

Information security policy

Ensuring Data Confidentiality, Integrity, and Availability in Healthcare



September 17, 2023

QuantumVerse Technologies LLC

Jomael Ortiz Perez

21982 University Ln, Orange Bech AL 36561

**QuantumVerse Technologies LLC**

QuantumVerse Technologies LLC stands at the forefront of medical innovation. As a leader in the medical industry, the company seamlessly blends advanced technologies with healthcare solutions. Specializing in medical research, digital health platforms, innovative diagnostic tools, and healthcare consultancy, QuantumVerse Technologies LLC is dedicated to elevating patient care and transforming the medical landscape for the future.

**Table of Contents**

[**1.** **INTRODUCTION** 6](#_Toc145871047)

[1.1. PURPOSE 6](#_Toc145871048)

[QuantumVerse Technologies LLC stands at the forefront of medical innovation. As a leader in the medical industry, the company seamlessly blends advanced technologies with healthcare solutions. Specializing in medical research, digital health platforms, innovative diagnostic tools, and healthcare consultancy, QuantumVerse Technologies LLC is dedicated to elevating patient care and transforming the medical landscape for the future. 6](#_Toc145871049)

[This policy defines the technical controls and security configurations users and Information Technology (IT) administrators must implement to ensure the integrity and availability of the data environment at QuantomVerse Technologies LLC. It serves as a central policy document with which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides IT managers with policies and guidelines concerning the acceptable use of the company's technology equipment, e-mail, internet connections, voicemail, facsimile, future technology resources, and information processing. 6](#_Toc145871050)

[The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. 6](#_Toc145871051)

[All QuantumVerse Technologies LLC employees or temporary workers must adhere to this policy at all locations and contractors. 6](#_Toc145871052)

[1.2. SCOPE 6](#_Toc145871053)

[1.3. ACRONYMS / DEFINITIONS 7](#_Toc145871054)

[**2.** **APPLICATION SECURITY** 8](#_Toc145871055)

[**3.** **DATA BACKUP AND STORAGE** 9](#_Toc145871056)

[3.1. DATA CLASSIFICATION AND PRIORITY 9](#_Toc145871057)

[3.2. BACKUP FREQUENCY 10](#_Toc145871058)

[3.3. BACKUP METHODS 10](#_Toc145871059)

[3.4. STORAGE LOCATIONS 10](#_Toc145871060)

[3.5. DATA ENCRYPTION 10](#_Toc145871061)

[3.6. RETENTION POLICY 10](#_Toc145871062)

[3.7. DATA RESTORATION 10](#_Toc145871063)

[3.8. PHYSICAL STORAGE SECURITY 11](#_Toc145871064)

[3.9. CLOUD STORAGE VENDORS 11](#_Toc145871065)

[3.10. INCIDENT REPORTING 11](#_Toc145871066)

[3.11 TRAINING AND AWARENESS 11](#_Toc145871067)

[**4.** **PHYSICAL SECURITY** 11](#_Toc145871068)

[4.1. BUILDING SECURITY 12](#_Toc145871069)

[**5.** **NETWORK DEVICE INSTALLATION AND CONFIGURATION** 13](#_Toc145871070)

[5.1. DEVICE APPROVAL 13](#_Toc145871071)

[5.2. STANDARDIZED CONFIGURATION 13](#_Toc145871072)

[5.3. SECURITY CONFIGURATIONS 13](#_Toc145871073)

[5.4. PHYSICAL SECURITY 13](#_Toc145871074)

[5.5. FIRMWARE AND SOFTWARE UPDATES 13](#_Toc145871075)

[5.6. REMOTE ACCESS 14](#_Toc145871076)

[5.7. BACKUP CONFIGURATIONS 14](#_Toc145871077)

[5.8. CHANGE MANAGEMENT 14](#_Toc145871078)

[5.9. DEVICE DECOMMISSIONING 14](#_Toc145871079)

[5.10. NETWORK SEGMENTATION 14](#_Toc145871080)

[5.11. MONITORING AND LOGGING 14](#_Toc145871081)

[5.12. TRAINING AND AWARENESS 14](#_Toc145871082)

[**6.** **DATA HANDLING** 15](#_Toc145871083)

[6.1. CLASSIFICATION OF DATA 15](#_Toc145871084)

[6.2. STORAGE AND RETENTION 15](#_Toc145871085)

[6.3. DATA ENCRYPTION 15](#_Toc145871086)

[6.4. ACCESS CONTROL 15](#_Toc145871087)

[6.5. DATA SHARING AND TRANSFER 15](#_Toc145871088)

[6.6. BACKUP AND RECOVERY 15](#_Toc145871089)

[6.7. PHYSICAL DATA SECURITY 16](#_Toc145871090)

[6.8. DATA DISPOSAL 16](#_Toc145871091)

[6.9. INCIDENT REPORTING 16](#_Toc145871092)

[6.10. TRAINING AND AWARENESS 16](#_Toc145871093)

[**7.** **REMOTE ACCESS** 16](#_Toc145871094)

[7.1 ELIGIBILITY FOR REMOTE ACCESS 16](#_Toc145871095)

[7.2. SECURE CONNECTION PROTOCOLS 16](#_Toc145871096)

[7.3. AUTHENTICATION 16](#_Toc145871097)

[7.4. ENDPOINT SECURITY 17](#_Toc145871098)

[7.5. DATA TRANSFER 17](#_Toc145871099)

[7.6. ACCESS LIMITATIONS 17](#_Toc145871100)

[7.7. SESSION TIMEOUT AND LOGGING 17](#_Toc145871101)

[7.8. SOFTWARE and APPLICATIONS 17](#_Toc145871102)

[7.9. REPORTING SUSPICIOUS ACTIVITY 17](#_Toc145871103)

[7.10. POLICY REVIEW AND AGREEMENT 17](#_Toc145871104)

[**8.** **EMAIL** 18](#_Toc145871105)

[**9.** **INTERNET AND WEB ACCESS** 19](#_Toc145871106)

[9.1 ACCEPTABLE USE 19](#_Toc145871107)

[9.2. PROHIBITED ACTIVITIES 20](#_Toc145871108)

[9.3. WEB FILTERING 20](#_Toc145871109)

[9.4. DOWNLOAD RESTRICTIONS 20](#_Toc145871110)

[9.5. CLOUD SERVICES 20](#_Toc145871111)

[9.6. SOCIAL MEDIA USE 20](#_Toc145871112)

[9.7. SECURITY PROTOCOLS 20](#_Toc145871113)

[9.8. EMAIL LINKS AND ATTACHMENTS 20](#_Toc145871114)

[9.9. BANDWIDTH USAGE 21](#_Toc145871115)

[9.10. EXTERNAL WEB SERVICES 21](#_Toc145871116)

[9.11. TRAINING AND AWARENESS 21](#_Toc145871117)

[**10. DEVICE SECURITY** 21](#_Toc145871118)

[10.1. DEVICE REGISTRATION 21](#_Toc145871119)

[10.2. PASSWORD PROTECTION 21](#_Toc145871120)

[10.3. ENCRYPTION 21](#_Toc145871121)

[10.4. ANTI-MALWARE AND FIREWALL 21](#_Toc145871122)

[10.5 REMOTE WIPE CAPABILITY 22](#_Toc145871123)

[10.6. SOFTWARE AND UPDATES 22](#_Toc145871124)

[10.7. PHYSICAL SECURITY 22](#_Toc145871125)

[10.8. NETWORK ACCESS CONTROL 22](#_Toc145871126)

[10.9 DEVICE DECOMMISSION AND DISPOSAL 22](#_Toc145871127)

[10.10 USER RESPONSIBILITY 22](#_Toc145871128)

[10.11 TRAINING AND AWARENESS 22](#_Toc145871129)

[**11.**  **COMMUNICATING TO STAKEHOLDERS** 22](#_Toc145871130)

[11.1. INITIAL COMMUNICATION 23](#_Toc145871131)

[11.2. STAKEHOLDER MEETINGS 23](#_Toc145871132)

[11.3. TRAINING SESSIONS 23](#_Toc145871133)

[11.4. POLICY ACCESSIBILITY 23](#_Toc145871134)

[11.5. FEEDBACK MECHANISM 23](#_Toc145871135)

[11.6. ANNUAL REVIEW 23](#_Toc145871136)

[11.7. NEW EMPLOYEE INDUCTION 24](#_Toc145871137)

[11.8. EXTERNAL PARTNERS AND VENDORS 24](#_Toc145871138)

[11.9. UPDATES AND REVISIONS 24](#_Toc145871139)

[**12.** **REFERENCES** 25](#_Toc145871140)

# **1. INTRODUCTION**

## 1.1. PURPOSE

## QuantumVerse Technologies LLC stands at the forefront of medical innovation. As a leader in the medical industry, the company seamlessly blends advanced technologies with healthcare solutions. Specializing in medical research, digital health platforms, innovative diagnostic tools, and healthcare consultancy, QuantumVerse Technologies LLC is dedicated to elevating patient care and transforming the medical landscape for the future.

## This policy defines the technical controls and security configurations users and Information Technology (IT) administrators must implement to ensure the integrity and availability of the data environment at QuantomVerse Technologies LLC. It serves as a central policy document with which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides IT managers with policies and guidelines concerning the acceptable use of the company's technology equipment, e-mail, internet connections, voicemail, facsimile, future technology resources, and information processing.

## The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms.

## All QuantumVerse Technologies LLC employees or temporary workers must adhere to this policy at all locations and contractors.

## 1.2. SCOPE

This policy document defines standard security requirements for all personnel and systems that create, maintain, store, access, process, or transmit information. This policy also applies to information resources owned by others, such as contractors and private sector entities, where the company has a legal, contractual, or fiduciary duty to protect said resources while in the company's custody. In the event of a conflict, the more restrictive measures apply. This policy covers the company's network system, which comprises various hardware, software, communication equipment, and other devices designed to assist the company in creating, receiving, storing, processing, and transmitting information. This definition includes equipment connected to any company's domain or VLAN, either hardwired or wirelessly, and all stand-alone equipment deployed at its office or remote locations.

## 1.3. ACRONYMS / DEFINITIONS

Common terms and acronyms that may be used throughout this document.

**CEO:** The Chief Executive Officer is responsible for the overall privacy and security practices of the company.

**CIO**: The Chief Information Officer.

**CMO:** The Chief Medical Officer.

**CO:** The Confidentiality Officer is responsible for annual security training of all staff on confidentiality issues.

**CPO:** The Chief Privacy Officer is responsible for HIPAA privacy compliance issues.

**CST**: Confidentiality and Security Team.

**DoD:** Department of Defense.

**Encryption**: The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific ‘need to know.’

**External Media –i.e.,** CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes.

**FAT:** File Allocation Table - The FAT file system is uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.

**Firewall:** a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

**FTP**: File Transfer Protocol.

**HIPAA** - Health Insurance Portability and Accountability Act.

**IT** - Information Technology.

**LAN:** Local Area Network: a computer network that covers a small geographic area, i.e., a group of buildings, an office.

**NTFS:** New Technology File Systems**:** NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.

**SOW - Statement of Work -** An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.

**User** - Any person authorized to access an information resource.

**Privileged Users:** system administrators and others specifically identified and authorized by Company management.

**Users with edit/update capabilities:** individuals who are permitted, based on job assignment, to add, delete, or change records in a database**.**

**Users with inquiry (read only) capabilities:** individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.

**VLAN:** Virtual Local Area Network: A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.

**VPN:** Virtual Private Network: Provides a secure passage through the public Internet.

**WAN**: Wide Area Network: A computer network that enables communication across a broad area, i.e., regional, national.

**Virus -** a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer, attacks. A true virus cannot spread to another computer without human assistance.

# **2. APPLICATION SECURITY**

1. QuantumVerse Technologies LLC, specific departments, and third-party contractors are mandated to uphold application security standards, ensuring robust controls over systems they directly oversee.

a. When QuantumVerse Technologies LLC manages a software environment or application, it is accountable for executing the application security measures.

b. Departments directly managing an environment or application bear the responsibility for the application's security standards.

c. If a contractor manages an environment or software for a particular department, it is the department's duty to confirm the contractor's adherence to the security guidelines.

d. QuantumVerse Technologies LLC employees and contractors employing third-party hosting solutions or authorized functions must:

i. Seek prior sanction from the Information Resources Manager or their representative.

ii. Refrain from sharing sensitive or confidential company data.

iii. Service availability and support agreements, such as 24/7 or weekdays-only, should align with the application's expected uptime and must be relayed to QuantumVerse Technologies LLC.

1. Software installations or updates must adhere to the application lifecycle.
2. Every user, be it a developer, admin, or end-user, should possess distinct credentials for application access.
3. Verified users should only be granted access to an application to the extent they need it, in line with the principle of least privilege.
4. Application data owners must endorse the initiation or alteration of user or group access.
5. Application developers must prioritize security by adhering to best practices, aiming to mitigate potential attack repercussions.
6. Developers are advised against using live production data for application development or testing.
7. All logs—server, application, and web service—must be accumulated and stored in a legible format for a duration mandated by relevant state regulations.
8. Maintain a comprehensive list of all software solutions, highlighting authentication mechanisms, data classifications, and the criticality level of every application.

10. Formulate explicit guidelines and methodologies for reviewing, revoking, and granting authorizations.

11. Critical access rights to software should be promptly revoked for individuals who have exited the company, changed departments, or transitioned into distinct roles.

# **3. DATA BACKUP AND STORAGE**

## 3.1. DATA CLASSIFICATION AND PRIORITY

Data will be categorized based on its sensitivity, importance, and regulatory requirements. This classification will determine the backup frequency and storage type.

## 3.2. BACKUP FREQUENCY

1. Critical data: Daily
2. Important data: Weekly
3. General data: Monthly

These frequencies can be adjusted based on specific departmental or operational needs.

## 3.3. BACKUP METHODS

Incremental backups will capture changes since the last full backup, saving storage space and time. Full backups will be taken periodically to provide a comprehensive data snapshot.

## 3.4. STORAGE LOCATIONS

Backups will be stored in at least two different physical locations: one on-site for easy recovery and one off-site to safeguard against local disasters. Cloud storage may be used for off-site backups, provided the service meets the company’s security standards.

## 3.5. DATA ENCRYPTION

All backups, especially those containing sensitive data, should be encrypted during transit and at rest.

## 3.6. RETENTION POLICY

Backup data will be retained based on regulatory requirements and company needs. Older backups will be securely deleted or archived once they exceed their retention period.

## 3.7. DATA RESTORATION

Restoration tests will be conducted periodically to ensure data integrity and the efficacy of the backup process. A clear procedure will be in place detailing how to initiate a data restoration process.

## 3.8. PHYSICAL STORAGE SECURITY

On-site backup storage devices (like tapes or external hard drives) should be kept in a secure, climate-controlled environment to prevent unauthorized access and potential damage.

## 3.9. CLOUD STORAGE VENDORS

Vendors must comply with industry security standards and demonstrate a commitment to data privacy and protection. Vendor agreements should be reviewed for data ownership rights and their backup procedures.

## 3.10. INCIDENT REPORTING

Any issues, failures, or anomalies during the backup process should be reported to the IT department immediately for resolution.

## 3.11 TRAINING AND AWARENESS

Staff members involved in the backup process should receive periodic training on best practices and updates to the policy. All employees should be aware of the importance of backups and their role in the process, if applicable.

# **4. PHYSICAL SECURITY**

The first line of defense in data security is the individual user. The company’s users are responsible for the security of all data that may come to them in any format. The company is responsible for maintaining ongoing training programs to inform all users of these requirements.

**Wear an Identifying Badge so that it may be easily viewed by others:** To help maintain building security, all employees should prominently display their employee identification badge. Contractors who may be in the company’s facilities are provided with different colored identification badges. Other people who may be within the company’s facilities should wear visitor badges and should be accompanied.

**Challenge Unrecognized Personnel:** It is the responsibility of all personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted office location, you should challenge them as to their right to be there. All visitors to the company’s offices must sign in at the front desk. In addition, all visitors, excluding patients, must wear a visitor/contractor badge. All other personnel must be employees. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

**Secure Laptop with a Cable Lock:** When out of the office all laptop computers must be secured with the use of a cable lock. Cable locks are provided with all new laptops’ computers during the original set up. All users will be instructed on their use and a simple user document, reviewed during employee orientation, is included on all laptop computers. Most computers will contain sensitive data either of a medical, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during stressful periods while traveling. The cable locks are not foolproof but do provide an additional level of security. Many laptop computers are stolen in snatched and run robberies, where the thief runs through an office or hotel room and grabs all the equipment, he/she can quickly remove. The use of a cable lock helps to thwart this type of event.

**Unattended Computers:** The user will lock unattended computers when leaving the work area. This feature is discussed with all employees during yearly security training. Company policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen minutes of inactivity. Employees are not allowed to take any action which would override this setting.

## 4.1. BUILDING SECURITY

1. Entrance to the building during non-working hours is controlled by a security code system. Attempted entrance without this code results in immediate notification to the police department.
2. Only specific employees are given the security code for entrance. Disclosure of the security code to non-employees is prohibited.
3. The security code is changed on a periodic basis and eligible employees are notified by company e-mail or voicemail. Security codes are changed upon termination of employees that had access.
4. The door to the reception area is always locked and requires appropriate credentials or escort past the reception or waiting area door(s).
5. The reception area is always staffed during the working hours of 8:00 AM to 5:00 PM.
6. Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk, wear a visitor badge (excluding patients), and be accompanied by a staff member. In some situations, non-employee personnel, who have signed the confidentiality agreement, do not always need to be accompanied.
7. Swipe cards control access to all other doors. Each card is coded to allow admission to specific areas based on everyone’s job function or need to know.
8. The first floor of the building has motion detection sensors that are activated after hours. Any movement within the building will result in immediate notification to the police department.
9. All outside windows have glass breakage sensors which, if tripped, will result in immediate notification to the police department.
10. The building is equipped with security cameras to record activities in the parking lot and within the area encompassing the front entrance. All activities in these areas are recorded on a 24 hour a day 365 day per year basis.

# **5. NETWORK DEVICE INSTALLATION AND CONFIGURATION**

## 5.1. DEVICE APPROVAL

Only authorized and approved network devices shall be installed on QuantumVerse's network. Approval must be sought from the IT department before purchase or installation.

## 5.2. STANDARDIZED CONFIGURATION

Network devices should be configured according to the company's standardized settings to ensure uniformity, interoperability, and security across the network.

## 5.3. SECURITY CONFIGURATIONS

Default usernames and passwords on devices must be changed before the device is integrated into the network. Unnecessary services and ports on the device should be disabled to minimize potential vulnerabilities.

## 5.4. PHYSICAL SECURITY

Network devices should be installed in secure, access-controlled areas, such as locked server rooms or cabinets, to prevent unauthorized physical access.

## 5.5. FIRMWARE AND SOFTWARE UPDATES

Regularly update network devices with the latest firmware or software patches to protect against known vulnerabilities. Updates should be tested in a controlled environment before being deployed broadly.

## 5.6. REMOTE ACCESS

Remote administrative access to network devices should be restricted and secured using strong encryption protocols, like VPNs with multi-factor authentication.

## 5.7. BACKUP CONFIGURATIONS

Regular backups of device configurations should be taken and stored securely. This ensures quick recovery in case of device failures or errors.

## 5.8. CHANGE MANAGEMENT

Any significant changes to device configurations should follow a documented change management process, which includes approval, testing, and documentation of the change.

## 5.9. DEVICE DECOMMISSIONING

Devices that are no longer in use or are outdated should be decommissioned securely. All configurations and data should be wiped, and the device should be physically secured or disposed of properly.

## 5.10. NETWORK SEGMENTATION

Sensitive data or operations should be isolated in separate network segments. Network devices should be configured to enforce these segmentation rules and access controls.

## 5.11. MONITORING AND LOGGING

Network devices should be set up to provide logs and alerts for unusual or unauthorized activities. These logs should be regularly reviewed and stored securely.

## 5.12. TRAINING AND AWARENESS

The IT personnel responsible for installing and configuring network devices should undergo regular training to stay updated on best practices and emerging threats.

# **6. DATA HANDLING**

## 6.1. CLASSIFICATION OF DATA

All data will be classified into categories such as 'Public', 'Internal', 'Confidential', and 'Sensitive' based on its nature and sensitivity. Access to data will be granted based on its classification and the user's role within the company.

## 6.2. STORAGE AND RETENTION

All data should be stored in designated and approved storage locations, be it on-premises servers, cloud storage, or physical files. Data retention periods must be adhered to, depending on the type and classification of the data. After this period, data must be securely deleted or archived.

## 6.3. DATA ENCRYPTION

Sensitive and confidential data, both in transit and at rest, must be encrypted using company-approved encryption methods.

## 6.4. ACCESS CONTROL

Users should only have access to data necessary for their job functions (principle of least privilege). Any change in roles or responsibilities should result in a review and modification of data access rights.

## 6.5. DATA SHARING AND TRANSFER

Data should only be shared with authorized individuals or entities and through secure channels. Sensitive data transferred outside the organization must be encrypted and, where possible, sent using secure file transfer protocols.

## 6.6. BACKUP AND RECOVERY

Regular backups of critical data will be maintained. Backup frequency and methods will be determined by the data's nature and importance. Restoration procedures should be tested periodically to ensure data integrity and availability.

## 6.7. PHYSICAL DATA SECURITY

Physical data (e.g., printouts) should be stored securely when not in use and disposed of using shredders or approved disposal methods. Data storage areas, such as server rooms or file cabinets, should be secure against unauthorized access.

## 6.8. DATA DISPOSAL

Electronic data should be securely wiped or deleted when no longer needed, ensuring it is irretrievable. Physical data should be shredded or disposed of in a manner that ensures it cannot be reconstructed.

## 6.9. INCIDENT REPORTING

Any suspected or confirmed data breaches, losses, or unauthorized access should be reported immediately to the IT department and the data protection officer.

## 6.10. TRAINING AND AWARENESS

Employees should undergo regular training in data handling procedures, emphasizing the importance of data protection and the consequences of mishandling.

# **7. REMOTE ACCESS**

## 7.1 ELIGIBILITY FOR REMOTE ACCESS

Remote access will be granted to employees based on their job functions and a verified business need. Not all employees may be eligible for remote access.

## 7.2. SECURE CONNECTION PROTOCOLS

All remote connections must use secure, encrypted channels approved by the IT department, such as VPNs or secure shell (SSH). Unsecured methods like Telnet are prohibited.

## 7.3. AUTHENTICATION

Two-factor authentication (2FA) or multi-factor authentication (MFA) is mandatory for remote access. Users should never share their credentials. Passwords must conform to the company's password policy and should be changed regularly.

## 7.4. ENDPOINT SECURITY

Devices used for remote access must have updated anti-virus and anti-malware software. The IT department may conduct periodic checks to ensure remote devices comply with security standards. Personal devices, if allowed, must meet specific security requirements before being granted access.

## 7.5. DATA TRANSFER

Sensitive data must be encrypted during transfer. Users should not store sensitive or confidential company data on their personal devices unless they are encrypted and approved by the IT department.

## 7.6. ACCESS LIMITATIONS

Remote users should access only the data and systems necessary for their job functions (principle of least privilege). Unauthorized access to other parts of the network or systems is prohibited.

## 7.7. SESSION TIMEOUT AND LOGGING

Remote access sessions will automatically timeout after a period of inactivity. Users will need to re-authenticate to resume access. All remote access sessions will be logged, including user details, time, and duration of access.

## 7.8. SOFTWARE and APPLICATIONS

Remote users can only use company-approved software when accessing the internal network. Any software installations or updates on remote devices must be approved by the IT department.

## 7.9. REPORTING SUSPICIOUS ACTIVITY

Any suspicious activity, like unfamiliar prompts or unexpected session terminations, should be reported immediately to the IT department.

## 7.10. POLICY REVIEW AND AGREEMENT

Employees approved for remote access must review this policy annually and sign an acknowledgment form. Violations of the remote access policy may result in revocation of access and potential disciplinary action

# **8. EMAIL**

As a productivity enhancement tool, The Company encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or managed by Company owned equipment are considered the property of the Company – not the property of individual users. Consequently, this policy applies to all Company employees and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voicemail, instant messaging, Internet, fax, personal computers, and servers.

Company provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

1. it does not consume more than a trivial amount of employee time or resources,
2. it does not interfere with staff productivity,
3. it does not preempt any business activity,
4. it does not violate any of the following:
   1. Copyright violations: This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
   2. Illegal activities: Use of Company information resources for or in support of illegal purposes as defined by federal, state, or local law is prohibited.
   3. Commercial use: Use of Company information resources for personal or commercial profit is prohibited.
   4. Political Activities: All political activities are prohibited on Company premises. The Company encourages all its employees to vote and to participate in the election process, but these activities must not be performed using Company assets or resources.
   5. Harassment: The Company strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Company prohibits the use of computers, e-mail, voicemail, instant messaging, texting, and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is prohibited. Other examples of misuse include, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
   6. Junk E-mail: All communications using IT resources shall be purposeful and appropriate. Distributing “junk” mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several people with a request that each send copies of the letter to an equal number of people. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward an e-mail message to anyone.

While it is **NOT** the policy of the Company to monitor the content of any electronic communication, the Company is responsible for servicing and protecting the Company’s equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to/from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems, and detecting patterns of abuse or illegal activity.

The Company reserves the right, at its discretion, to review any employee’s files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Company policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed, or stored by others.

# **9. INTERNET AND WEB ACCESS**

## 9.1 ACCEPTABLE USE

Employees should utilize the internet and web services primarily for business purposes. Occasional personal use is permitted, provided it does not interfere with job performance or violate other company policies.

## 9.2. PROHIBITED ACTIVITIES

Downloading or streaming of unauthorized content, such as pirated software or media. Visiting websites that host malicious content, adult material, or promote hate or violence. Engaging in illegal activities or accessing the dark web.

## 9.3. WEB FILTERING

IT will implement a web filtering solution to block access to known malicious sites and content that is not in line with company values or poses a security risk.

## 9.4. DOWNLOAD RESTRICTIONS

Only trusted and necessary files should be downloaded. Employees should avoid downloading files from unknown sources or suspicious emails.

## 9.5. CLOUD SERVICES

Before utilizing third-party cloud services for storing or sharing company data, employees must obtain approval from the IT department. Only approved and vetted cloud services should be used.

## 9.6. SOCIAL MEDIA USE

Employees should exercise caution when discussing company matters on social media platforms. Confidential or sensitive information must never be shared. Official company accounts should adhere to the company's communication guidelines.

## 9.7. SECURITY PROTOCOLS

Employees should always ensure that connections to websites, especially those asking for personal or company information, are secured (https://). VPNs should be utilized when accessing company data from non-secure networks, such as public Wi-Fi.

## 9.8. EMAIL LINKS AND ATTACHMENTS

Avoid clicking on unknown or suspicious links in emails. Always verify unexpected attachments before opening.

## 9.9. BANDWIDTH USAGE

High-bandwidth activities for personal use, such as streaming videos or large downloads, should be avoided during peak business hours to ensure network performance for all users.

## 9.10. EXTERNAL WEB SERVICES

For those hosting or managing external-facing company web services, ensure regular updates, patches, and security reviews to prevent vulnerabilities.

## 9.11. TRAINING AND AWARENESS

Periodic training sessions will be held for employees, highlighting the risks associated with internet use, best practices, and this policy's essentials. Employees should report any suspicious activity or potential breaches to the IT department immediately.

# **10. DEVICE SECURITY**

## 10.1. DEVICE REGISTRATION

All devices used for company purposes, whether owned by the company or personal, must be registered with the IT department. Unregistered devices are not permitted to access the company network or handle company data.

## 10.2. PASSWORD PROTECTION

Devices must be secured with strong, unique passwords that adhere to the company's password policy. Devices should be set to auto-lock after a period of inactivity and require password re-entry upon waking.

## 10.3. ENCRYPTION

All company-owned devices and personal devices accessing company data must have full disk encryption enabled to protect stored data.

## 10.4. ANTI-MALWARE AND FIREWALL

Devices should have updated anti-malware software and a firewall installed. Regular scans and updates are mandatory.

## 10.5 REMOTE WIPE CAPABILITY

Mobile devices and laptops that can access company data should have remote wipe capabilities enabled to ensure data can be deleted in case of loss or theft.

## 10.6. SOFTWARE AND UPDATES

Only company-approved software should be installed on devices. Regular software and operating system updates should be performed to patch vulnerabilities.

## 10.7. PHYSICAL SECURITY

Refer to the [Physical Security section](#_4._PHYSICAL_SECURITY).

## 10.8. NETWORK ACCESS CONTROL

Devices should only connect to trusted networks. Public Wi-Fi should be used cautiously, preferably with a VPN.

## 10.9 DEVICE DECOMMISSION AND DISPOSAL

Devices being decommissioned should have all data securely wiped. The IT department should oversee the disposal process to ensure no data is retrievable.

## 10.10 USER RESPONSIBILITY

Users are responsible for the security of their devices and the data they access. Any suspicious activity, such as unrecognized prompts or potential breaches, should be reported to the IT department.

## 10.11 TRAINING AND AWARENESS

Employees should be trained in device security best practices, the importance of maintaining device security, and potential threats.

# **11. COMMUNICATING TO STAKEHOLDERS**

## 11.1. INITIAL COMMUNICATION

Upon the release or update of the IT policy, the IT Department, in collaboration with the Communication and HR Departments, will send out an official notification to all employees and relevant stakeholders via email. This email will contain:

1. A brief overview of the changes or introduction of the policy.
2. A link or attachment to the complete policy document.
3. Contact information for any queries or clarifications.

## 11.2. STAKEHOLDER MEETINGS

Regularly scheduled meetings will be organized for major stakeholders, especially department heads and team leaders, to discuss the policy in detail. These meetings will provide a platform for clarifying doubts, discussing implementations, and addressing any concerns.

## 11.3. TRAINING SESSIONS

QuantumVerse Technologies LLC will host mandatory training sessions for all employees to ensure they understand and can effectively adhere to the policy. These sessions will be organized by the IT and HR Departments and will be tailored to various roles within the company, focusing on the aspects of the policy most relevant to each role.

## 11.4. POLICY ACCESSIBILITY

The IT policy will be continuously accessible to all stakeholders via the company’s intranet or a dedicated portal. Physical copies will also be available upon request.

## 11.5. FEEDBACK MECHANISM

A system will be set up to allow stakeholders to provide feedback on the IT policy. This can be done through the company intranet, suggestion boxes, or dedicated email channels. Feedback will be periodically reviewed, and constructive suggestions may be incorporated into future policy revisions.

## 11.6. ANNUAL REVIEW

At least once a year, stakeholders will receive a reminder about the IT policy, any changes made in the past year, and a prompt to review and familiarize themselves with the policy once more.

## 11.7. NEW EMPLOYEE INDUCTION

All new employees, regardless of their role, will be introduced to the IT policy as part of their onboarding process. They will be provided with both a digital and physical copy and will be required to sign an acknowledgment form indicating they have read and understood the policy.

## 11.8. EXTERNAL PARTNERS AND VENDORS

Any external entities working closely with QuantumVerse Technologies LLC, especially those handling sensitive medical data, will be provided with relevant excerpts of the IT policy. They may be required to adhere to specific parts of the policy or, at a minimum, be aware of it.

## 11.9. UPDATES AND REVISIONS

Whenever significant revisions are made to the IT policy, the communication process will be repeated to ensure all stakeholders are aware of and understand the changes. It is essential for QuantumVerse Technologies LLC to regularly assess the effectiveness of this communication process and make necessary adjustments based on stakeholder feedback and the evolving needs of the company.

# **12. REFERENCES**

*Information Security Policy Template | HealthIT.gov*. (n.d.). https://www.healthit.gov/resource/information-security-policy-template

Kurtz, J. (2020). Securing Internet-Connected Medical Devices | NIST. *NIST*. https://www.nist.gov/blogs/manufacturing-innovation-blog/securing-internet-connected-medical-devices

Sam Houston State University. (n.d.). *Information Technology Policies - SAM Houston State University*. SHSU. https://www.shsu.edu/intranet/policies/information\_technology\_policies/index.ht

Santos, O. (2018). Developing Cybersecurity Programs and Policies (3rd ed.). Pearson Technology Group. https://online.vitalsource.com/books/9780134858548