Information Security Policy

Department Responsible: IT	Version: 3.0
Document Author: Jobin Mathew	Effective Date: 01/03/2022
Document Approver: Sudeep Chandran, Director	Review Date: 28/02/2022

Change Rec

Date	Author	Version	Change Reference
20/07/2019	Aneesh Kumar	1.0	First Draft
01/12/2020	Jobin Mathew	2.0	Policy Update
21/02/2022	Jobin Mathew	3.0	Policy Update

Table of Contents

Information Security Policy

Introduction

1.1 Purpose

Information Security Policy

We at Gapblue recognize that information is one of our most important assets. As we are operating in a competitive market, our ability to achieve our business goals is dependent on our competence to safeguard the information. We shall protect our information assets to ensure their Confidentiality, Integrity, and Availability. Gapblue in its normal course of business generates data and this data when assimilated constitutes information. This information, when analyzed may give the reader enough knowledge¯ of the way we perform, the reasons for our success and the key contributors to our market leadership position.

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement to ensure the integrity and availability of the data environment at Gapblue Software Labs, hereinafter, referred to as the Gapblue. 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 within Gapblue with policies and guidelines concerning the acceptable use of Gapblue 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. This policy must be adhered to by all Gapblue employees or temporary workers at all locations and by contractors working with Gapblue as subcontractors.

Gapblue's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Gapblue's established culture of openness, trust, and integrity. We are committed to protecting Gapblue's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.2 Scope

This policy document defines common security requirements for all Gapblue 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 of the Gapblue, entities in the private sector, in cases

where the Gapblue has a legal, contractual, or fiduciary duty to protect said resources while in Gapblue custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Gapblue network system which is comprised of various hardware, software, communication equipment and other devices designed to assist Gapblue in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Gapblue domain or VLAN, either hardwired or wirelessly and includes all stand-alone equipment that is deployed by the Gapblue at its office locations or remote locales.

2 Employee Responsibilities

2.1 Employee Requirements

The first line of defense in data security is the individual Gapblue user. Gapblue users are responsible for the security of all data which may come to them in whatever format. Gapblue is responsible for maintaining ongoing training programs to inform all users of these requirements.

Challenge Unrecognized Personnel **-** It is the responsibility of all Gapblue personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted Gapblue office location, you should challenge them as to their right to be there. All visitors to Gapblue 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 of Gapblue. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Unattended Computers **-** Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Gapblue policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15) minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Home Use of Gapblue Corporate Assets - Only computer hardware and software owned by and installed by Gapblue IT is permitted to be connected to the company network. The only software that has been approved for corporate use by IT may be installed on any type of equipment. Personal computers/Laptops/Mobile devices supplied by Gapblue are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by Gapblue for home use.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of Gapblue are the property of Gapblue unless covered by a

contractual agreement. Nothing contained herein applies to software purchased by Gapblue employees at their own expense.

2.2 Prohibited Activities

Personnel is prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred because of a user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.
- Exception: Authorized information system support personnel, or others authorized by the Gapblue IT officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on Gapblue computers must be approved by Gapblue.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by Gapblue is strictly prohibited.
- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures, or business interests of Gapblue is strictly prohibited.

2.3 Electronic Communication, E-mail, Internet Usage

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

Information Security Policy

Gapblue 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 if:

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:

    a) 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.
    b) Illegal activities – Use of Gapblue information resources for or in support of illegal purposes as defined by federal, state, or local law is strictly prohibited.
    c) Commercial use – The use of Gapblue information resources for personal or commercial profit is strictly prohibited.
    d) Political Activities – All political activities are strictly prohibited on Gapblue premises. Gapblue encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Gapblue assets or resources.
    e) Harassment –Gapblue strives to maintain a workplace free of harassment that is sensitive to the diversity of its employees. Therefore, Gapblue prohibits the use of computers, e-mail, voice mail, 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 are strictly prohibited. Other examples of misuse include, but are 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.
    f) 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 the e-mail message to anyone.

Gapblue is responsible for servicing and protecting Gapblue’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, electronic communications may be monitored including, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

Information Security Policy

Gapblue 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 Gapblue's policies.

2.4 Report Security Incidents

It is the responsibility of each Gapblue employee or contractor to report perceived security incidents continuously to the appropriate manager or security person. A user is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the IT officer. Users should report any perceived security incident to either their immediate supervisor, their department head, or any member of Gapblue IT.

Reports of security incidents shall be escalated as quickly as possible. Each member of the Gapblue IT must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary.

Security breaches shall be promptly investigated. If criminal activity is suspected, the Gapblue IT officer shall contact the appropriate law enforcement and investigative authorities immediately.

2.5 Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information by the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by Gapblue and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Gapblue policy and will result in personnel action and may result in legal action.

2.6 Transferring Software and Files between Home and Work

Personal software shall not be used on Gapblue computers or networks. If a need for specific software exists, submit a request to your manager or department head. Users shall not use Gapblue purchased software at home or non-Gapblue computers or equipment.

Information Security Policy

Gapblue proprietary data, IT Systems information, financial information, or human resource data, shall not be placed on any computer that is not the property of Gapblue without the written consent of the respective manager or department head. It is crucial to Gapblue to protect all data and, to do that effectively, we control the systems in which it is contained. If a manager or department head receives a request to transfer Gapblue data to a non-Gapblue Computer System, the manager or department head should notify the IT officer or appropriate personnel of the intentions and the need for such a transfer of data.

The Gapblue Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since Gapblue does not control non-Gapblue personal computers, Gapblue cannot be sure of the methods that may or may not be in place to protect Gapblue sensitive information, hence the need for this restriction.

2.7 Internet Considerations

Special precautions are required to block Internet (public) access to Gapblue information resources not intended for public access, and to protect confidential Gapblue information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of the Gapblue IT Officer or appropriate personnel authorized by Gapblue shall be obtained before:

- An Internet, or other external network connection, is established.
- Gapblue information (including notices, memoranda, documentation, and software) is made available on any Internet-accessible computer (e.g., web or FTP server) or device.
- Users may not install or download any software (applications, screen savers, etc.). If users need additional software, the user is to contact their supervisor.
- The use shall be consistent with the goals of Gapblue. The network can be used to market services related to Gapblue, however, use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, login passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- The encryption software used, and the specific encryption keys (e.g., passwords, passphrases), shall be escrowed with the Gapblue IT officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

2.8 Use of WinZip encrypted and zipped e-mail

This software allows Gapblue personnel to exchange e-mails with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Gapblue staff member who desires to utilize this technology may request this software from the IT officer or appropriate personnel.

3 Identification and Authentication

3.1 User Logon IDs

Individual users shall have unique login IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their login ID.

All user login IDs are audited at least twice yearly, and all inactive login IDs are revoked. Gapblue Human Resources Department notifies the Security Officer or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

The login ID is locked or revoked after a maximum of three (3) unsuccessful login attempts which then require the passwords to be reset by the appropriate Administrator.

Users who desire to obtain access to Gapblue systems or networks must have a completed and signed Network Access Form (Appendix C). This form must be signed by the manager or department head of each user requesting access.

3.2 Passwords

User Account Passwords

User IDs and passwords are required to gain access to all Gapblue networks and workstations. All passwords are restricted by a corporate-wide password policy to be “Strong.” This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password to obtain access to any electronic information both at the server level and at

the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are required to be a minimum of eight characters.

Content Requirements - Passwords must contain a combination of upper- and lower-case alphabetic characters, numeric characters, and special characters.

Change Frequency – Passwords must be changed every 90 days (about 3 months). Compromised passwords shall be changed immediately.

Reuse - The previous twelve passwords cannot be reused.

Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential.

Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens and are never printed or included in reports or logs.

Two-Factor authentication – Users are also required setup and maintain a two-factor authentication for their user account based on any one of company approved methods

3.3 Confidentiality Agreement

Users of Gapblue information resources shall sign, as a condition for employment, an appropriate confidentiality agreement (Appendix D). The agreement shall include the following statement or a paraphrase of it:

> *I understand that any unauthorized use or disclosure of information residing on the Gapblue information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.*

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document before accessing Gapblue information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending, or employees are leaving an organization.

3.4 Access Control

Information resources are protected using access control systems. Access control systems include both internal (i.e., passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e., port protection devices, firewalls, host-based authentication, etc.).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources. Access is granted only by the completion of a Network Access Request Form (Appendix C). This form can only be initiated by the appropriate department head and must be signed by the department head and the Security Officer or appropriate personnel.

Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

3.5 User Login Entitlement Reviews

If an employee changes positions at the Gapblue, the employee's new manager or department head shall promptly notify the Information Technology ("IT") Department of the change of roles by indicating on the Network Access Request Form (Appendix C) both the roles or access that need to be added and the roles or access that need to be removed so that employee has access to the minimum necessary data to effectively perform their new job functions. The effective date of the position change should also be noted on the Form so that the IT department can ensure that the employee will have appropriate roles, access, and applications for their new job responsibilities. For a limited training period, it may be necessary for the employee who is changing positions to maintain their previous access as well as add the roles and access necessary for their new job responsibilities.

No less than annually, the IT Manager shall facilitate entitlement reviews with department heads to ensure that all employees have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum necessary data to facilitate HIPAA compliance and protect client data.

3.6 Termination of User Logon Account

Upon termination of an employee, whether voluntary or involuntary, the employee's manager or department head shall promptly notify the IT Department by indicating "Remove Access" on the employee's Network Access Request Form and submitting the form to the IT Department. If an employee's termination is voluntary and the employee provides notice, the employee's manager or department head shall promptly notify the IT Department of the employee's last scheduled workday so that their user account(s) can be configured to expire. The employee's department head shall be responsible for ensuring that all keys, ID badges, and other access devices, as well as Gapblue equipment and property, is returned to the Gapblue before the employee leaves the Gapblue on their final day of employment.

No less than quarterly, the IT manager or their designee shall provide a list of active user accounts for both network and application access, Department heads shall review the employee access lists within five (5) business days of receipt. If any of the employees on the list are no longer employed by Gapblue, the department head will immediately notify the IT Department of the employee's termination status and submit the updated Network Access Request Form.

4 Network Connectivity

4.1 Telecommunication Equipment

Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the IT officer or appropriate personnel and ordered by the appropriate personnel. Telecommunication equipment and services include but are not limited to the following:

- Phone headsets
- Software type phones installed on workstations
- Conference calling contracts
- Cell phones
- Android or iOS devices
- Call routing software
- Call reporting software
- Phone system administration equipment
- T1/Network lines
- Long-distance lines
- Telephone equipment

4.2 Permanent Connections

Information Security Policy

The security of Gapblue systems can be jeopardized from third party locations if security resources are inadequate. When there is a need to connect to a third-party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of Gapblue systems. The IT Officer or appropriate personnel should be involved in the process, design, and approval.

4.3 Emphasis on Security in Third-Party Contracts

Access to Gapblue computer systems or corporate networks should not be granted until a review of the following concerns has been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the Gapblue Information Security Policy have been reviewed and considered.
- Policies and standards established in the Gapblue information security program have been enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- A description of each service is to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to Gapblue computer systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized users.
- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding the protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreement agreed upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

4.4 Firewalls

Authority from the IT officer or appropriate personnel must be received before any employee or contractor is granted access to a Gapblue router or firewall.

5 Malicious Code

5.1 Antivirus Software Installation

Antivirus software is installed on all Gapblue personal computers and servers. Virus update patterns are updated daily on the Gapblue servers and workstations. Virus update engines and data files are monitored by an appropriate administrative staff that is responsible for keeping all virus patterns up to date.

Configuration - The antivirus software currently implemented by Gapblue is Bitdefender. End point protection is also established using Microsoft Defender on Windows laptops/desktops.

Remote Deployment Configuration - Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as-needed basis.

Monitoring/Reporting – A record of virus patterns for all workstations and servers on the Gapblue network may be maintained. The appropriate administrative staff is responsible for providing reports for auditing and emergencies as requested by the IT officer or appropriate personnel.

5.2 New Software Distribution

Only software created by Gapblue application staff, if applicable, or software approved by the IT officer or appropriate personnel will be used on internal computers and networks. A list of approved software is maintained in Appendix C. All new software will be tested by appropriate personnel to ensure compatibility with currently installed software and network configuration. In addition, the appropriate personnel must scan all software for viruses before installation.

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the IT Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Gapblue computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage Gapblue hardware, software, or data and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a Gapblue computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Gapblue personnel for instructions for scanning files for viruses.

5.3 Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of Gapblue are the property of Gapblue unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Gapblue ownership at the time of employment. Nothing contained herein applies to software purchased by Gapblue employees at their own expense.

5.4 File Transfer Protocol (FTP)

Files may be transferred to secure FTP sites using appropriate security precautions. Requests for any FTP transfers should be directed to the IT officer or appropriate personnel.

5.5 Secure Socket Layer (SSL) Web Interface

Any EHR hosted (ASP) system, if applicable, will require access to a secure SSL website. Any such access must be requested using the Network Access Request Form and have appropriate approval from the manager or department head as well as the IT officer or appropriate personnel before any access is granted.

6 Building Security

It is the policy of Gapblue to provide building access securely. Each site, if applicable, is unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, Gapblue strives to continuously upgrade and expand its security and to enhance the protection of its assets and medical information that has been entrusted to it. The following list identifies measures that are in effect at the Gapblue. All other facilities, if applicable, have similar security appropriate for that location.

- Entrance to the building during non-working hours is controlled by a fingerprint and facial recognition system. Attempted entrance without this code results in immediate notification to the security department.

- The door to the reception area is always locked and requires appropriate credentials or escort past the reception or waiting for area door(s).
- The reception area is always staffed during the working hours of 9:00 AM to 5:00 PM.
- 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 and be accompanied by a Gapblue staff member. In some situations, non-Gapblue personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times.
- Swipe cards control access to all other doors. Each card is coded to allow admission to specific areas based on each individual's job function or need to know.
- 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 day 365-day yearly basis.
- Fire Protection: Use of local building codes will be observed. The manufacturer's recommendations on the fire protection of individual hardware will be followed.

7 Remote Work

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. Gapblue considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy applies to all employees and contractors who work either permanently or only occasionally outside of the Gapblue office environment. It applies to users who work from their home full time to employees on temporary travel, to users who work from a remote office location, and to any user who connects to the Gapblue network, if applicable, from a remote location.

While telecommuting can be an advantage for users and the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to Gapblue's network become an extension of the wide-area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate data to risks not present in the traditional work environment.

7.1 General Requirements

Telecommuting workers are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that apply to other employees/contractors.

- Need to Know: Telecommuting Users will have access based on the same 'need to know as they have when in the office.

- **Password Use:** The use of a strong password, changed at least every 90 days (about 3 months), is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- **Training:** Personnel who telecommute must complete the same annual training as all other employees.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

7.2 Required Equipment

Employees approved for telecommuting must understand that Gapblue will not provide all equipment necessary to ensure proper protection of information to which the employee has access; however, the following lists define the equipment and environment required:

Gapblue Provided:

Gapblue supplied workstation.

If printing, a Gapblue supplied printer.

If approved by your supervisor, a Gapblue supplied the phone.

Employee Provided:

Broadband connection and fees,

Paper shredder,

Secure office environment isolated from visitors and family.

A lockable file cabinet or safe to secure documents when away from the home office.

7.3 Hardware Security Protections

Virus Protection: Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all Gapblue personal computers and is set to update the virus pattern daily. This update is critical to the security of all data and must be allowed to complete.

VPN and Firewall Use: Established procedures must be rigidly followed when accessing Gapblue information of any type. Gapblue requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is a reason for termination.

Security Locks: Use security cable locks for laptops at all times, even at home or the office. Cable locks have been demonstrated as effective in thwarting robberies.

Lock Screens: No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected by HIPAA or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 15 minutes of inactivity.

7.4 Data Security Protection

Data Backup: Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established, or if you have external media that is not encrypted, contact the appropriate Gapblue personnel for assistance. Protect external media by keeping it in your possession when travelling.

Transferring Data to the Gapblue: Transferring data to the Gapblue requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your method, when transferring data to the Gapblue.

External System Access: If you require access to an external system, contact your manager or department head. IT officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the IT officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-Gapblue Networks: Extreme care must be taken when connecting Gapblue equipment to a home or hotel network. Although Gapblue actively monitors its security status and maintains organization-wide protection policies to protect the data within all contracts, Gapblue cannot monitor or control the security procedures on non-Gapblue networks.

Protect Data in Your Possession: View or access only the information that you need to see to complete your work assignment. Store electronic data only in encrypted workspaces. If your laptop has not been set up with an encrypted workspace, contact the IT officer or appropriate personnel for assistance.

Hard Copy Reports or Work Papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks that require the use of sensitive corporate or client level information when you are in a public area, i.e., airports, aeroplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside the Gapblue: All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any client-level information to anyone outside the Gapblue without the written approval of your supervisor.

7.5 Disposal of Paper and/or External Media

Shredding: All paper that contains sensitive information that is no longer needed must be shredded before being disposed of. Do not place in a trash container without first shredding. All employees working from home, or another non-Gapblue work environment, MUST have direct access to a shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed by IT compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your manager.
- External media must be wiped clean of all data. The IT Officer or appropriate personnel has very definitive procedures for doing this – so all external media must be sent to them.
- The last step in this process is to forward the media for disposal by a certified destruction agency.

8 Specific Protocols and Devices

8.1 Wireless Usage Standards and Policy

Due to the emergence of wireless access points in hotels, airports, and homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for Gapblue employees. This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of Gapblue laptops and mobile devices.

Approval Procedure - To be granted the ability to utilize the wireless network interface on your Gapblue laptop or mobile device you will be required to gain the approval of your immediate manager or department head and the IT Officer or appropriate personnel of the Gapblue. The Network Access Request Form (found in Appendix A) is used to make such a request. Once this form is completed and approved you will be contacted by the appropriate Gapblue personnel to set up your laptop and schedule training.

Software Requirements - The following is a list of minimum software requirements for any Gapblue laptop that is granted the privilege to use wireless access:

- Windows 10 or higher
- Mac OS 11.6 or higher

- Antivirus software
- Full Disk Encryption
- Appropriate VPN Client, if applicable

If your laptop does not have all of these software components, please notify your manager or department head so these components can be installed.

Training Requirements - Once you have gained approval for wireless access on your Gapblue computer, you will be required to attend a usage and security training session to be provided by the IT Officer or appropriate personnel. This training session will cover the basics of connecting to wireless networks, securing your computer when connected to a wireless network, and the proper method for disconnecting from wireless networks. This training will be conducted within a reasonable period once wireless access approval has been granted, and in most cases will include several individuals at once

8.2 Use of Transportable Media

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB devices.

The purpose of this policy is to guide employees/contractors of Gapblue in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Gapblue networks. Every workstation or server that has been used by either Gapblue employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore, procedures must be carefully followed when copying data to or from transportable media to protect sensitive Gapblue data. Since transportable media, by their very design, are easily lost, care and protection of these devices must be addressed. Since transportable media will likely be provided to a Gapblue employee by an external source for the exchange of information, all employees must have guidance in the appropriate use of media from other companies.

Rules governing the use of transportable media include:

- No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB devices used to store Gapblue data or sensitive data must be encrypted with USB keys issued by the IT Officer or appropriate personnel. The use of a personal USB device is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by Gapblue.
- Non-Gapblue workstations and laptops may not have the same security protection standards required by the Gapblue, and accordingly, virus patterns could potentially be transferred from the non-Gapblue device to the media and then back to the Gapblue workstation.

Example: Do not copy a working spreadsheet to your USB device and take it home to work on your home PC.

- Data may be exchanged between Gapblue workstations/networks and workstations used within Gapblue. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

  Examples of necessary data exchange include:

  Data was provided to auditors via USB key during the course of the audit.

- It is permissible to connect transferable media from other businesses or individuals into Gapblue workstations or servers if the source of the media is on the Gapblue Approved Vendor list (Appendix D).
- Before initial use and before any *sensitive data* may be transferred to transportable media, the media must be sent to the IT Officer or appropriate personnel to ensure appropriate and approved encryption is used. Copy *sensitive data* only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.
- Report all loss of transportable media to your manager or department head. The CST team must be notified either directly from the employee or contractor or by the manager or department head immediately.
- When an employee leaves the Gapblue, all transportable media in their possession must be returned to the IT officer or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

Gapblue utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The IT officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all Gapblue laptops, workstations, or servers must be wiped of data. All transportable media must be wiped according to the set standards. Thus, all transportable media must be returned to the IT officer or appropriate personnel for data erasure when no longer in use.

9 Change Management

Statement of Policy

To ensure that Gapblue is tracking changes to networks, systems, and workstations including software releases and updates. Change tracking allows the Information Technology (“IT”) Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Procedure

1. The IT staff or other designated Gapblue employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
    a. When changes are tracked within a system, i.e., Windows updates in the Add or Remove Programs component or elect any updates performed and logged by the vendor, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are performed before the change.
3. The employee implementing the change shall also be familiar with the rollback process if the change causes an adverse effect within the system and needs to be removed.

10 Audit Controls

Statement of Policy

To ensure that Gapblue implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain electronically protected health information ("ePHI"). Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

Gapblue is committed to routinely auditing users' activities to continually assess potential risks and vulnerabilities to the network.

Procedure

1. The Information Technology Services shall enable event auditing on all computers that process, transmit, and/or store information to generate audit logs. Each audit log shall include, at a minimum: user ID, login time and date, and scope of client data being accessed for each attempted access. Audit trails shall be stored on a separate computer system to minimize the impact of such auditing on business operations and to minimize access to audit trails.

2. Gapblue utilizes appropriate network-based and host-based intrusion detection systems. The Information Technology Services shall be responsible for installing, maintaining, and updating such systems.

11 Information System Activity Review

Statement of Policy

To establish the process for conducting, periodically, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. Gapblue shall regularly conduct an internal review of records of system activity to minimize security violations.

Procedure

1. The Information Technology Services shall be responsible for conducting reviews of Gapblue's information systems' activities. Such a person(s) shall have the appropriate technical skills concerning the operating system and applications to access and interpret audit logs and related information appropriately.
2. The Security Officer shall develop a report format to capture the review findings. Such a report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such a report shall be in a checklist format.
3. Such reviews shall be conducted annually. Audits also shall be conducted if Gapblue has reason to suspect wrongdoing. In conducting these reviews, the Information Technology Services shall examine audit logs for security-significant events including, but not limited to, the following:
    a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
    b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.
    c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.

d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems have such access to the information and/or system.

12 Data Integrity

Statement of Policy

Gapblue shall implement and maintain appropriate electronic mechanisms to corroborate that any information has not been altered or destroyed in an unauthorized manner.

The purpose of this policy is to protect Gapblue's data from improper alteration or destruction.

Procedure

To the fullest extent possible, Gapblue shall utilize applications with built-in intelligence that automatically checks for human errors.

Gapblue shall acquire appropriate network-based and host-based intrusion detection systems. The Security Officer shall be responsible for installing, maintaining, and updating such systems.

To prevent transmission errors as data passes from one computer to another, Gapblue will use encryption, as determined to be appropriate, to preserve the integrity of data.

Gapblue will check for possible duplication of data in its computer systems to prevent poor data integration between different computer systems.

To prevent programming or software bugs, Gapblue will test its information systems for accuracy and functionality before it starts to use them. Gapblue will update its systems when IT vendors release fixes to address known bugs or problems.

1. Gapblue will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.

13 Security Awareness and Training

Statement of Policy

To establish a security awareness and training program for all members of Gapblue's workforce, including management.

Information Security Policy

All workforce members shall receive appropriate training concerning Gapblue's security policies and procedures. Such training shall be provided before joining and on an ongoing basis for all new employees. Such training shall be repeated annually for all employees.

Procedure

a. Security Training Program

   i. The Security Officer shall have responsibility for the development and delivery of initial security training. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation of all training activities.

b. Security Reminders

   i. The Security Officer shall generate and distribute to all workforce members routine security reminders regularly. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, promotional items such as coffee mugs, mousepads, sticky notes, etc. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.
   ii. The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

c. Protection from Malicious Software

   i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training should include the following:

      a) Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail,

      b) The importance of updating anti-virus software and how to check a workstation or other device to determine if the virus protection is current,

      c) Instructions to never download files from unknown or suspicious sources,

      d) Recognizing signs of a potential virus that could sneak past antivirus software or could arrive before an update to anti-virus software,

e) The importance of backing up critical data regularly and storing the data in a safe place,

f) Damage caused by viruses and worms, and

g) What to do if a virus or worm is detected.

d. Password Management

i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords:

a) Passwords must be changed every 90 days (about 3 months).

b) A user cannot reuse the last 12 passwords.

c) Passwords must be at least eight characters and contain upper case letters, lower case letters, numbers, and special characters.

d) Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.

e) A password must be promptly changed if it is suspected of being disclosed or known to have been disclosed.

f) Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to "fix" a computer or handle an emergency or individuals, including family members.

g) Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

h) Employees should refuse all offers by software and/or Internet sites to automatically log in the next time that they access those resources.

i) Any employee who is directed by the Security Officer to change his/her password to conform to the aforementioned standards shall do so immediately.

Information Security Policy

14 Security Management Process

Statement of Policy

To ensure Gapblue conducts an accurate and thorough assessment of the potential risks and vulnerabilities to confidentiality, and integrity.

Gapblue shall conduct an accurate and thorough risk analysis to serve as the basis for Gapblue's Security Rule compliance efforts. Gapblue shall re-assess the security risks and evaluate the effectiveness of its security measures and safeguards as necessary considering changes to business and technological advancements.

Procedure

a. The Security Officer shall be responsible for coordinating Gapblue's risk analysis. The Security Officer shall identify appropriate people within the organization to assist with the risk analysis.

b. The risk analysis shall proceed in the following manner:

i. Document Gapblue's current information systems.

a) Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired, location, vendor, licenses, maintenance schedule, and function. Update/develop network diagram illustrating how the organization's information system network is configured.

b) Update/develop facility layout showing location of all information systems equipment, power sources, telephone jacks, and other telecommunications equipment, network access points, fire and burglary alarm equipment, and storage for hazardous materials.

c) For each application identified, identify each licensee (*i.e.,* authorized user) by job title and describe how authorization is granted.

d) For each application identified:

i) Describe the data associated with that application.

ii) Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.

iii) Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.

iv) Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for some time.

v) Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.

vi) For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.

e) Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of ePHI created, received, maintained, or transmitted by Gapblue. Consider the following:

i) Natural threats, e.g., earthquakes, storm damage.

ii) Environmental threats, e.g., fire and smoke damage, power outage, utility problems.

iii) Human threats

a. Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls

b. Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment

c. Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, extortion

d. External attacks, e.g., malicious cracking, scanning, demon dialing, virus introduction

iv) Identify and document vulnerabilities in Gapblue's information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally

exploited, resulting in unauthorized access to ePHI, modification of ePHI, denial of service, or repudiation (*i.e.,* the inability to identify the source and hold some person accountable for an action). To accomplish this task, conduct a self-analysis utilizing the standards and implementation specifications to identify vulnerabilities.

15 Sanction Policy

Policy

It is the policy of Gapblue that all workforce members must protect the confidentiality, integrity, and availability of sensitive information always. Gapblue will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.

Gapblue will take appropriate disciplinary action against employees, contractors, or any individuals who violate Gapblue's information security and IT policies or state, or federal confidentiality laws or regulations.

Purpose

To ensure that there are appropriate sanctions that will be applied to workforce members who violate Gapblue's security policies, Directives, and/or any other state or federal regulatory requirements.

Violations

Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation

Level	Description of Violation
1	• Accessing information that you do not need to know to do your job. • Sharing computer access codes (username & password). • Leaving computer unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area

Level	Description of Violation
	or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the Information Security Officer, IT Officer, Chief Information Officer, and/or authorized designee.
2	• Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (username & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	• Third occurrence of any Level 1 offense (does not have to be the same offense). • Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

16 Employee Background Checks

The Gapblue may conduct employment reference checks, investigative consumer reports, and background investigations on all candidates for employment before making a final offer of employment and may use a third party to conduct these background checks. Gapblue will obtain written consent from applicants and employees before ordering reports from third-party providers and will provide a description of applicant and employee rights and all other documentation as required by law to each applicant.

An investigative consumer report compiles information on a candidate's general reputation, personal characteristics, or mode of living. This information may be gathered online including social networking sites, through public or educational records, or through interviews with employers, friends, neighbors, associates, or anyone else who may have information about the employee or potential employee. In the

pre-employment process, investigative consumer reports typically include such things as criminal records checks, education verification checks, and employment verification checks.

The type of information that will be collected by Gapblue in background checks may include, but is not limited to, some or all the following:

- Private and government agency reports related to any history of criminal, dishonest, or violent behavior, and other reports that relate to the suitability for employment
- Education (including degrees awarded and GPA)
- Employment history, abilities, and reasons for termination of employment
- Professional licensing board reports
- Address history
- Civil court filings
- Motor vehicle and driving records
- Professional or personal references

17 Compliance and Enforcement

All managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to discipline up to and including termination under Gapblue's Sanction Policy.

End of Document