INFORMATION SECURITY POLICY

Version 3.0, 22 MAY 2024

INDEX

1. Introduction

This Policy Document encompasses all aspects of security surrounding confidential Quantum Spiral information and must be distributed to all Quantum Spiral employees. All Quantum Spiral employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by Management on an annual basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable

2. Information Security Policy

Quantum Spiral does not handle sensitive cardholder information on any basis.

Quantum Spiral requires no and has no access to cardholder data.

Quantum Spiral handles sensitive merchant information daily, including but not limited to know your customer information, certified copies of utilities bills and passports, merchant financial information and merchant financial results.

Sensitive Information must have adequate safeguards in place to protect it, to protect merchant privacy, to ensure compliance with various regulations and to guard the future of the organisation. Quantum Spiral commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties.

To this end management are committed to maintaining a secure environment in which to process information so that we can meet these promises.

Employees handling sensitive data should ensure:

- Handle the information in a manner that fits with their sensitivity;
- Limit personal use of Quantum Spiral information and telecommunication systems and ensure it does not interfere with your job performance;
- Quantum Spiral reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Quantum Spiral resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally.
- We each have a responsibility for ensuring our Quantum Spiral systems and data are protected from unauthorised access and improper use.

- If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.
- Quantum Spiral does not handle sensitive cardholder information on any basis.
- Quantum Spiral requires no and has no access to cardholder data.

3. Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Quantum Spiral established culture of openness, trust and integrity.

Management is committed to protecting the employees, partners and Quantum Spiral from illegal or damaging actions by individuals, either knowingly or unknowingly.

Quantum Spiral does not manage, maintain, supply, offer, sell, handle, service, repair or deal in any way with any POS devices and PIN entry devices.

Quantum Spiral will maintain an approved list of technologies and devices and personnel with access to such devices as detailed in Appendix B

- Employees are responsible for exercising good judgement regarding the reasonableness of personal use
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies
- Employees should take all necessary steps to prevent unauthorised access to confidential data which includes data
- Employees should ensure that technologies should be used and set-up in acceptable network locations
- Keep passwords secure and do not share accounts
- Authorised users are responsible for the security of their passwords and accounts
- All PCs, laptops and workstations should be secured with a password-protected screen saver with the automatic activation feature
- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered
- Because information contained on portable computers is especially vulnerable, special care should be exercised
- Postings by employees from a Quantum Spiral email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Quantum Spiral, 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 viruses, e-mail bombs, or Trojan horse code

Quantum Spiral does not manage, maintain, supply, offer, sell, handle, service, repair or deal in any way with any POS devices and PIN entry devices.

4. Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment.

Claims of ignorance, good intentions or using poor judgement will not be used as excuses for non-compliance

5. Protect Stored Data

- All sensitive data stored and handled by Quantum Spiral and its employees must be securely protected against unauthorised use at all times
- Any sensitive data that is no longer required by Quantum Spiral for business reasons must be discarded in a secure and irrecoverable manner
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.
- PAN'S which are not protected as stated above should not be sent to the outside network via end user messaging technologies like chats, ICQ messenger etc.
- It is strictly prohibited to possess and store for any reason:
- The contents of the payment card magnetic stripe (track data) on any media whatsoever
- The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever
- The PIN or the encrypted PIN Block under any circumstance

6. Information Classification

Data and media containing data must always be labelled to indicate sensitivity level

- Confidential data might include information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Quantum Spiral if disclosed or modified

- Confidential data includes merchant data
- Internal Use data might include information that the data owner feels should be protected to prevent unauthorised disclosure
- Public data is information that may be freely disseminated

7. Access To The Sensitive Cardholder Data

- Quantum Spiral require no and has no access to cardholder data.
- If Quantum Spiral were in the future duly authorised and fully PCIDSS compliant, then the following would apply.
- All Access to sensitive cardholder should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined
- Any display of the cardholder should be restricted at a minimum of the first 6 and the last 4 digits of the cardholder data
- Access rights to privileged user IDs should be restricted to least privileges necessary to perform job responsibilities
- Privileges should be assigned to individuals based on job classification and function (Role based access control)
- Access to sensitive cardholder information such as PANs, personal information and business data is restricted to employees that have a legitimate need to view such information
- No other employees should have access to this confidential data unless they have a genuine business need
- If cardholder data is shared with a Service Provider (3rd party) then a list of such Service Providers will be maintained as detailed in Appendix B
- Ensure a written agreement that includes an acknowledgement is in place that the Service Provider will be responsible for the for the cardholder data that the Service Provider possess
- Ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider
- Have a process in place to monitor the PCIDSS compliance status of the Service provider
- Quantum Spiral require no and has no access to cardholder data.
- If Quantum Spiral were in future duly authorised and fully PCIDSS compliant, then the above paragraph 7 would apply.

8. Physical Security

- Quantum Spiral do not manage, maintain, supply, offer, sell, handle, service, repair or deal in any way with any POS devices and PIN entry devices.

- Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.
- Employees are responsible for exercising good judgement regarding the reasonableness of personal use.
- Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
- Employees should take all necessary steps to prevent unauthorised access to confidential data which includes data.
- Employees should ensure that technologies should be used and set-up in acceptable network locations.
- A list of devices that accept data should be maintained
- The list should include make, model and location of the device
- The list should have the serial number or a unique identifier of the device
- The list should be updated when devices are added, removed or relocated
- POS devices surfaces should be periodically inspected to detect tampering or substitution
- Personnel using the devices should be trained and aware of handling the POS devices
- Personnel using the devices should verify the identity of any third party personnel claiming to repair or run maintenance tasks on the devices, install new devices or replace devices
- Personnel using the devices should be trained to report suspicious behaviour and indications of tampering of the devices to the appropriate personnel
- A is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day
- Keep passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts
- Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.
- Media containing sensitive information must be handled and distributed in a secure manner by trusted individuals
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive information
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where sensitive data is accessible. Employee refers to full-time and part-time employees, temporary employees and personnel, and consultants who are permanently based on Quantum Spiral sites. A visitor is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than one day.
- Network Jacks located in public and areas accessible to visitors must be disabled and enabled when network access is explicitly authorised.

- All POS and PIN entry devices should be appropriately protected and secured so they cannot be tampered or altered.
- Strict control is maintained over the external or internal distribution of any media containing data and has to be approved by management.
- Strict control is maintained over the storage and accessibility of media.
- All computer that store sensitive data must have a password protected screen saver enabled to prevent unauthorised use.
- Quantum Spiral do not manage, maintain, supply, offer, sell, handle, service, repair or deal in any way with any POS devices and PIN entry devices.

9. Protect Data In Transit

- All sensitive data must be protected securely if it is to be transported physically or electronically
- Data must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. AES encryption, PGP encryption, SSH, SSL, TLS, IPSEC, GSM, GPRS, Wireless technologies etc.,)
- The transportation of media containing sensitive data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

10. Disposal Of Stored Data

- All data must be securely disposed of when no longer required by Quantum Spiral, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete on-line data, when no longer required.
- All hard copies of data must be manually destroyed as when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic data has been appropriately disposed of in a timely manner.
- Quantum Spiral will have procedures for the destruction of hard copy (paper) materials. These will require that all hard copy materials are cross-cut shredded, incinerated or pulped so they cannot be reconstructed.
- Quantum Spiral will have documented procedures for the destruction of electronic media. These will require:

- All data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical destruction of the media.
- If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.
- All data awaiting destruction must be held in lockable storage containers clearly marked To Be Shredded - access to these containers must be restricted.

11. Security Awareness And Procedures

- The policies and procedures outlined below must be incorporated into Quantum Spiral practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors:
- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day Quantum Spiral practice.
- Distribute this security policy document to all Quantum Spiral employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A).
- All employees that handle sensitive data will undergo background checks (such as criminal and credit record checks, within the limits of the local law) before they commence their employment with the Quantum Spiral.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCIDSS).
- Quantum Spiral security policies must be reviewed annually and updated as needed.

12. Network Security

- Firewalls must be implemented at each internet connection and any demilitarized zone and the internal Quantum Spiral network.
- A network diagram detailing all the inbound and outbound connections must be maintained and reviewed every 6 months.
- A firewall and router configuration document must be maintained which includes a documented list of services, protocols and ports including a business justification.
- Firewall and router configurations must restrict connections between untrusted networks and any systems in the data environment.

- Stateful Firewall technology must be implemented where the Internet enters Quantum Spiral network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- All inbound and outbound traffic must be restricted to that which is required for the data environment
- All inbound network traffic is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- All outbound traffic has to be authorised by management (i.e. what are the white listed category of sites that can be visited by the employees) and the restrictions have to be documented.
- Quantum Spiral will have firewalls between any wireless networks and the data environment.
- Quantum Spiral will quarantine wireless users into a DMZ, where they will be authenticated and fire walled as if they were coming in from the Internet.
- Disclosure of private IP addresses to external entities must be authorised.
- A topology of the firewall environment has to be documented and has to be updated in accordance to the changes in the network.
- The firewall rules will be reviewed on a six months basis to ensure validity and the firewall has to have clean up rule at the bottom of the rule base.
- Quantum Spiral have to quarantine wireless users into a DMZ, where they were authenticated and fire walled as if they were coming in from the Internet.
- No direct connections from Internet to the data environment will be permitted. All traffic has to traverse through a firewall.

13. System And Password Policy

- All users, including contractors and vendors with access to Quantum Spiral systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.
- A system configuration standard must be developed along industry acceptable hardening standards (SANS, NIST, ISO).
- System configurations should be updated as new issues are identified (as defined in PCIDSS requirement 6.1).
- System configurations must include common security parameter settings.
- The systems configuration standard should be applied to any news systems configured.
- All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into Quantum Spiral network and all unnecessary services and user/system accounts have to be disabled..

- All unnecessary default accounts must be removed or disabled before installing a system on the network.
- Security parameter settings must me set appropriately on System components.
- All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.
- All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.
- Any insecure protocols, daemons, services in use must be documented and justified.
- All users with access to data must have a unique ID.
- All user must use a password to access Quantum Spiral network or any other electronic resources.
- All user ID's for terminated users must be deactivated or removed immediately.
- The User ID will be locked out if there are more than 3 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled for a minimum period of 30 minutes or until the administrator enables the account.
- All system and user level passwords must be changed on at least a quarterly basis.
- A minimum password history of four must be implemented.
- A unique password must be set-up for new users and the users prompted to change the password on first login.
- Group, shared or generic user account or password or other authentication methods must not be used to administer any system components.
- Where SNMP is used, the community strings must be defined as something other than the Standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.
- All non-console administrative access will use appropriate technologies like SSH, VPN, SSL etc. or strong encryption is invoked before the administrator password is requested.
- System services and parameters will be configured to prevent the use of insecure technologies like Telnet and other insecure remote login commands.
- Administrator access to web based management interfaces is encrypted using strong cryptography
- The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:
- Be as long as possible (never shorter than 6 characters).
- Include mixed-case letters, if possible.
- Include digits and punctuation marks, if possible.
- Not be based on any personal information.
- Not be based on any dictionary word, in any language.

- If an operating system other than Linux and FreeBSD without embedded security features is used (such as DOS, Windows or MacOS), then an intruder only needs temporary physical access to the console to insert a keyboard monitor program. If the workstation is not physically secured, then an intruder can reboot even a secure operating system, restart the workstation from his own media, and insert the offending program.
- To protect against network analysis attacks, both the workstation and server should be cryptographically secured. Examples of strong protocols are the encrypted Netware login and Kerberos.

14. Anti-Virus Policy

- All machines must be configured to run the latest anti-virus software as approved by Quantum Spiral. The preferred applications to use is CLAMAV, SOPHOS & COMODO Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The Anti-Virus should have periodic scanning enabled for all the systems.
- The Anti-Virus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits).
- All removable media (for example USB thumb drives and others) should be scanned for viruses before being used.
- All the logs generated from the Anti-Virus solutions have to be retained as per legal/regulatory/contractual requirements or at a minimum of PCIDSS requirement 10.7 of 3 months online and 1 year offline.
- Master Installations of the Anti-Virus software should be set-up for automatic updates and periodic scans.
- End users must not be able to modify and any settings or alter the Anti-Virus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

15. Patch Management Policy

- All workstations, servers, software, system components etc. owned by Quantum Spiral must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
- Where ever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors.

- Security patches have to be installed within one month of release from the respective vendor and have to follow the process in accordance with change control process.
- Any exceptions to this process have to be documented.

16. Remote Access Policy

- It is the responsibility of Quantum Spiral employees, contractors, vendors and agents with remote access privileges to the Quantum Spiral corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Quantum Spiral.
- Secure remote access must be strictly controlled. Control will be enforced by two factor authentication via one-time password authentication or public/private keys with strong pass-phrases.
- Vendor accounts with access to Quantum Spiral network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.
- Remote access connection will be set-up to be disconnected automatically after 30 minutes of inactivity.
- All hosts that are connected to Quantum Spiral internal networks via remote access technologies will be monitored on a regular basis.
- All remote access accounts used by vendors or 3rd parties will be reconciled at regular interviews and the accounts will be revoked if there is no further business justification
- Vendor accounts with access to Quantum Spiral network will only be enabled during the time period the access is required and will be disabled or removed once access is no longer required.

17. Vulnerability Management Policy

- All the vulnerabilities would be assigned a risk ranking such as High, Medium and Low based on industry best practices such as CVSS base score.
- As part of the PCIDSS Compliance requirements, Quantum Spiral will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Quarterly internal vulnerability scans must be performed by Quantum Spiral by internal staff or a 3rd party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCIDSS Requirement 6.2 are resolved.

- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by Quantum Spiral internal staff. The scan process should include re-scans until passing results are obtained.

18. Configuration Standards

Information systems that process transmit or store data must be configured in accordance with the applicable standard for that class of device or system. Standards must be written and maintained by the team responsible for the management of the system in conjunction with the Information Security Office.

All network device configurations must adhere to Quantum Spiral required standards before being placed on the network as specified in Quantum Spiral configuration guide. Using this guide, a boilerplate configuration has been created that will be applied to all network devices before being placed on the network.

Before being deployed into production, a system must be certified to meet the applicable configuration standard.

Updates to network device operating system and/or configuration settings that fall under Quantum Spiral standards are announced by the Information Security Office. Updates must be applied within the time frame identified by the Information Security Office.

Administrators of network devices that do not adhere to Quantum Spiral standards (as identified via a previous exception) must document and follow a review process of announced vendor updates to operating system and/or configuration settings. This process must include a review schedule, risk analysis method and update method.

All network device configurations must be checked annually against the configuration boilerplate to ensure the configuration continues to meet required standards.

Where possible, network configuration management software will be used to automate the process of confirming adherence to the boilerplate configuration.

For other devices an audit will be performed quarterly to compare the boilerplate configuration to the configuration currently in place.

All discrepancies will be evaluated and remediated by Network Administration.

19. Change Control Process

- Changes to information resources shall be managed and executed according to a formal change control process. The control process will ensure that changes proposed are reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.
- The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical Quantum Spiral information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.
- All change requests shall be logged whether approved or rejected on a standardised and central system. The approval of all change requests and the results thereof shall be documented.
- A documented audit trail, maintained at a Business Unit Level, containing relevant information shall be maintained at all times. This should include change request documentation, change authorisation and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorised personnel.
- A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed.
- The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.
- All change requests shall be prioritised in terms of benefits, urgency, effort required and potential impact on operations.
- Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimise the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.
- Any software change and/or update shall be controlled with version control. Older versions shall be retained in accordance with corporate retention and storage management policies.
- All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorised user, the impact assessment was performed and proposed changes were tested.
- All users, significantly affected by a change, shall be notified of the change. The user representative shall sign-off on the change. Users shall be required to make submissions and comment prior to the acceptance of the change.

- Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.
- Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas.
- Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.
- Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.
- Specific procedures to ensure the proper control, authorisation, and documentation of emergency changes shall be in place. Specific parameters will be defined as a standard for classifying changes as Emergency changes.
- All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

20. Audit And Log Review

This procedure covers all logs generated for systems within the data environment, based on the flow of data over the Quantum Spiral network, including the following components:

- Operating System Logs (Event Logs and other logs).
- Database Audit Logs.
- Firewalls & Network Switch Logs.
- IDS Logs.
- Anti-Virus Logs.
- CCTV Video recordings.
- File integrity monitoring system logs.
- Audit Logs must be maintained for a minimum of 3 months online (available for immediate analysis) and 12 months offline.
- Review of logs is to be carried out by means of Quantum Spiral network monitoring system (Quantum Spiral to define hostname), which is controlled from Quantum Spiral console.

The console is installed on the server (, located within Quantum Spiral data centre environment.

- The following personnel are the only people permitted to access log files (Quantum Spiral to define which individuals have a job-related need to view audit trails and access log files).
- The network monitoring system software (is configured to alert the Quantum Spiral CISO to any conditions deemed to be potentially suspicious, for further investigation.

Alerts are configured to:

- A dashboard browser-based interface, monitored by the Quantum Spiral CISO
- Email / SMS alerts to Quantum Spiral tech mailbox with a summary of the incident. The Quantum Spiral CISO also receives details of email alerts for informational purposes
- The following Operating System Events are configured for logging, and are monitored by the console (:
- Any additions, modifications or deletions of user accounts.
- Any failed or unauthorised attempt at user logon.
- Any modification to system files.
- Any access to the server, or application running on the server, including files that hold data.
- Actions taken by any individual with root or administrative privileges.
- Any user access to audit trails.
- Any creation / deletion of system-level objects installed by Linux. (No system-level objects run with administrator privileges, none can be abused to gain administrator access to a system.

The following Database System Events are configured for logging, and are monitored by the network monitoring system (:

- Any failed user access attempts to log in to the database.
- Any login that has been added or removed as a database user to a database.
- Any login that has been added or removed from a role.
- Any database role that has been added or removed from a database.
- Any password that has been changed for an application role.
- Any database that has been created, altered, or dropped.
- Any database object, such as a schema, that has been connected to.
- Actions taken by any individual with DBA privileges.

The following Firewall Events are configured for logging, and are monitored by the network monitoring system (:

- ACL violations
- Invalid user authentication attempts.
- Logon and actions taken by any individual using privileged accounts.
- Configuration changes made to the firewall (e.g. policies disabled, added, deleted, or modified)
- The following Switch Events are to be configured for logging and monitored by the network monitoring system (:
- Invalid user authentication attempts.
- Logon and actions taken by any individual using privileged accounts.
- Configuration changes made to the switch (e.g. configuration disabled, added, deleted, or modified).

The following Intrusion Detection Events are to be configured for logging, and are monitored by the network monitoring system (:

- Any vulnerability listed in the Common Vulnerability Entry (CVE) database.
- Any generic attack(s) not listed in CVE.
- Any known denial of service attack(s).
- Any traffic patterns that indicated pre-attack reconnaissance occurred.
- Any attempts to exploit security-related configuration errors.
- Any authentication failure(s) that might indicate an attack.
- Any traffic to or from a back-door program.
- Any traffic typical of known stealth attacks.
-
- The following File Integrity Events are to be configured for logging and monitored by (Quantum Spiral to define software and hostname):
-
- Any modification to system files.
- Actions taken by any individual with Administrative privileges.
- Any user access to audit trails.
- Any Creation / Deletion of system-level objects installed by DOS, Windows and MacOS. (Almost all system-level objects run with administrator privileges, and some can be abused to gain administrator access to a system.)

For any suspicious event confirmed, the following must be recorded on the Log Review Form, and Quantum Spiral CISO informed:

- User Identification.
- Event Type.
- Date & Time.
- Success or Failure indication.
- Event Origination (e.g. IP address).
- Reference to the data, system component or resource affected.

21. Secure Application Development

The Secure Application development policy is a plan of action to guide developers decisions and actions during the software development lifecycle (SDLC) to ensure software security.
This policy aims to be language and platform independent so that it is applicable across all software development projects.
The adherence to and use of Secure Application Development Coding Policy is a requirement for all software development on Quantum Spiral information technology systems and trusted contractor sites processing Quantum Spiral data.

Each phase of the SDLC is mapped with security activities, as explained below:

- Design Phase.
- Identify Design Requirements from security perspective.
- Architecture & Design Reviews.
- Threat Modelling.
- Coding Phase.
- Coding Best Practices.
- Perform Static Analysis.
- Testing Phase.
- Vulnerability Assessment.
- Fuzzing.
- Deployment Phase.
- Server Configuration Review.
- Network Configuration Review.

Development of code shall be checked and validated with the most current versions of Quantum Spiral Coding Standards for Secure Application Development. All code developers shall verify that their code is in compliance with the most recent and approved coding standards and guidelines

Only validated code shall be implemented into Quantum Spiral production environment.

A review and validation ensures that code exhibits fundamental security properties to include correctness, predictability, and attack tolerance

Application Code Developers shall:

- Ensure code meets the level of confidence that software is free from exploitable code vulnerabilities, regardless of whether they are already designed into the software or inserted later in its life cycle.

- Ensure code provides predictable execution or justifiable confidence and that the software, when executed, will provide security functionality as intended.
- Coding techniques must address injection flaws particularly SQL injection, buffer overflow vulnerabilities, cross site scripting vulnerabilities, improper access control (insecure direct object reference, failure to restrict URL access, directory traversal etc.,), cross site request forgery (CSRF), broken authentication and session management.
- Never trust incoming data to the system, apply checks to this data.
- Never rely on the client to store sensitive data no matter how trivial.
- Disable Error messages that return any information to the user.
- Use object inheritance, encapsulation, and polymorphism wherever possible.
- Use environment variables prudently and always check boundaries and buffers.
- Applications must validate input to ensure it is well-formed and meaningful.

22. Penetration Testing Methodology

In this section should be listed the risks inherent in conducting penetration testing over the information systems of the Quantum Spiral. Additionally, it should be noted for each mitigation measures that will be taken. Examples might be:

Example 1#
Risk: Denial of Service in systems or network devices because of the network scans.

- Mitigation measure 1: Network scans must be performed in a controlled manner. The start and end of the scan must be notified to responsible personnel to allow monitoring during testing. For any sign of trouble will abort the scan in progress
- Mitigation measure 2: Scanning tools must be configured to guarantee that the volume of sent packets or sessions established per minute does not cause a problem for network elements. In this sense, we must perform the first scans in a very controlled way and a use minimum configuration that may be expanded when is evident that the configuration is not dangerous for network devices or servers in the organisation

Key staff involved in the project by the organisation will be listed:

- Technical Project Manager.
- Chief Information Security Officer (CISO).
- Chief Information Officer.
- Head of Communications.
- Responsible for web site www.quantumspiral.co.za

- External intrusion tests will be performed remotely from the supplier's premises.
- Internal intrusion tests will be conducted in the office Quantum Spiral of the Organisation.
- Audit team must to have access to the Organisation's network. It must manage access permissions to the building early enough to ensure that the audit team can access without problems during planning period.
- All the tests will be conducted from the equipment owned by the audit team so no equipment for the execution of the tests is required. The only requirement in this regard will be to have an active network connection for each member of the audit team. Those connections must provide access to the target network segment in every case.
- If an incident occurs during the execution of the tests that have an impact on the systems or services of the organisation, the incident should be brought immediately to the attention of those responsible for incident management in the project.

It should be noted that in order to comply with PCIDSS the scope of the test should include, at least the following:

- All systems and applications that are part of the perimeter of the data environment card (CDE)Example:
- Systems included in the scope: System 1: IP: System: System Description System, 2: IP: System: System Description Wi-Fi network the Quantum Spiral.
- Applications included in the scope: Application 1: URL: Description of the application.
- Systems excluded from the scope: System 5: IP: System: System Description, System 6: IP: System: System Description.
- Applications excluded from the scope: Application 3: URL: Description of the application.
- Technical tests must follow the Open Source Security Testing Methodology Manual (OSSTMM).

Tests must be conducted at network, system and application level and must ensure that at least identifies any vulnerabilities documented by OWASP and SANS, as well as those identified in the PCIDSS standard v3:

- Injections: Code, SQL, OS commands, LDAP, XPath, etc.
- Buffer overflows.
- Insecure storage of cryptographic keys.
- Insecure Communications.
- Improper error handling.
- Cross-site scripting (XSS).
- Control of inappropriate access.

- Cross-site request forgery (CSRF).
- Broken authentication and incorrectly session management.
- Any other vulnerability considered High Risk by the organisation.

For all findings or vulnerabilities identified during the tests carried out will be generated and documented sufficient evidence to prove the existence of the same.

The format of the evidence can be variable in each case, screen capture, raw output of security tools, photographs, paper documents, etc.

As a result of tests performed should generate a document containing at least the following sections:

- Introduction.
- Executive Summary.
- Methodology.
- Identified vulnerabilities.
- Recommendations for correcting vulnerabilities.
- Conclusions.
- Evidence.

23. Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to our communications or information processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage Quantum Spiral.

The Incident response plan has to be tested once annually. Copies of this incident response plan is to be made available to all relevant staff members, and take steps to ensure that they understand it and what is expected of them.

Employees of Quantum Spiral will be expected to report to the security officer for any security related issues

Quantum Spiral PCI security incident response plan is as follows:

- Each department must report an incident to the Information Security Officer (preferably) or to another member of the PCI Response Team.
- That member of the team receiving the report will advise the PCI Response Team of the incident.

- The PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of data and in mitigating the risks associated with the incident.
- The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.
- The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.
- If an unauthorised wireless access point or devices is identified or detected as part of the quarterly test this is should be immediately escalated to the Security officer or someone with similar privileges who has the authority to stop, cease, shut down, and remove the offending device immediately.
- A department that reasonably believes it may have an account breach, or a breach of data or of systems related to the PCI environment in general, must inform Quantum Spiral PCI Incident Response Team.
- After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment departments response plans.

Quantum Spiral PCI Security Incident Response Team:

- CIO.
- Communications Director.
- Compliance Officer.
- Counsel.
- Information Security Officer.
- Collections & Merchant Services.
- Risk Manager.
- Incident Response Notification.
- Escalation Members.
- Escalation First Level.
- Information Security Officer.
- Controller.
- Executive Project Director for Credit Collections and Merchant Services Legal Counsel.
- Risk Manager.
- Director of Quantum Spiral Communications.
- Open Source Security Testing Methodology Manual.
- Quantum Spiral Managing Director.
- Executive Cabinet.
- Internal Audit.

- Auxiliary members as needed.
- External Contacts (as needed).
- Merchant Provider.
- Card Brands (if applicable).
- Internet Service Provider (if applicable).
- Internet Service Provider of Intruder (if applicable).
- Communication Carriers (local and long distance).
- Business Partners.
- Insurance Carrier.
- External Response Team as applicable (CERT Coordination Centre 1, etc.).
- Law Enforcement Agencies as applicable in local jurisdiction.

In response to a systems compromise, the PCI Response Team and designees will:

- Ensure compromised system/s is isolated on/from the network.
- Gather, review and analyse the logs and related information from various central and local safeguards and security controls.
- Conduct appropriate forensic analysis of compromised system.
- Contact internal and external departments and entities as appropriate.
- Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
- Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.
- Quantum Spiral require no and has no access to cardholder data.
- If Quantum Spiral were in future duly authorised and fully PCIDSS compliant, then the following would apply.
- The card companies have individually specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data.
- Incident Response notifications to various card schemes.
- In the event of a suspected security breach, alert the information security officer or your line manager immediately.
- The security officer will carry out an initial investigation of the suspected security breach.
- Upon confirmation that a security breach has occurred, the security officer will alert management and begin informing all relevant parties that may be affected by the compromise.

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hours.

For more Information visit:

http://USA.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as VISA Secret:

- Executive Summary.
- Include overview of the incident.
- Include RISK Level(High, Medium, Low).
- Determine if compromise has been contained II.
- Background.
- Include forensic tools used during investigation V.
- Findings.
- Number of accounts at risk, identify those stores and compromised.
- Type of account information at risk.

Identify ALL systems analysed. Include the following:

- Domain Name System (DNS) names.
- Internet Protocol (IP) addresses.
- Operating System (OS) version.
- Function of system(s).

Identify ALL compromised systems. Include the following:

- DNS names.
- IP addresses.
- OS version.
- Function of System(s).
- Time frame of compromise.
- Any data exported by intruder.

- Establish how and source of compromise.
- Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers machines, etc.).
- If applicable, review VisaNet endpoint security and determine risk.
- Compromised Entity Action.
- Recommendations.
- Contact(s) at entity and security assessor performing investigation.

This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorised disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand

MasterCard Steps:

- Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
- Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to:compromised_account_team@mastercard.com
- Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
- Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
- Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
- Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
- Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.
- Once MasterCard obtains the details of the account data compromise and the list of compromised .account numbers, MasterCard will:

    - Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.

- Distribute the account number data to its respective issuers.
- Employees of Quantum Spiral will be expected to report to the security officer for any security related issues.
- The role of the security officer is to.
- Effectively communicate all security policies and procedures to employees within Quantum Spiral and contractors.
- In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally,
- Oversee the implantation of the incident response plan in the event of a sensitive data compromise
- Discover Card Steps.
- Within 24 hours of an account compromise event, notify Discover Fraud Prevention.
- Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
- Prepare a list of all known compromised account numbers.
- Obtain additional specific requirements from Discover Card.

American Express Steps

- Within 24 hours of an account compromise event, notify American Express Merchant Services.
- Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
- Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express.
- Quantum Spiral require no and has no access to cardholder data.
- If Quantum Spiral were in future duly authorised and fully PCIDSS compliant, then the above card association rules would fully apply.

24. Roles And Responsibilities:

Chief Security Officer (or equivalent) is responsible for overseeing all aspects of information security, including but not limited to:

- Creating and distributing security policies and procedures.
- Monitoring and analysing security alerts and distributing information to appropriate information security and business unit management personnel.
- Creating and distributing security incident response and escalation procedures that include:

- Maintaining a formal security awareness program for all employees that provide multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings).
- The Information Technology Office (or equivalent) shall maintain daily administrative and technical operational security procedures that are consistent with the PCIDSS (for example, user account maintenance procedures, and log review procedures).

System and Application Administrators shall:

- Monitor and analyse security alerts and information and distribute to appropriate personnel.
- Administer user accounts and manage authentication.
- Monitor and control all access to data.
- Maintain a list of service providers.
- Ensure there is a process for engaging service providers including proper due diligence prior to engagement.
- Maintain a program to verify service providers PCIDSS compliant status, with supporting documentation.

The Human Resources Office (or equivalent) is responsible for tracking employee participation in the security awareness program, including:

- Facilitating participation upon hire and at least annually.
- Ensuring that employees acknowledge in writing at least annually that they have read and understand Quantum Spiral information security policy.

General Counsel (or equivalent) will ensure that for service providers with whom information is shared:

- Written contracts require adherence to PCIDSS by the service provider.
- Written contracts include acknowledgement or responsibility for the security of data by the service provider.

25. Third Party Access To Cardholder Data

- Quantum Spiral require no and has no access to cardholder data.
- Quantum Spiral are unable to provide any third party with access to any cardholder data.
- All third-party companies providing critical services to Quantum Spiral must provide an agreed Service Level Agreement.
- All third-party companies providing hosting facilities must comply with Quantum Spiral Physical Security and Access Control Policy.

All third-party companies, including processing banks and payment gateway technology providers, which exclusively have access to cardholder information must:

- Adhere to the PCIDSS security requirements.
- Acknowledge their responsibility for securing the cardholder data.
- Acknowledge that the cardholder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service or for uses specifically required by law.
- Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.
- Provide full cooperation and access to conduct a thorough security review after a security intrusion to a Payment Card industry representative, or a Payment Card industry approved third party.
- Quantum Spiral require no and has no access to cardholder data.
- Quantum Spiral are unable to provide any third party with access to any cardholder data.

26. User Access Management

- Access to Quantum Spiral is controlled through a formal user registration process beginning with a formal notification from HR or from a line manager.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions.
- The use of group IDs is only permitted where they are suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorised by HR/line management.
- The job function of the user decides the level of access the employee has to data.
- A request for service must be made in writing (email or hard copy) by the newcomer's line manager or by HR.

The request is free format, but must state:

- Name of person making request.
- Job title of the newcomers and work group.
- Start date.
- Services required (default services are: Mail, Libre Office, Mozilla Firefox and Internet access).
- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure.

- The user signs the form indicating that they understand the conditions of access.
- Access to all Quantum Spiral systems is provided by IT and can only be started after proper procedures are completed.
- As soon as an individual leaves Quantum Spiral employment, all his/her system logons must be immediately revoked.
- As part of the employee termination process HR (or line managers in the case of contractors) will inform IT operations of all leavers and their date of leaving.

27. Access Control Policy

- Access Control systems are in place to protect the interests of all users of Quantum Spiral computer systems by providing a safe, secure and readily accessible environment in which to work.
- Quantum Spiral will provide all employees and other users with the information they need to carry out their responsibilities in as effective and efficient manner as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT Services.
- Technical teams shall guard against issuing privilege rights to entire teams to prevent loss of confidentiality.
- Access rights will be accorded following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or maintaining a separate database must only do so where such an action is in accord with the data classification.
- Users are obligated to report instances of non-compliance to the Quantum Spiral CISO.
- Access to Quantum Spiral IT resources and services will be given through the provision of a unique Active Directory account and complex password.
- No access to any Quantum Spiral IT resources and services will be provided without prior authentication and authorization of a user's Quantum Spiral Active Directory account.
- Password issuing, strength requirements, changing and control will be managed through formal processes. Password length, complexity and

expiration times will be controlled through Active Directory Group Policy Objects.
- Access to Confidential, Restricted and Protected information will be limited to authorised persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed or revoked must be made in writing.
- Users are expected to become familiar with and abide by Quantum Spiral policies, standards and guidelines for appropriate and acceptable usage of the networks and systems.
- Access for remote users shall be subject to authorization by IT Services and be provided in accordance with the Remote Access Policy and the Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is variously and appropriately controlled according to the data classification levels described in the Information Security Management Policy.
- Access control methods include logon access rights, file share and disk permissions, user account privileges, server and workstation access rights, firewall permissions, IIS Intranet/Extranet authentication rights, SQL database rights, isolated networks and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT Services to review users access rights. The review shall be logged and IT
- Services shall sign off the review to give authority for users continued access rights.

28. Wireless Policy

- Installation or use of any wireless device or wireless network intended to be used to connect to any of the Quantum Spiral networks or environments is prohibited.
- A quarterly test should be run to discover any wireless access points connected to Quantum Spiral network.

Usage of appropriate testing using tools like NET STUMBLER, KISMET etc. must be performed on a quarterly basis to ensure that:

- Any devices which support wireless communication remain disabled or decommissioned.
- If any violation of the Wireless Policy is discovered as a result of the normal audit processes, the security officer or any one with similar job description has the authorisation to stop, cease, shut down, and remove the offending device immediately.

If the need arises to use wireless technology it should be approved by Quantum Spiral and the following wireless standards have to be adhered to:

- Default SNMP community strings and passwords, pass phrases, encryption keys/security related vendor defaults (if applicable) should be changed immediately after the installation of the device and if anyone with knowledge of these leaves the Quantum Spiral.
- The firmware on the wireless devices has to be updated accordingly as per vendors release schedule.
- The firmware on the wireless devices must support strong encryption for authentication and transmission over wireless networks.
- Any other security related wireless vendor defaults should be changed if applicable.
- Wireless networks must implement industry best practices (IEEE 802.11i) and strong encryption for authentication and transmission of data.
- An Inventory of authorised access points along with a business justification must be maintained.

More Information

Please feel free to contact us if you require any further information.

Appendix A:

Agreement to Comply With Information Security Policies

_____

Employee Name (printed)

_____

Department

I agree to take all reasonable precautions to assure that Quantum Spiral internal information, or information that has been entrusted to Quantum Spiral by third parties such as customers, will not be disclosed to unauthorised persons.

At the end of my employment or contract with the Quantum Spiral, I agree to return all information to which I have had access as a result of my position.

I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job.

As a condition of continued employment, I agree to abide by the policies and other requirements found in Quantum Spiral security policy.

I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated security officer.

_____ _____

Employee Signature Date

Appendix B

Redacted from online version of this policy for security reasons.

List of Service Providers

Name: Wix
PCIDSS Compliant?: Yes
Most Recent Information: https://support.wix.com/en/article/security-of-wixs-billing-services-and-pci-compliance

Name: Amazon Web Services
PCIDSS Compliant?: Yes
Most Recent Information: https://aws.amazon.com/compliance/services-in-scope/