CitiusTech User Security and IT Policy (CUSIP)

Version 3.0

27th Dec 2024

Kapil Gurav

Revision History

Document Version	Revision Date	Prepared By	Approved By	Approval Date	Summary of Changes
2.0	29nd Oct 2020	Sanjiv M	Punam Shejale	30th Oct 2020	Updated as per HiTrust requirements and did minor changes like formatting and grammar.
2.1	16th Jan 2022	Ruchi V	Punam Shejale	7th Feb 2022	Updated for Sec-4.8 E-Mail Usage, Internet Usage and Security & Sec-5.0 Enforcement of CUSIP, other minor changes.
2.2	06th Feb 2023	Ruchi V	Punam Shejale	10th Feb 2023	Annual revision, no change.
2.3	10th Feb 2024	Lavin P.	Punam Shejale	14th Feb 2024	Annual revision, no change.
3.0	22nd Dec 2024	Lavin P	Punam Shejale	27th Dec 2024	Annual Review, No change

1.0 Key Terms and Definitions Used in the Document

The following is the list of Key Terms used throughout the document along with their definitions:

- **CitiusTech** refers to CitiusTech Healthcare Technology Private Limited along with all of its overseas branches and subsidiaries.

- **User** refers to all authorized users of ANY IT systems at CitiusTech, including full time employees and contractors (whether full time or part time, and whether working from a CitiusTech office or remotely, including consultants, freelancers, and personnel affiliated with CitiusTech on behalf of third parties).

- **CUSIP** refers to the CitiusTech User Security & IT Policy which includes the HIPAA guidelines.

- **Workstation** refers to all desktop computers, laptop computers, tablet devices, thin clients, and all other similar devices.

- **Confidential Information** refers to information about CitiusTech and/or its Clients that is confidential in nature and not known to the general public. This includes information that is technical and non-technical in nature.

- **Protected Health Information (PHI)** refers to PHI is health information in any form or medium that identifies an individual, and relates to:
  -an individual's past, present or future physical or mental condition

  -provision of healthcare to the individual

  -the past, present or future payment for the provision of healthcare to the individual

- **Electronic Protected Health Information (ePHI)** refers to health information that a HIPAA covered entity creates or receives in electronic (computer) media and / or is maintained in any form of electronic media, including but not limited to:
  - computer files & email; shared network drives for HIPAA covered programs
  - laptop computers, CDs and any other portable electronic devices

- **Personally, Identifiable Information (PII)** refers to any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains, e.g. individual's name, SSN number, Driver's License, financial credit card account numbers etc.

- **CitiusTech Systems** refers to CitiusTech Workstations, LAN/WAN equipment, file servers, computer equipment, software, operating systems, software applications, storage media, network devices, accounts providing electronic mail, WWW browsing facilities, client data, and FTP sites at / of CitiusTech.

- **Official Work** refers to any work required to be done in the course of the business of CitiusTech, including work for the Clients of CitiusTech.

- **Blogging** refers to a personal journal published on the World Wide Web consisting of discrete entries ("posts") including postings in Q&A forums and technical and personal blogs.

- **Social media** refers to web-based and mobile technologies which are used to turn communication into an interactive dialogue & allow the creation and exchange of User-generated content, whether by a focus group, an individual or an organization.

2.0 Overview and Purpose

Effective security is a team effort involving the participation and support of every User who deals with information and/or information systems. It is the responsibility of every User to know and understand CUSIP, HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation) and other data privacy compliance requirements and to conduct his/her activities accordingly.

CUSIP outlines the acceptable use of CitiusTech Systems. In addition, CUSIP also includes the HIPAA, GDPR and data privacy requirements that employees and partners need to comply with. CUSIP is designed to protect the interests of employees, customers, partners and CitiusTech. Breach of CUSIP by any User may expose CitiusTech, its partners and customers to risks including virus attacks, compromise of network systems and services, damage to reputation, legal risks and penalties.

It is every User's responsibility to attend the Security & HIPAA awareness programs at least once in six months.

All employees, third-party users, contractors acknowledge that their actions may be monitored, and that they consent to such monitoring by signing CUSIP.

The CUSIP will be periodically reviewed for currency & applicability. The most recent version of the document will be available on InterCT, CitiusTech's intranet.

3.0 Scope

This policy applies to all Users as defined in Section 1.0 above. In addition, this policy applies to all equipment and physical premises that is owned or leased by CitiusTech.

All Users are required to abide by the CitiusTech's policies and procedures, as applicable to them. Users are responsible for exercising good judgment regarding the reasonableness of this policy. All user activities on CitiusTech network, applications and workstation will be logged and monitored. In- case of any uncertainty, a User may consult with his / her supervisor or manager.

4.0 Information Security & HIPAA Compliance Requirements

4.1 Physical Control

- All Users are required to visibly display their identity cards at all times when in CitiusTech's premises.
- All users & visitors shall declare personal removable media at reception & surrender if required.
- All visitors to provide visitor privacy consent by signing the visitor register before entering CitiusTech premises.
- All visitors to CitiusTech's premises are required to be accompanied by a CitiusTech employee at all times and visitor access needs to be restricted to common areas only.
- Visitors within the CitiusTech premises are required to visibly display their identity cards at all times when in CitiusTech's premises.
- Under no circumstances is a User authorized to engage in any activity that is illegal under local, state, federal or international law while using CitiusTech owned resources, or client provided end-points, whether from CitiusTech premises or client premises.

4.2 Access Control & Password Management

- Users are assigned a unique "User ID" for logging into the network and for accessing internal IT systems. Each User is provided "role-based" access which is limited to the information needed to perform the User's job.
- Users are responsible for the security of their passwords / User IDs and complying with prescribed password management guidelines.
- Users are required to follow CitiusTech password policy on application and databases managed by them.
- Users are EXPLICITLY PROHIBITED from sharing User IDs & passwords with ANYONE else (including but not limited to the reporting head of the User). Sharing User IDs & Passwords gives UNAUTHORIZED access to other individuals to information that they are not entitled to. Similarly, Users should not share passwords with family members or any non-CitiusTech personnel when working from home.
- Any breach arising from sharing User IDs & passwords is the responsibility of the person sharing the User ID & Password and the person receiving this information.
- Users are required to always lock or log-off their workstations before leaving a workstation unattended to prevent other individuals from accessing any confidential & proprietary information.

4.3 Computer Systems & Network Security

- CitiusTech reserves the right to audit networks and systems periodically to ensure compliance with CUSIP without prior intimation.

- For security and network maintenance purposes, CitiusTech may monitor equipment, system use and network traffic at any time.
- Bluetooth, USB & CD drives are disabled on all computers, except for Executive management, BLLs, DLs, sales, function heads and members traveling onsite for project / business development purposes.
- Connecting portable media such as external USB / pen drives, hard disks, CD/ DVD writers, audio/ video media players, cameras, mobile phones is prohibited. Sharing of files through LAN is not allowed.
- Effecting security breaches of network communication is strictly prohibited. Security breaches include, but are not limited to, accessing data which the User is not meant to access, or logging into a server or account that the User is not explicitly authorized to access. Port scanning or security scanning is prohibited unless authorized.
- Effecting disruptions of network communication is strictly prohibited. Disruptions include, but are not limited to, network sniffing, network monitoring, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes, or circumventing user authentication or security of any host, network, or account.
  For any remote access to CitiusTech network, users are required to seek approval from their reporting managers.

  For remote access, only company provided laptops are to be used. Use of Personal desktops and laptops is PROHIBITED for connecting to the CitiusTech Network.

- Users are required to ensure the following network security standards for remote access:
  - Anti-virus and Anti-spyware software are running and up-to-date.
  - Unnecessary services and programs are turned off.
  - Physical security safeguards are in place to prevent unauthorized access.
- To implement Clear Screen & Clear Desk policy users shall abide by the following guidelines:
  - All confidential or restricted information shall be kept under lock & key when the User is away from desk.
  - All printouts of confidential or restricted information shall be destroyed when not required.
  - Users are required to lock their screens before leaving a workstation unattended to prevent other individuals from accessing any confidential & proprietary information and risk of overlooking by unauthorized persons.
- Users shall ensure compliance to Client as well as CitiusTech computer and network security policies when using Client laptop/desktop in CitiusTech premises.
- Users shall ensure assets are protected from unauthorized access, disclosure, modification, destruction or interference;
- To ensure Mobile security users shall comply to following guidelines:
  - Personal laptops/tablets/iPad shall not be brought within CitiusTech premises and shall not be used to access CitiusTech and/or client data.

- Team laptops/iPad/tablets etc. shall be accessed using CitiusTech IT team provided credentials ONLY.
- Mobile devices shall not be left unattended at any given point in time and they shall ensure that these devices are kept under lock and key.
- No client or CitiusTech data shall reside on the local drives of Team laptops/iPad/tablets. These devices shall not be carried outside CitiusTech premises, unless there is an explicit management approval for the same.
- CitiusTech email IDs on smartphones (CitiusTech issued or personal), shall be configured by the CitiusTech IT team only if there is a valid business need and the same is approved by the user's Reporting Head.

- Disciplinary actions & monetary penalties may be levied for loss of Client or CitiusTech provided hardware asset e.g. iPod, iPhone, laptops, removable media, etc.

4.4 Data and Information Management

- ALL data on the CitiusTech corporate systems remains the property of CitiusTech and/or its Clients.
- Users are responsible for protecting ALL Confidential Information whether it belongs to them or otherwise. All Users are required to take necessary steps to prevent unauthorized access to Confidential Information residing on CitiusTech's network including any client confidential data.
- CitiusTech does not commit to ensuring that User e-mail accounts are backed up. In case any User e-mail contains information that needs to be stored & backed up, the same should also be kept in the designated area allocated on the File Server for that Project/ Function to ensure backups are taken.
  No backups shall be taken of information stored only on the local laptops or desktops. All information assets that are not personal in nature needs to be kept in the designated area allocated on the File Server for that Project/ Function to ensure backups are taken.
- Users may access PII/ PHI / ePHI as part of their work, PII/PHI ePHI is required to be managed as Confidential Information and need special consideration as described in Section 4.5 of this document.
- Users are required to not leave any Confidential Information in the public domain e.g., paper documents on the workstations, near printers / copiers etc.
- Sharing any CitiusTech information which is not available in the public domain with anyone is strictly prohibited, unless it is explicitly authorized.
- Users may use CitiusTech systems for personal use in a limited and reasonable manner, only to the extent permitted by CitiusTech's policies. It is clearly understood that CitiusTech does not and cannot guarantee the confidentiality of any personal information stored on its systems. Personal information on CitiusTech Systems will be subject to monitoring and reviews as required by CitiusTech for security, compliance and/or any other needs.
- Users **ARE NOT** permitted to connect any portable devices (USB/hard drive/CDs etc.) to CitiusTech provided workstations (laptops/desktops).

- Users **ARE NOT** permitted to download or store non-work-related video or music files on CitiusTech provided workstations (laptops/desktops) or anywhere else on the CitiusTech network.
- Users shall not access non-work-related websites, download installable when connected to client or CT network.

4.5 PHI/PII Data Security

Users are required to follow the special guidelines for handling Personally Identifiable Information (PII), Protected Health Information (PHI) & Electronic Protected Health Information (ePHI) at all times:

- To ensure privacy of personal information, only relevant personal information should be gathered and processed for the specified purposes, if required. This information should not be retained for a period longer than is necessary for the purpose.
- Client PII/ PHI/ePHI should not be stored on CitiusTech network. If PII/PHI/ePHI is required to be stored for any reason, it shall be done only with Client approval. Also, the PII/ PHI / ePHI can be stored in PHI Vault (PHI Vault is a secure server hosted only for storing PHI) only and NOT on local machines or any other CitiusTech network locations.
- CitiusTech employee, vendor, contractor and visitor PII will be stored under appropriate security controls to ensure data confidentiality and privacy. Any access should be minimum necessary and as per role with appropriate authorizations.
- Do not send PII/PHI on email to anyone. Sending PII/PHI on email is permitted only after receiving required approval. Use Client email (if provided) for sharing password protected PII/PHI data over mail.
    - In case confidential/PHI/ PII files are required to be shared over email, then the files should be protected through use of encryption or passwords. Such e-mails can only be sent to known parties as approved by client or function head.
    - Passwords shall NOT be communicated in the same email as the file. Password shall not be shared with multiple people at the same time.
    - There shall be a delay of at least 15 minutes from the time the first email with the file was sent.
    - Otherwise passwords shall be shared using a different mode than the mode used for sharing the confidential file. Example, the file is shared on email/ over SFTP & password is communicated over call/ SMS.
- PII/ PHI cannot be printed without approval and ensure that no PII/PHI documents are left unattended at any time. All PII/PHI documents need to be filed in secure lockers only.
- Dispose paper containing PII/PHI using a shredder ONLY.
- In case of any doubt on handling PII/PHI, get in touch with your Reporting Manager/ ADL/ DL or Chief Information Security Officer (CISO) or Data Protection Officer (DPO).

Refer to CitiusTech Privacy Policy on CitiusTech website or on the Intranet for more details on how CitiusTech handles personal information and data privacy.

4.6 Production & Test data Security

- Get client confirmation if the data received is test data or production data prior to using the data for development or testing purposes. As a best practice avoid bringing & using any production data into CitiusTech network.
- Project Teams shall avoid using the production data for any testing that triggers emails. All such fields shall be replaced by dummy email IDs in the data.
- In case the data is production data, the same shall be treated as confidential data and all controls as applicable to handling such confidential data shall be implemented. Following controls shall apply: -
    - Production
    - Data shall be used only for the instance it was shared. It shall not be used for any other instance without prior client confirmation.
    - Access shall be restricted on need to know basis. Periodic access review shall be performed.
    - No local/ multiple copies of the data shall be created.
    - Production data shall be deleted once no longer required.

4.7 Virus and Malicious Code Security

- All hosts connected to the CitiusTech Internet/Intranet/Extranet, whether owned by CitiusTech or otherwise, need to continually execute approved virus-scanning software with a current virus database.
- Turning off the approved virus-scanning software is prohibited without prior authorization.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited.
- Users shall regularly check status of antivirus client on their machines and log an issue with IT if antivirus client on their machine is out of date or corrupt.

4.8 E-Mail Usage, Internet Usage and Security

- Users are required to use the official "@citiustech.com" email ID for Official Work-related communication. Use of personal email IDs is strictly prohibited for Official Work.
- Client Email IDs given to Users for communication are required to be used only for Official Work and use of such email IDs for any other purposes including personal use will be regarded as a breach of CUSIP.
- Users are required to ensure that no PII/PHI/ ePHI data is emailed to anyone without prior Client authorization. In case a User receives an email with PII/PHI data, the User is required to store it securely on approved secure server locations only. Such emails should NOT be distributed and PII/PHI content should be permanently deleted from the email boxes (including DELETE folder).

- Users are required to use extreme caution and discretion when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- Users are required to ensure that no PII/PHI / ePHI data is emailed to anyone without prior authorization. In case a User receives an email with PII/PHI data, the User is required to store it securely and NOT distribute the same through email OR otherwise without prior authorization.
- The following activities are STRICTLY PROHIBITED:
    - Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). o Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
    - Unauthorized use, or forging, of email header information.
    - Solicitation of email for any other email address, other than that of the person's account, with the intent to harass or to collect replies.
    - Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
    - Use of unsolicited email originating from within CitiusTech's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CitiusTech or connected via CitiusTech's network.
    - Mass mailing or posting non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Internet Access is provided for Official Work-related tasks ONLY.
- Limited personal use is permitted at CitiusTech's discretion. This personal privilege can be revoked by CitiusTech without citing any reason whatsoever, including intentional or unintentional misuse / abuse of Internet for any reason.
- While connected to CitiusTech's network, using USB or Bluetooth devices for connecting to the internet is prohibited – e.g. using USB data cards, modems, using mobile phones as modems, etc.
- Internet access while connected to client networks (either using dial up VPN or any other mode) is STRICTLY for Official Work ONLY. Any use of client internet for personal reasons, while connected to the client network for accessing social media sites, personal email accounts, accessing IM services, downloading/ uploading any non-Official Work-related content will be considered as a breach of CUSIP.
- Blogging or using any social media by Users, is also subject to the following terms and restrictions:
    - Limited use of blogging or accessing social media websites is acceptable, provided that such access is used in a professional and responsible manner, does not otherwise violate CUSIP and it does not interfere with the User's regular work duties.
    - Users understand and acknowledge that accessing social media websites and personal email accounts (Facebook, Orkut, Twitter, YouTube, Yahoo, Hotmail, Gmail etc.) from CitiusTech Workstations is subject to monitoring by CitiusTech.

- While blogging or using any social media, Users are required to ALWAYS comply with the following conditions:
    - Users are prohibited from revealing any CitiusTech or client confidential or proprietary information, client names, solutions offered to clients, business segments, trade secrets or any other material covered in the CUSIP when engaged in blogging or accessing social media sites.
    - Users are required to not engage in any blogging and social media activities that may harm or tarnish the image, reputation and/or goodwill of CitiusTech and/or any of its employees or Clients.
    - Users are prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by policies at CitiusTech.
    - Users may also not attribute personal statements, opinions or beliefs to CitiusTech. o If a User expresses his or her beliefs and/or opinions in blogs, they may not, expressly or implicitly, represent themselves as an employee or representative of CitiusTech.
    - Users assume any and all risk associated with blogging or using social media.
    - CitiusTech's trademarks, logos, and any other intellectual property of CitiusTech may also not be used in connection with any blogging or social media activity unless authorized.

4.9 Protection of Intellectual Property & Software Anti-Piracy

- CitiusTech adheres to the highest levels of compliance with respect to protection of intellectual property of other parties and software anti-piracy regulations.
- The following activities are strictly prohibited, with NO EXCEPTIONS:
    - Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by CitiusTech.
    - Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CitiusTech or the end user does not have an active license.
    - Using CitiusTech computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment laws or hostile workplace laws in the User's local jurisdiction. o Publicly commenting on trademark or copyrighted material including software reviews unless authorized.
    - Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.
- Any content, software program, application created using CitiusTech's systems / premises remains the intellectual property of CitiusTech and/or its Clients as the case may be, and Users are required to ensure that such content is not shared without explicit authorization.

- Disciplinary actions & additional monetary penalties may also be levied for the use of unauthorized, pirated or cracked versions of licenses, software & and downloaded media files- music/videos/ movies/pictures, etc. found on either on the individual, project or CT computers and network.

4.10 Business Continuity & Disaster Management

All Users are required to support and participate actively in any business continuity and disaster management programs implemented by CitiusTech from time to time.

4.11 Incident Reporting

All Users are required to report any suspicious behaviour observed, potential data breach or breach of any policy contained in the CUSIP by sending an E-mail to: infosec@citiustech.com

5.0 Enforcement of CUSIP

- Any user found to have violated this policy may be subject to disciplinary actions including monetary penalties, suspension from services, termination of contract and/or employment with CitiusTech. Additional actions may be initiated based on management discretion and nature of violation or incident.
- Any unauthorized, wilful or malicious release of any information associated with Protected Health Information or data breach may result in personal civil or criminal liability.
- Appropriate management approvals are needed for any activity which is prohibited under CUSIP.
- Any amendments to the CUSIP will be made available to all on the Intranet and the same shall be applicable to all, including those who may have signed the earlier version.
- All users are mandatorily required to complete Information Security Awareness Training and Test every 6 months, which reinforces and records re-attestation of CUSIP by all users.

6.0 Employee and Partner Acceptance

I have read and understood the **CitiusTech User Security & IT Policy** and I agree and accept the requirements in its entirety without exceptions.

ID: 37370

Name: Kapil Chandrashekhar Gurav

Signature: Kapil Gurav

Date: 13/08/2025