within twelve (12) months.

2.02 Default System and Security Parameters

Relevant PCI DSS 3.2 Requirements: 2.1 (2.1.1), 2.2 (2.2.1 – 2.2.5), 2.3 – 2.6

The following configuration items must ensure that:

- Vendor default passwords and other vendor default settings are changed prior to system implementation in order to prevent a system from being compromised by malicious individuals making use of standard configuration parameters
- Default settings for any wireless environments connected to WCM's cardholder data environment must also be changed, including, but not limited to:
    - o encryption keys
    - o shared passwords and administrator passwords
    - o Servers are configured for ***one*** purpose, only
    - o Only necessary services, protocols, daemons, etc. as required for the system's business purpose are enabled
    - o Additional security controls are established and documented for insecure services

All systems in-scope for GoldenComm's cardholder data environment must be inventoried and updated accordingly.

3. Protect Cardholder Data

3.01 Protection of Stored Cardholder Data

Relevant PCI DSS 3.2 Requirements: 3.1, 3.2 (3.2.1 – 3.2.3), 3.3

As GoldenComm has implemented end-to-end encryption for its transmission of cardholder data, no digital cardholder data shall be stored after authorization in the GoldenComm cardholder data environment. For situations where cardholder data is collected in a paper format, the following controls must be adhered to:

- Paper documents containing cardholder data must be redacted of sensitive authentication data (full track data, card validation code or value, and PIN data) after the credit card has been authorized.
- All redacted paper documents may be retained in accordance with the institution or department's data retention policies.
- Any retained paper documents should be reviewed on a yearly basis and documents older than the retention period must be securely shredded.
- In situations where the cardholder's primary account number (PAN) is displayed, the PAN must be masked

such that only the first six or last four digits are displayed. Only personnel with a legitimate business need shall have the authorizations to review the full PAN.

3.02 Encryption of Transmitted Cardholder Data

Relevant PCI DSS 3.2 Requirements: 4.1 (4.1.1), 4.2, 4.3

The GoldenComm cardholder data environment must be isolated and segregated from the rest of the GoldenComm network. In addition, there is no access to the GoldenComm cardholder data environment from unsecure networks, including any wireless technologies.

- Any transmission of cardholder data must be encrypted using strong cryptography and security protocols. The encryption standard must be approved by the OPS Team.
- For any browser-based transactions of cardholder data, the system must be configured to utilize HTTP Secure, over TLS version 1.2 or greater, for encryption. All versions of SSL are considered weak encryption mechanisms and must not be used.
- Cardholder data must never be sent unprotected via email, text message, instant messaging, chat, or other communication protocols. It is strongly recommended to never send sensitive authentication data through these protocols, even with added encryption.

4. Vulnerability Management

4.01 Malware Protection

Relevant PCI DSS 3.2 Requirements: 5.1 (5.1.1, 5.1.2), 5.2 – 5.4

While there are several security monitoring tools in place to detect and protect against the presence of malware (malicious software, including viruses, worms, and trojans) on the GoldenComm network, the cardholder data environment must be configured and monitored accordingly to protect against malware infections.

- The OPS approved antivirus software must be deployed, configured, and activated on all workstations and servers within the cardholder data environment that are handling or processing cardholder data.
- All antivirus clients must be current (within 3 update revisions) with the latest definition updates and rulesets.
- The antivirus software must be configured to generate audit logs at time of detection or quarantine of malware.
- The antivirus software must be capable of performing a periodic scan if initiated by the system administrator.
- The antivirus software must be configured in such a way to prevent other users of the system from disabling or altering the configuration settings.
- Any exceptions or exclusions that result in a temporary or permanent change to the antivirus software must be submitted to the OPS Team for review and implementation.

4.02 Secure Systems and Applications

Relevant PCI DSS 3.2 Requirements: 6.1, 6.2

In order to maintain a secure environment, GoldenComm runs automated vulnerability scans of all systems within the cardholder data environment.

The vulnerability scanning tool is configured such that:

- All systems within the cardholder data environment are scanned on at least a monthly basis
- All systems are categorized and assessed with a risk score based on sensitivity of data, exposure to threats, and likelihood of compromise – all of which are compiled based on outside security metrics and threat bulletins

In addition, all systems are patched with the latest security updates on a monthly basis. Any system that appears to be vulnerable to a threat and has a high likelihood of compromise may be blocked by GoldenComm from accessing the network, including the internet.

5. Access Control

5.01 Logical Access Control Measures

Relevant PCI DSS 3.2 Requirements: 7.1 (7.1.1 – 7.1.4)

Cardholder data can only be accessed by authorized personnel. Access to the cardholder data environment must be restricted on a "need to know" basis to only authorized individuals based on role, job function, and responsibility.

Individuals which process cardholder data must complete the appropriate training courses offered by GoldenComm in order to gain access to the electronic payment modules. Such users must be authorized by a Department Lead in order to complete the training in accordance with their job functions and responsibilities.

Users that do not require access to the cardholder data environment must not be permitted to gain access without proper authorization, Active Directory group membership, or other application and network access control measures.

Access to the cardholder data environment should be reviewed and recertified on an at least an annual basis to ensure authorizations are accurate and reflect current responsibilities.

5.02 Authentication to System Components

Relevant PCI DSS 3.2 Requirements: 8.1 (8.1.1 – 8.1.8), 8.2 (8.2.1 – 8.2.6), 8.3 – 8.5 (8.5.1), 8.6, 8.8

The following controls and requirements apply to ***all*** individuals accessing the cardholder data environment including vendors or other third parties supporting systems or services within the cardholder data environment:

- Access to the cardholder data environment must utilize a uniquely-assigned account
- The uniquely-assigned accounts must be granted access to only the roles and modules required for the purposes of support ("need to know" method)
- All access accounts must be recertified by the OPS Team on a yearly basis; sign-off is required by the sponsor in order to maintain access to the system
- Vendor accounts must only be enabled when required for troubleshooting a support request, responding to an incident, or providing ongoing support for a required business function; accounts can be enabled through the use of a support ticket with OPS Team
- Remote access audit logs may be reviewed at any time by OPS Team in the event suspicious or malicious activity has occurred

Individuals responsible for administering the cardholder data environment must enroll in and utilize GoldenComm's approved multi-factor authentication technology before interactively logging in to a server or system. Remote connections to the cardholder data environment (including those established by vendor support personnel) must also utilize multi-factor authentication for added security.

5.03 Physical Access Control Measures

Relevant PCI DSS 3.2 Requirements: 9.1.2, 9.5, 9.6 (9.6.1 – 9.6.3), 9.7, 9.8 (9.8.1), 9.9 (9.9.1 – 9.9.3)

The following controls must be adhered to in order to ensure adequate physical security around cardholder data:

- Network jacks or wireless access points located in public areas and areas accessible to visitors must not provide direct access to the dedicated cardholder data environment virtual local area network (VLAN).
- Any media containing high risk data, which includes cardholder data, must be physically secured to prevent unauthorized access or disclosure.
- Confidential data must never be left in plain sight. Workstations must be locked when left unattended and cardholder data stored in paper format must be securely stored and locked when unattended.
- Cardholder data must never be transmitted through email. Under extreme circumstances, any data must be sent using modern industry standard encryption.
- An inventory of cardholder data must be maintained, such that the location of cardholder data in electronic and paper formats is known (e.g., specific storage closets, cabinets, servers, or data centers).
- All media containing cardholder data must be destroyed when it is no longer needed for business or legal reasons. Media must be destroyed using an approved technique (disintegrate, pulverize, melt, incinerate, or shred) to ensure cardholder data is not recoverable.

- Devices that capture payment card data via direct physical interaction with the card (e.g., a card swipe or dip device) must be protected from tampering or substitution.
  - Where possible, card swipe devices should be removed at the end of the business day and securely stored in a locked cabinet or office to protect against tampering or substitution.
- All individuals interacting with credit cards and card swipe devices should be aware of and trained against the requirements set forth in this policy to ensure devices have not been tampered with or substituted.

6. Network Monitoring and Testing

6.01 Monitoring of Network Resources

Relevant PCI DSS 3.2 Requirements: 10.1, 10.2 (10.2.1 – 10.2.7), 10.3 (10.3.1 – 10.3.6), 10.5, 10.6 (10.6.1 – 10.6.3),10.7, 10.9

All critical system and network components within the cardholder data environment should be configured to track and record audit logs that link individuals to actions. Logs should be forwarded to the centralized security information and event manager (SIEM) to ensure they are (a) tracked, reviewed, and monitored daily, and (b) stored in a secure location where they cannot be modified.

Automated logs should include the following events in order to reconstruct a timeline in the event of an incident or investigation:

- All individual user accesses to cardholder data, whether at the operating system or application level
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails by any individual
- Individual or denied access attempts, such as failed or bad password
- Use of and changes to authentication mechanisms, such as creating new accounts, elevating user privileges, etc.
- Initialization, stopping, or pausing of the audit logs
- Creation and deletion of system-level objects

All system components within the cardholder data environment should record the following events in system audit logs:

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

Any errors, anomalies, or suspicious entries must be reviewed and escalated according to standard incident response processes and procedures. All audit log entries, specific to the cardholder data environment, must be retained for at least one year, with a minimum of three months immediately available for analysis.

6.02 Security System and Process Testing

Relevant PCI DSS 3.2 Requirements: 11.2 (11.2.1 – 11.2.3), 11.3 (11.3.1 – 11.3.4), 11.5 (11.5.1), 11.6

System components, processes, and applications need to be tested frequently to ensure security controls continue to reflect a changing environment.

- Vulnerability scans must be run at least quarterly and after any significant change in the network which impacts the cardholder data environment (such changes may include new system component installations, changes in network topology, firewall rule modifications, or product upgrades)
- Internal quarterly vulnerability scanning must be performed by members of the OPS Team ("qualified personnel")
- Internal quarterly vulnerability scans must be repeated until all "high-risk" vulnerabilities are resolved, remediated, and/or exempted (requires OPS Team approval)
- External quarterly vulnerability scanning must be performed by an Approved Scanning Vendor (ASV)—presently, Security Metrics and AlertLogic—approved by the Payment Card Industry Security

Standards Council (PCI SSC)

- External quarterly vulnerability scans must be repeated until all “high-risk” vulnerabilities are resolved, remediated, and/or exempted (requires OPS Team approval)

In order to continually assess the cardholder data environment, penetration testing (both internal and external) must be conducted by a qualified external security services firm every twelve months or after any significant infrastructure or application upgrade or modification. Penetration testing should include the following:

- Based on industry-accepted penetration testing approaches, such as *NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment*
- Coverage of the entire cardholder data environment perimeter and critical systems and applications
- Testing from both inside and outside the network
- Testing to validate all out-of-scope systems are segmented from systems in the cardholder data environment
- Network-layer penetration tests to include components that support network functions as well as operating systems
- Review and consideration of threats and vulnerabilities experienced in the last 12 months

Any application-layer penetration tests for commercial “off-the-shelf” products need to be coordinated in conjunction with the software vendor. All penetration testing results and remediation activities must be maintained by the OPS Team. The cardholder data environment must be secured with intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. In addition, change-detection software must be installed and configured on cardholder data systems to detect unauthorized changes, additions, and deletions of critical system files.

OPS Team must be able to receive and monitor alerts for traffic at the perimeter of the cardholder data environment as well as at critical points within the environment. Signatures, definitions, engines, and agents must be current with GoldenComm standard builds and deployments.

7. Additional Resources

The following referenced guidelines are available on the NIST website:

- NIST Special Publication 800-88 Revision 1 Guidelines for Media Sanitization
- NIST Special Publication 800-115 Technical Guide to Information Security Testing and Assessment

The following additional resources are available on the PCI website:

- Glossary of Terms, Abbreviations, and Acronyms v3.2
- PCI DSS v3.2.1
- SAQ D v3.2.1 - Service Provider

Appendix A: Definitions

These definitions apply to institutions and regulations as they are used in this policy.

	GoldenComm	Golden Communications, Inc.
	OPS	Special Operations Team
	Security Metrics	SecurityMetrics, Inc.
	AlertLogic	Alert Logic, Inc.