QUINT DIGITAL LIMITED

(FORMERLY QUINT DIGITAL MEDIA LIMITED)

IT SECURITY, POLICY AND PROCEDURES

TABLE OF CONTENTS

Introduction

The Quint Digital Limited ("QDL" or "the Company") IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the organization which must be followed by all staff. It also provides guidelines to the Company which will be used to administer these policies, with the correct procedure to follow.

QDL will keep all IT policies updated. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all the employees.

Overall IT Structure

The QDM has an AD Servers acting as DNS, DHCP Server configured as a backup because currently DHCP service is enabled on Firewall. PTI News wire Server. QDM has a centralized Firewalls "Sophos XGS2300" in HA System those are working in Active Passive mode. All the access rights and back-end services are provided from there. The IT Department deals with installation of desktop/laptop/user Management. The rights that have been provided to the employees are based on approvals received from various HOD.

1. Comprehensive IT Security Policy and Procedure

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the organization to ensure integrity, confidentiality and availability of data and assets.

Perimeter Security Maintenance

Perimeter security for this organization is maintained by a Sophos XGS2300 firewall. This firewall has a redundant fail-over unit using HA configuration to provide service continuity, should the primary firewall unit fail. The Sophos XGS2300 firewall(s) will inspect packets and sessions to determine if they should be transmitted or dropped. In effect, the firewalls will act as a single point of network access where traffic can be analyzed and controlled.

Firewall Logon Access

Enabled or privileged logon access to the firewall will be restricted to a Primary /Secondary firewall administrator and one designer. Enable password construction will be consistent with the strong password creation practices utilized in the department.

Firewall Operational Maintenance and Responsibility

Day-to-Day operation and maintenance will be the responsibility of the department's Network and Security Engineer (or assigned position). Firewall support duties for the Network and Security Engineer include:

- Act as a departmental technical lead for the departmental security policy and procedure implementation has the primary responsibility for ensuring operational continuity for the department's security policy.
- Perform firewall rule set changes, adds and deletions as approved by the department Head.
- Perform Firewall software maintenance and hardware upgrades to the firewall; Implement feature set on firewalls as approved by the departmental Head.
- Monitor firewall logs, and intrusion detection system.

Firewall Rule Set Management and Change Control Process

The department Head must approve all rule set (ACL's) changes. The department Head must approve all Firmware changes and upgrades. At a minimum, the following information will be included in any firewall change request.

- Requesters Name and POC information
- Requested Due Date (when change will be applied)
- Change impact statement. Include any supporting documentation necessary to determine why the change is necessary. The change request will be delayed until the change requirement has been established and approved.
- Rule Change Notification requirements (who need to be alerted about the change because of potential operational impact).

Firewall rule sets (ACL's) will work to achieve a "best practices" approach to balance security risk and operational access requirements. Recommended practices include:

- Anything from inside the network is allowed out.
- All access to the firewall itself is blocked from the Internet.
- Restricted internal access to the firewall, except selected IT Personnel.
- ICMP services turned off.
- Block Ping and Telnet access to all internal servers from the Internet, only required ports are allowed.
- Remote access services for authorized users via VPN with HOD's Approval.
- Guests are given Internet access using GUEST-WIFI Profile with no access to Internal Network Devices/Servers/Printers.

- Block Ping and Telnet access to all internal servers from the Internet, only required ports are allowed.

Network Connection Policy

The Technical HOD must approve all connections from the intra network to any external networks. Only network connections that have been found to have acceptable security controls and procedures will be allowed to connect to the internal/external network. Every attempt will be made to ensure that all external connections will pass through firewalls that meet the guidelines established by this policy. All connections and accounts related to external network connections shall be validated on an annual basis. When a network connection is no longer needed all policies/accounts and system processes related to the connection should be deleted within one workweek.

Trusted Networks Policy

Network Trust Relationships Overview Approved and authorized network connections are considered trusted networks. Trusted networks share the similar security policy or implement security controls and procedures.

The following networks are considered trusted networks and permitted controlled access by the firewall(s).

The Backbone/Corporate Network (192.168.X.X)

These Network Segment are configured on Cisco 3850 Core Switch with Fail-Over unit Uplink to all Cisco 2960, HP 2510-48G and SG 500X-24 Access.

Non-trusted Networks Policy

All networks not specifically listed as a trusted network are non-trusted networks. Access to the network will be denied by the firewall(s). If complete access control cannot be managed by the firewall(s), other security technologies will be used in tandem with firewalls to mitigate the security threat. Modem connections with business partners and/or remote sites are also considered un- trusted networks connections. The IT Engineer may terminate unauthorized connections to network without notice. An active network port or connection does not imply authorization for connectivity. To support this policy, unused and/or unknown network connections (switch ports, analog lines, etc.) will be disabled until they are properly identified, documented, and placed in or out of service.

Periodic Review of Firewall Security Policies

Firewall security policies will be reviewed Quarterly. When there are major changes to the network requirements this may warrant changes to the firewall security policy.

Changes include events such as the implementation of major enterprise computing environment modifications and any occurrence of a major information security incident.
When new policy/project/applications are being considered, a HOD will evaluate new services before the firewall administrators are formally notified to implement the service. Alternatively,

when a policy/project/application is phased out or upgraded, the firewall ruleset should be formally changed where appropriate.

(This approach helps to minimize the presence of old and potentially insecure rules that are no longer needed.)

Firewall installations will be audited on a regular, periodic basis. These periodic reviews can be conducted on paper by reviewing hard-copy configurations provided by appropriate systems administration staff. In other cases, periodic reviews should involve actual audits and vulnerability assessments of the firewall.

Physical Security

For all servers and other network assets, the area must be secured with adequate ventilation and appropriate access through server room key only.

It will be the responsibility of the IT Team to ensure that this requirement is always followed. Any employee becoming aware of a breach of this security requirement is obliged to notify the Admin, Tech & Operation Dept. immediately.

All security and safety of all portable technology, such as Laptops & Chargers, HDMI Cables/Converters Notepads, iPad, Wireless Mouse/Keyboard etc. will be the responsibility of the employee who has been issued with the Laptops, Power Adapters, HDMI Cables/Converters, USB Dongles, Data Cards, Notepads, iPad, Wireless Mouse/Keyboard phones etc. Each employee is required to use given lockers & Password Protection to ensure the asset is always kept safely to protect the security of the asset issued to them.

In the event of loss or damage, the IT & Finance Team will assess the security measures undertaken to determine if the employee will be required to reimburse the organization for the loss or damage.

All assets such as Adapters, HDMI Cables/Converters, USB Dongles, Data Cards, Notepads, iPad, Wireless Mouse/Keyboard Phones etc.} When kept at the office desk is to be secured/Monitored by CCTV Surveillance & personal Lockers provided by Admin Dept.

Backup and Restoration

Purpose of the Policy

All sensitive, valuable, or critical organization data or provide a checklist of all data to be backed up/Archived.

Network Devices & Servers

Sophos XGS2300: -
There are Two Sophos XGS2300 configured HA for Fail-over & Backup is taken on 15 days.

CISCO Switches: -
Backup for all Cisco switches are taken on 15 days.

ARUBA IAP 335: -
There are 3 Aruba IPA 335 Access Point with Fail-over configuration as Master-Slave & backup is taken on 15 days.

NAS STORAGE: -
This is common Storage for all clients for day-day activity, all the contents are stored by the users on this common storage and this storage is only accessible from the office network only. The users can access this NAS storage only through secured VPN from outside the office network.

Servers: -
Backup of AD server, DHCP server and PTI Server is taken on 15 days.

User Access Management Policy & Procedures

Technology Access & Procedures

Login access to New Joinee

When a new employee joins the Company, the HR Dept. informs the IT Department to confirm the designation of the new employee & his reporting HOD (Head of Department) . The HOD of the relevant dept. informs IT Department all the details regarding the designation of the new employee, his responsibilities and the areas to be handled by him/her are also communicated. Based on this, the IT department creates a login ID for the employee in the Active Directory.

Every employee will be issued a unique ID based on the name (First and Last name) of the respective employee. No two user IDs can be the same, so even if the names of two employees are the same, the ID is distinguished by adding a numeral to one of them to access the organization technology and will be required to reset/change a password, there is a mandatory requirement of changing the password every 90 days.

In the case of existing users, additional access rights are granted only if a mail is received from the relevant HOD stating that a respective employee would be overseeing such additional areas for a limited amount of time.

The personnel can keep anything as his/her password within the limit and is not to be shared with any employee within the institution.

Where an employee forgets the password or is 'locked out' then IT TEAM is authorized to 'Unlock' or reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

Work from Home

For the Users who are working from home can access to in-house application using SSL VPN access facility by creating login on Sophos XGS2300 Firewall with HOD Approval.

Wi-Fi access

Internet access using WIFI is maintained by Aruba IAP Access Points.

These IAPs are working as a master and slave mode if the master AP gets down the other APs from the group will become the master and Wi-Fi will be up without affecting the Wi-Fi services.

Guests are given Internet access using GUEST -WIFI Profile with no access to Internal Network Devices/Servers/Printers.

The ID & PASSWORD to access GUEST-WIFI lie solely with the IT Department. The rights to access the Wi-Fi APs lie solely with the IT Department.

IT TEAM is responsible for the issuing of the identification username and initial password for all employees.

Process in case of Resignation of Employee

In case of resignation of employee, once all the formalities have been completed, the HOD of the relevant department informs the HR Dept which further informs the IT Department the details of the employee who has resigned. The login IDs of the said employee is immediately frozen by the IT Department and cannot be accessed after that. However, a record of the activity log is kept for future reference, if required.

The e-mail of the resigned employee continues to operate for 30 days after the resignation (in case any mails are to be received from customers, suppliers etc.), after which it is deleted.

Anti-Virus / Malware protection
Scope of Anti-virus policy

1. Policy Overview

This document contains the Antivirus (AV) policy details including actions to be taken if non-compliance occurs. A definition of the terms 'virus', 'malware' and 'spam' are described as well as the approved AV software standards in the appendices.

2. Policy Scope

This policy aims to set out the anti-virus policy within QDM Network. This policy applies to all staff authorized to use/access IT systems and Internet network whether they are employed directly by Quint Digital Limited or Third Party, or Vendors granted access for support purposes.

Configuration Standards

1. Approved Anti-virus software MUST be correctly installed and configured on all supported endpoint and servers across QDM Network to the following configuration standards. See the list of approved software in appendix A.

2. Anti-virus software MUST be kept up to date including the definitions files.

3. Anti-virus software updates MUST be deployed across the network automatically following their receipt from the vendor and it must be configured to check for these updates every 60 minutes daily.

4. Virus and malware signature updates MUST be deployed across the network automatically following their receipt from the vendor and it must be configured to check for signature updates daily.

5. Anti-virus software MUST be configured for real time scanning and regular scheduled scans.

6. On-access scanning MUST be configured within Anti-virus software for removable media and Network Access/websites/Startups.

7. Anti-virus server MUST be monitored on a daily basis by nominated staff within the Information Technology team for virus alerts and any issues which cannot be resolved must be escalated to the Vendor Service Desk where an incident will be raised and a technician assigned to immediately investigate remotely via centralized management console or on-site visit.

8. Weekly Anti-Virus Scan reports MUST be provided to the IT HEAD In the event that systems are found to be non-compliant a report including suggested remediation will be created by the IT team which will be provided to Technical HEAD.

9. Tamper protection MUST be enabled to prevent end users or malware altering the anti-virus software's configuration or disabling the protection.

User Responsibilities

1. All IT equipment and removable media MUST be scanned for viruses and malware before being introduced or prior to use on the corporate /Broadcast network, system or device.

2. Users MUST not accept, or run, software from non-trusted sources.

3. Users must not undertake any activities with the intention to create and/or distribute malicious programs (e.g., viruses, worms, Trojans, e-mail bombs, etc.) into corporate/broadcast network(s) or system(s).

4. Users MUST inform the IT Service Desk immediately if a virus is detected on their system.

5. IT system(s) infected with a malware/virus that the anti-virus software has not been able to deal with MUST be disconnected/quarantined from the corporate/broadcast network until virus free.

Exceptions

1. Exceptions to the anti-virus policy require a formal documented risk assessment including steps taken to mitigate the risk and formal approval from Technical HEAD. Once approved exceptions will be implemented.

2. Any server or workstation that does not comply with policy must have an approved exception recorded in the Anti-virus exceptions file detailing the reason for the exception and the steps taken to mitigate the risk.

3. Systems will only have exception to the policy if scheduled updates or patches are deemed likely to cause major disruption to the system, resident software or service functionality or to facilitate problem diagnosis. All systems recorded within the Antivirus exceptions file must be reviewed on a weekly/quarterly basis by the IT team and the risk will be re- evaluated.

MONITORING AND COMPLIANCE

Anti-virus compliance level refers to the percentage of servers, workstations and laptops that have been successfully protected by an up-to-date Anti- virus product against virus or malware threats.

IT services will endeavor to achieve 100% compliance for all the end points under its management. For monitoring and compliance assessment the following levels must always be maintained 97% of all Desktops/laptops must be compliant with up-to-date anti-virus software and virus signatures installed within 2 days of the release.

POLICY NON-CONFORMANCE

Any system or workstation found to be without adequate protection as defined by this policy will be removed from the network until adequate protection is implemented.

Any user being found to be willfully violating the anti-virus policy may be subject to one or more of the following sanctions:

- Removal of any equipment used from the network until adequate protection is
- implemented
- Revocation of rights to access systems
- Subject to disciplinary action.

In the event of a virus outbreak, the IT Team reserves the right to temporarily remove equipment or disable parts of the network to safeguard other systems.

PROCEDURE FOR SUSPECTED INFECTION

If a user suspects the system may be infected, the following actions must be taken.

- Inform the IT service desk immediately.
- Switch off the machine.
- Ensure no-one uses the machine.
- Be prepared to inform IT of any actions taken which may have caused the infection.

The IT Team will:

- Check the infected PC and any media.
- Rebuild the PC if the infection is severe (e.g., Dridex, Ransomware)
- Check any servers that may have been accessed from the infected system.
- Attempt to determine the source of the infection.
- Ensure the incident is logged.

APPENDIX A: ANTIVIRUS STANDARD PRODUCTS

Approved Antivirus Software Products

Sophos Endpoint Security (Total. 165 for Corporate N /W).
Sophos Server Security (Total 5 for the Servers).

All information used within the organization is to adhere to the privacy laws and the organization's confidentiality requirements.

APPENDIX B - GLOSSARY OF TERMS

Adware
Software that automatically plays, displays, or downloads advertisements to a computer, often in exchange for the right to use a program without paying for it. The advertisements seen are based on monitoring of browser habits. Most adware is safe to use, but some can serve as spyware, gathering information about you from your hard drive, the websites you visit, or even your keystrokes. Certain types of adware have the capability to capture or transmit personal information.

Antivirus Software
A type of software that scans a computer's memory and disk drives for viruses. If it finds a virus, the application informs the user and may clean, delete, or quarantine any files, directories, or disks affected by the virus. The term antimalware is preferred because it covers more threats.

Browser Hijacker
A type of malware that alters your computer's browser settings so that you are redirected to websites that you had no intention of visiting. Most browser hijackers alter browser home pages, search pages, search results, error message pages, or other browser content with unexpected or unwanted content.

Dat Files
Also known as a data file, these files are used to update software programs, sent to users via the Internet. .DAT files contain up-to-date virus signatures and other information antivirus products use to protect your computer against virus attacks. DAT files are also known as detection definition files and signatures.

Keylogger
Software that tracks or logs the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. This Is usually done with malicious intent to collect information including instant messages, email text, email addresses, passwords, credit card and account numbers, addresses, and other private data.

Malware
A generic term used to describe any type of software or code specifically designed to exploit a computer or the data it contains, without consent. Malware includes viruses, Trojan horses, spyware, adware, most rootkits, and other malicious programs.

Phishing
A form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Typically, phishing emails request that recipients click on the link in the email to verify or update contact details or credit card information. Like spam, phishing emails are sent to a large number of email addresses, with the expectation that someone will act on the information in the email and disclose their personal information. Phishing can also happen via text messaging or phone.
Ransomware

Malicious software created by a hacker to restrict access to the computer system that it infects and demand a ransom paid to the creator of the malicious software for the restriction to be removed. Some forms of ransomware may encrypt files on the system's hard drive, while others may simply lock the system and display messages to coax the user into paying.

Spam

An unwanted electronic message, most commonly unsolicited bulk email. Typically, spam is sent to multiple recipients who did not ask to receive it. Types include email spam, instant messaging spam, web search engine spam, spam in biogs, and mobile phone-messaging spam. Spam includes legitimate advertisements, misleading advertisements, and phishing messages designed to trick recipients into giving up personal and financial. information. Email messages are not considered spam if. A user has signed up to receive them.

Spyware

Spyware spies on a user's computer. Spyware can capture information like web browsing habits, email messages, usernames and passwords, and credit card information. Just like viruses, spyware can be installed on a computer through an email attachment containing malicious software.

Trojan

Malicious programs disguised as legitimate software. Users are typically tricked into loading and executing it on their systems. One key factor that distinguishes a Trojan from viruses and worms is that Trojans don't replicate.

Change Management Policies and Procedures Guide

Purpose

Change management refers to a formal process for making planned and unplanned changes to the Quint Digital Limited Corporate IT environment. The primary objective of this document is to provide standardized methods and procedures to meet the change management requirements supporting Quint Digital Limited operations. This will ensure the day-to-day IT functions performed to provide effective change management satisfy corporate governance audit requirements that ultimately reduce risk. In addition to meeting all the audit requirements, these guidelines will provide a process for efficient and prompt handling of all IT changes completed by the IT department.

Change management generally includes the following steps

Submission: During this step a change is identified, and a change request is submitted. The change is evaluated, including determining the priority level of the service and the risk of the proposed change; determine the change type and the change process to use.

Planning: Plan the change, including the implementation design, scheduling, communication plan, test plan and roll-back plan.

Approval: obtaining approval for the change Plan from management as needed.

Implementation: Implement the change.

Review: Communicate and review Change Plan with peers and/or Change Tech Head regarding its success or failure and if the change resulted in a failure in service, define a mitigation strategy for future occurrences. Document all aspects of the change.

Close: The stage when the review is successful, and the change is closed.

DATES OF REVIEW/AMENDMENT

S. No.	Date of review/amendment
1.	January 21, 2023
2.	May 30, 2023