Policy and Procedure Document

Information Security

Business Information Systems
333 Industrial Park Road
Piney Flats, TN 37686

5/31/2018
v1.0

Table of Contents

Revisions

Revision	Description of Change	Author	Effective Date
v1.0	Initial Document Creation	Wendell Dingus	05/31/2018

1 Introduction

1.1 Purpose

This policy defines the technical controls and security configurations Business Information Systems (BIS) team members and Information Technology (IT) administrators are required to implement to ensure the integrity and availability of the data environment at BIS. It serves as a central policy document with which all employees and contractors must be familiar with and defines actions and prohibitions that everyone must follow. This policy provides details concerning the acceptable use of BIS technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to hosted environments, 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 virtual, hardware, software, and data transmission mechanisms. This policy must be adhered to by all BIS employees or temporary workers at all locations and by contractors working with BIS as subcontractors.

BIS' Security Program is considered a business-critical function. BIS includes appropriate funding into its yearly budget to ensure that all security requirements are met, this includes funding the overall security program, any compliance and audit initiatives, and appropriate staffing. BIS commits to ensuring all security resources, be they hardware, software or individuals are available for expenditure as planned and detailed in appropriate BIS budgeting documentation.

This policy will be reviewed, updated and approved by BIS executive management no less than annually.

1.2 Scope

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

1.3 Applicable Statutes / Regulations

The following is a list of the various agencies/organizations whose laws, mandates, frameworks and regulations were incorporated into the various policy statements included in this document.

Service Organization Controls (SOC 2)
PCI-DSS 3.2

Each of the policies defined in this document is applicable to the task being performed – not just to specific departments or job titles.

1.4 Security and Privacy Officer

BIS has established a Security Officer and Privacy Officer as required by laws, regulatory agencies and organizations. The Security Officer will oversee all ongoing activities related to the development, implementation, and maintenance of BIS' security policies, processes and controls in accordance with applicable laws, frameworks and regulations. The Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of BIS privacy policies in accordance with applicable laws and regulations.

The current Officer's for BIS are: Wendell Dingus (both roles)

1.5 Confidentiality / Security Team (CST)

BIS has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within BIS and act as the first line of defense in enhancing the appropriate security posture.

All members identified within this policy are approved to their positions by the Chief Information Officer. This team will consist of the positions within BIS most responsible for the overall security policy planning of the organization.

The current members of the CST are: Wendell Dingus, Scott Bigliardi

The CST will meet monthly to discuss security issues and to review concerns that arose during the month. The CST will identify areas that should be addressed and review/update security policies as necessary.

The CST will address security issues as they arise and recommend and approve immediate security actions to be undertaken. It is the responsibility of the CST to identify areas of concern within BIS and act as the first line of defense in enhancing the security posture of BIS.

The CST is responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the meetings.

The Security Officer (SO), Privacy Officer (PO) or other assigned personnel is responsible for maintaining a log of security enhancements and features that have been implemented to further protect all sensitive information and assets held by BIS. This log will also be reviewed during the monthly meetings.

2 Employee Responsibilities

2.1 Employee Requirements

The first line of defense in data security is the individual BIS team member. All team members are responsible for the security of all data which may come to them in whatever format. The Security Officer is responsible for maintaining ongoing training programs to inform all team members of these requirements.

Identity and Access Badge **-** To help maintain building security, all employees must maintain possession of their employee identification badge when in BIS' facilities. Badges must not be left unattended in open areas including the employees desk. Contractors who may be in BIS' facilities are provided with temporary identification badges. Other people who may be within BIS facilities must wear visitor badges and should be chaperoned.

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

Unattended Computers **-** Unattended computers must be locked by the user when leaving the work area, even momentarily. BIS 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 BIS Corporate Assets - Only computer hardware and software owned by and installed by BIS is permitted to be connected to or installed on BIS equipment and networks. Only software that has been approved for corporate use by BIS may be installed on BIS equipment. Personal computers supplied by BIS 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 BIS.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of BIS are the property of BIS unless covered by a contractual agreement. Nothing contained herein applies to software purchased by BIS employees at their own expense.

2.2 Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Additional 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 as a result of 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 BIS Security Officer or Privacy 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. BIS has access to client information which is protected by laws, regulations and contracts which stipulate a "need to know" before approval is granted to view the information. 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 BIS computers must be approved.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by BIS 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 BIS is strictly prohibited.
- Request for Credit Card Information. At no point should you request or make note of the entire credit card number. At most you may ask for the last four digits of the card number, and it is strongly recommended that any other identifying data for a transaction be used if possible, for example a transaction ID or batch number. Asking for or making note of an entire credit card number is grounds for immediate disciplinary action up to and including termination of employment and legal action. If a customer attempts to communicate the credit card number to you then you should interrupt them and politely inform them that you are not allowed to take the entire number. The only exception to this rule is if your job description explicitly states that taking of credit card information is one of your responsibilities. The rules for handling that information will be covered elsewhere.

2.3 Electronic Communication, E-Mail, Internet Usage

As a productivity enhancement tool, BIS encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by BIS owned equipment are considered the property of BIS – not the property of individual users. Consequently, this policy applies to all BIS 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.

BIS provided resources, such as individual 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 BIS information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.

c) Commercial use – Use of BIS information resources for personal or commercial profit is strictly prohibited.

d) Political Activities – All political activities are strictly prohibited on BIS premises. BIS encourages all its employees to vote and to participate in the election process, but these activities must not be performed using BIS assets or resources.

e) Harassment – BIS strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, BIS 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 is strictly 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.

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. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is **NOT** the policy of BIS to monitor the content of any electronic communication, BIS is responsible for servicing and protecting BIS’ equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. BIS does keep a log of message sent and received which includes the date the message was sent/received and the origin and destination of the message – the message content is not logged unless a specific business and/or legal need to do so arises.

BIS 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 BIS 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.

2.4 Internet Access

Internet access is provided for BIS users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by BIS should not be used for entertainment such as viewing sports, playing games, watching movies, etc. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available for business use.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, sharing applications, have already been blocked by BIS routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

2.5 Reporting Software Malfunctions

Users must inform the appropriate BIS personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, BIS computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel or Security Officer as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.

- Do not attempt to remove a suspected virus!

The Security Officer will monitor the resolution of the malfunction or incident and report the result of the action with recommendations on action steps to avert future similar occurrences.

2.6 Report Security Incidents

It is the responsibility of each BIS employee and contractor to report confirmed or perceived security incidents to the Security Officer or Privacy Officer. Everyone is responsible for the day-to-day, hands-on security of BIS information resources. Users are to formally report all security incidents or violations of the security policy immediately to the Security Officer (SO) or Privacy Officer (PO).

Reports of security incidents shall be escalated as quickly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged, and the remedial action indicated. It is the responsibility of the SO and PO to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be immediately investigated. If criminal action is suspected, BIS SO and PO shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

2.7 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 in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by BIS and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of BIS policy and will result in personnel action, and may result in legal action.

2.8 Transferring Software and Files between Home and Work

Personal software shall not be used on BIS computers or networks. If a need for specific software exists, submit an IT request. Users shall not use BIS purchased software on home or on non-BIS computers or equipment.

BIS proprietary data, including but not limited to client information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of BIS without written consent of a member of executive management. It is crucial to BIS to protect all data and, in order to do that effectively we must control the systems in which it is contained.

BIS 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 BIS does not control non-BIS personal computers, BIS cannot be sure of the methods that may or may not be in place to protect BIS sensitive information, hence the need for this restriction.

2.9 Internet Considerations

Special precautions are required for Internet access to protect BIS when data is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

- Users shall not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to submit an IT request for approval;
- Use shall be consistent with the goals of BIS. The network can be used to market services related to BIS, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
- Client or PII data must not be transferred other than using approved processes such as SFTP. Transferring this data using email or other non-encrypted means without approval by Security Officer and/or Privacy Officer is prohibited.

2.10 De/Re-identification of Personally Identifiable Information (PII)

All personally identifying information should be de-identified from all data that falls within the definition of PII before it is stored or exchanged.

De-identification is defined as the removal of any information that may be used to identify an individual or of relatives, employers, or household members.

PII includes:

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- Electronic mail addresses
- Social security numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images

Re-identification of confidential information: A cross-reference code or other means of record identification is used to re-identify data as long as the code is not derived from or related to information about the individual and cannot be translated to identify the individual. In addition, the code is not disclosed for any other purpose nor is the mechanism for re-identification disclosed.

3 Identification and Authentication

3.1 User Logon IDs

Individual users shall have unique logon 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 individual logon ID.

All user login IDs are audited at least quarterly and all inactive logon IDs are revoked. BIS Human Resources Department notifies the Network Services department or appropriate personnel upon the departure of all employees and contractors, at which time login IDs are revoked.

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

Human Resources must complete an IT request for users to be setup with access to BIS' systems or networks.

3.2 Passwords

User Account Passwords
User IDs and passwords are required to gain access to all BIS networks, computer systems, and laptops. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. 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 at the server, computer, or laptop 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. Compromised passwords shall be changed immediately.

Reuse - The previous three (3) 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. Passwords are stored in an encrypted format.

3.3 Confidentiality Agreement

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

> *I agree that any unauthorized use or disclosure of information residing on BIS 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 prior to accessing BIS 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 Human Resources and the appropriate department head.

This guideline satisfies the "need to know" requirement regulation, since the supervisor or department head is the person who most closely recognizes an employee's need to access data. Users may be added to the information system, network, etc. **only** upon the approval of the Security Officer, Privacy Officer or appropriate personnel who are responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited and that violators will be subject to criminal prosecution.

3.5 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.

3.6 User Login Entitlement Reviews

If an employee changes positions at BIS, employee's new supervisor or department head shall promptly notify the Information Technology ("IT") Department of the change of roles and indicate 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 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 adding the roles and access necessary for their new job responsibilities.

No less than quarterly, the Security Officer or Privacy Officer shall facilitate entitlement reviews on the BIS platform 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 compliance and protect data.

3.7 Termination of User Logon Account

Upon termination of an employee, whether voluntary or involuntary, Human Resources, the employee's supervisor or department head shall promptly notify the IT Department. If employee's termination is voluntary and employee provides notice, employee's supervisor or department head shall promptly notify the IT Department of employee's last scheduled work day so that their user account(s) can be configured to expire. The employee's department head shall be responsible for insuring that all keys, ID badges, and other access devices as well as BIS equipment and property is returned to BIS prior to the employee leaving BIS on their final day of employment.

4 Network Connectivity

4.1 Inbound Network Connections

Systems that allow public access to host computers, including mission-critical servers, warrants additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Access privileges are granted only upon the request of a department head and the approval of the Security Officer, Privacy Officer or appropriate personnel.

4.2 Outbound Network Connections

BIS provides a link to an Internet Service Provider**.** If a user has a specific need to link with an outside computer or network through a direct link, approval must be obtained from the Security Officer, Privacy Officer or appropriate personnel. The appropriate personnel will ensure adequate security measures are in place.

4.3 Permanent Connections

The security of BIS' systems can be jeopardized from third party locations if security practices and 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 BIS' systems. The Security Officer, Privacy Officer or appropriate personnel should be involved in the process, design and approval.

4.4 Emphasis on Security in Third Party Contracts

Access to BIS 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 BIS Information Security Policy have been reviewed and considered.
- Policies and standards established in BIS 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.
- Arrangements for reporting and investigating security incidents must be included in the agreement.
- A description of each service 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 list of users with access to BIS 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 protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- 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 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.

- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorize users who will need 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.
- Because annual confidentiality training is required, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
- 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.

4.5 Firewalls

Authority from the Security Officer or Privacy Officer or appropriate personnel must be received before any employee or contractor is granted access to a BIS router or firewall.

5 Malicious Code

5.1 Antivirus Software Installation

Antivirus software must be installed on all BIS computers, laptops, and servers with virus update patterns updated at least daily. Antivirus software must not be uninstalled, disabled or reconfigured in any way without approval by the Security Officer or Privacy Officer.

Configuration **-** Through an automated procedure, antivirus software updates and patches are installed as they are released and signatures are updated daily.

Monitoring/Reporting – A record of virus patterns for all computers and servers are maintained. The Security Officer and Privacy Officer are responsible for reviewing reports for auditing.

5.2 New Software Distribution

Only software created by BIS application staff, if applicable, or software approved by the Security Officer, Privacy Officer or appropriate personnel will be used on internal computers and networks. All new software may be tested by appropriate personnel to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks.

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 Security Officer, Privacy Officer, Legal or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on BIS computers and networks. These precautions include determining that the software does not interfere with or damage BIS 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 BIS computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate BIS personnel for instructions for scanning files for viruses.

Every CD-ROM, DVD and USB device is a potential source for a computer virus, therefore, must be scanned for virus infection prior to copying information to a BIS computer or network.

Computers shall never be “booted” from a CD-ROM, DVD or USB device received from an outside source. A CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the CD_ROM, DVD or USB device is not “bootable”.

5.3 Retention of Ownership

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

6 Encryption

6.1 Definition

Encryption is the translation of data into a secret code. Encryption is a very effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.

6.2 Using Encryption

If justified by risk analysis, confidential data and files shall be encrypted before being transmitted through networks.

Encryption requires the user to provide a key as input. An encryption key specifies the transformation of plain text into cipher text, or vice versa during decryption.

When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, BIS shall establish the criteria in conjunction with the Security Officer, Privacy Officer or appropriate personnel. BIS employs several methods of secure data transmission.

6.3 SSH File Transfer Protocol (SFTP)

Files may be transferred to secure SFTP sites using appropriate security precautions. Requests for any SFTP transfers should be directed to the Security Officer or Privacy Officer or appropriate personnel.

6.4 Securing client and PII data

Any system transmitting confidential information including client data and/or PII data will require the use of SSL with a modern encryption algorithm.

Any system storing confidential information including client data and/or PII data will require the use of encrypting with a modern encryption algorithm.

7 Building Security

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

BIS Main Campus:

- Entrance to the building during non-working hours is controlled by a badge and conditional access system. Attempted entrance without this badge and access key results in immediate notification to law enforcement.
- Disclosure of any security code to non-employees is strictly prohibited.
- Conditional access keys are removed upon termination of employees that had access.
- Conditional access keys are disabled if lost, stolen, or not returned upon termination.
- The reception area is staffed during the working hours of 8:00 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 BIS staff member. In some situations, non-BIS personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times.
- BIS identification badges control access to doors. Each card is coded to allow admission to specific areas based on each individual's job function or need to know.
- Motion detection sensors are activated after hours. Any movement within the building will result in immediate notification to law enforcement.
- Fire Protection: Use of local building codes will be managed by building owner and observed by BIS as required. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

8 Remote Access and Telecommuting

BIS considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of BIS office environment. It applies to users who work from their home temporarily, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to BIS network and/or managed systems, if applicable, from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to BIS' 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 as well as client data to risks not present in the traditional work environment.

8.1 General Requirements

Telecommuting workers are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that are applicable 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 as per policy, is even more critical in the telecommuting environment. Do not share your password or write it down.
- **Training:** Personnel who telecommute must complete the same annual privacy training as all other employees.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

8.2 Required Equipment

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

Company Provided:
BIS supplied laptop.

Employee Provided:
Broadband connection.

8.3 Hardware Security Protections

Virus Protection**:** Users must never stop the update process for Virus Protection. Virus Protection software is installed on all BIS computers and is set to update the virus pattern on at least a daily basis. 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 BIS information of any type. BIS requires the use of VPN software and an application firewall. Disabling a virus scanner or firewall is reason for termination.

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 privacy regulations or may contain confidential information. An automatic lock feature has been set to turn on after 2 minutes of inactivity.

Remote Access Sessions: Always disconnect remote access sessions when not in use, the connection may provide access to data protected by privacy regulations or may contain confidential information. An automatic disconnect feature has been set to close inactive sessions after 30 minutes.

8.4 Data Security Protection

Data Backup**:** Encrypted backup and retention procedures have been established for all data. 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 personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to BIS**:** Transferring of data to BIS requires the use of an approved method (i.e. SFTP) to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to BIS.

External System Access: If you require access to an external system, contact the Security Officer, Privacy Officer or appropriate personnel to assist in establishing a secure method of access.

E-mail: Do not send any client data or individual-identifiable information (PII) via e-mail. If you need assistance, contact the Security Officer, Privacy Officer or appropriate personnel to ensure an approved mechanism is used for transmission.

Non-Company Networks: Extreme care must be taken when connecting BIS equipment to a home or hotel network. Although BIS actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, BIS has no ability to monitor or control the security procedures on non-BIS networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Ensure that your workstation is never left unlocked when unattended, and use a privacy screen where possible.

Hard Copy Reports or Work Papers: Never leave confidential paper records around your work area. Lock all confidential 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 which require the use of confidential corporate or client level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

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

Storage of Covered Information (PII): Covered information must only be permanently stored in a BIS production database instance hosted within our data center or one of our hosting partners. Covered information must never be used or made available in lower environments, such as development and QA.

8.5 Disposal of Paper and/or External Media

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

Disposal of Electronic Media: All external media containing sensitive data must be sanitized or destroyed in accordance with BIS compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to the appropriate personnel.
- External media must be wiped clean of all data. The Security Officer, Privacy Officer or appropriate personnel has very definitive procedures for doing this – so all external media must be sent to them.

9 Specific Protocols and Devices

9.1 Wireless Usage Standards and Policy

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

BIS Wireless Network **–** Only approved BIS managed and controlled devices are allowed to access the BIS network. Due to the inability to ensure the security of personal devices, BYOD (Bring Your Own Device) is prohibited from accessing any BIS network.

Public Wi-Fi **–** Public Wi-Fi is inherently open to security threats. Follow these tips for staying safe on public Wi-Fi:

- Check the authenticity – Ask the Wi-Fi owner of the correct network name and password.
- Use a VPN
- Look for HTTPS – Ensure the web pages you visit are https encrypted where possible.
- Avoid accessing sensitive information
- Manually select Wi-Fi networks – Do not automatically connect to public Wi-Fi networks

9.2 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 or contractors of BIS in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from BIS networks. Every workstation or server that has been used by either BIS 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 company data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a BIS employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is common practice within BIS. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of BIS networks. Transportable media received from an external source could potentially pose a threat to BIS networks. ***Sensitive data*** includes but is not limited to all human resource data, financial data, and BIS proprietary information.

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected. They now come in rugged formats which connects to a key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No ***sensitive (confidential or secret) data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB keys used to store BIS data or sensitive data must be an encrypted USB key issued by the Security Officer, Privacy Officer or appropriate personnel. The use of a personal USB key is strictly prohibited.

- Users must never connect their company provided transportable media to a workstation that is not issued by BIS.
- Non-company workstations and laptops may not have the same security protection standards required by BIS, and accordingly virus patterns could potentially be transferred from the non-company device to the media and then back to BIS laptop.

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

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

  - Exmaple: Data 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 BIS workstations or servers as long as the source of the media in on BIS 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 Privacy 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 supervisor or department head. It is important that the CST team is notified either directly from the employee or contractor or by the supervisor or department head immediately.
- When an employee leaves BIS, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

BIS utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Security Officer, Privacy Officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all BIS laptops, workstations, or servers must be wiped of data in a manner which conforms to NIST guidelines. All transportable media must be wiped according to the same standards. Thus, all transportable media must be returned to the Security Officer, Privacy Officer or appropriate personnel for data erasure when no longer in use.

10 Router/Firewall Configuration and Review

10.1 Policy Statement

Where Electronic Equipment is used to capture, process or store data identified as “Confidential” and the Electronic Equipment is accessible via a direct or indirect Internet connection, a Network Firewall appropriately installed, configured and maintained is **required**.

All installations and implementations of and modifications to a Network Firewall and its Configuration and Ruleset are the responsibility of the CIO and/or their designates.

Where Electronic Equipment is used to capture, process or store data identified as “Confidential” and the Electronic Equipment is accessible via an Internet connection, a Host Firewall appropriately installed, configured and maintained is **required** where the operating environment supports that installation. The maintenance of the Host Firewall’s Configuration and Ruleset is the responsibility of that system’s administrator.

Where Electronic Equipment is used to capture, process or store data identified as “Internal” or “Public” and the Electronic Equipment is accessible via an Internet connection, a Host and/or Network Firewall is **recommended**.

Use of a Host Firewall is **recommended** for any individual Host with access to the Internet; its maintenance is the responsibility of the individual user or designated support personnel.

In order to verify that there are no undocumented openings to the Internet, a bi-annually review of the firewall rule set will be performed.

10.2 Procedures

Configuration and management

1. All Firewall implementations should adopt the principal of “least privilege” and deny all inbound traffic by default. The Ruleset should be opened incrementally to only allow permissible traffic.
2. Firewalls must be installed within production environments where “Confidential Information” is captured, processed or stored, to help achieve functional separation between web-servers, application servers and database servers.
3. Firewall Rulesets and Configurations require biannual periodic review to ensure they afford the desired levels of protection.
4. Firewall Rulesets and Configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained in order to preserve the integrity of the data, should restoration be required. Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.
5. Network Firewall administration logs (showing administrative activities) and event logs (showing traffic activity) are to be written to alternate storage (not on the same device) and reviewed regularly. It is recommended that utilities or programs that facilitate the review process be employed. Appropriate access to logs and copies is permitted to those responsible for Firewall and/or system maintenance, support and review.
6. Firewall Administrators will execute approved changes to the Firewall Rulesets as defined by Change Mangement Policy/Procedure.
7. Firewall Administrators will perform changes to Firewall Configurations according to approved production maintenance schedules.

Review

1. Validate that all firewall rules are still applicable.
2. Identify if there are changes since the last review period. For any change:

a) Review that there is a documented business reason for the change(s).
b) Review that the changes were authorized and approved by the Security Officer.

3. Follow the change control process to request changes to the firewall rules for rules no longer needed.
4. Record the completion of the review. Include date, person completing the review, list of firewalls reviewed and supporting documentation.

11 Retention / Destruction of Information

Many laws regulate the retention and destruction of different types of information. BIS actively conforms to these laws and follows the strictest regulation if/when a conflict occurs.

Covered Data Storage - Covered data must only be stored in a BIS production database, and must use an industry standard encryption algorithm, such as AES256. Covered data storage must be kept to a minimum.

Data Retention / Destruction – BIS production data is retained for the term of the contract and promptly deleted after the end of term or at client request. Data stored in backups is retained for 365 days as part of the backup cycle.

Record Retention - Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information practice, responses to amend or correct their information, and a complaint record are maintained for a period of 6 years.

Record Destruction - All hardcopy records that require destruction are shredded using NIST guidelines.

12 Disposal of External Media / Hardware

12.1 Disposal of External Media

It must be assumed that any external media in the possession of an employee is likely to contain sensitive information. Accordingly, external media (CD-ROMs, DVDs, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
- External media should never be thrown in the trash.
- When no longer needed all forms of external media are to be sent to the Service Department or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 g

12.2 Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

12.3 Disposition of Excess Equipment

As the older BIS computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.

12.4 Definition of Storage Media

Storage Media shall be defined as any device which holds electronic data. Examples include but may not be limited to hard disk drives, CD-ROMs, DVDs, floppy disk drives and flash storage devices. The media may be fully or partially written. Storage media may be from a client's office or from internal sources at the BIS offices. Storage media may already be encrypted but that fact will not alter the steps we take to securely dispose of that media.

12.5 Two Categories of Storage Media

Re-Usable Storage Media
We define storage media as "re-usable" if it is in working condition, regardless of whether we actually intend to use it. If we intend to re-use the media then follow only Method 1. If we intend to sell or donate while it is in working condition then follow only Method 1. If we intend to recycle or otherwise dispose of the media then follow both Method 1 and Method 2. The technician must also print, fill out and sign the Certificate of Destruction (Appendix A). This certificate shall be given to the technician's supervisor once completed. The supervisor will scan the document and attach it to the CRM ticket pertaining to the device in question.

Unusable Storage Media
We define storage media as "unusable" if it is not in a working state or cannot be brought into a working state. Unusable storage media should be processed using Method 2.

12.6 Methods for Securely Removing Access to Data on Storage Media

Method 1: Overwrite the Data
Use a software product to securely overwrite the media with random data. Linux and Windows have native solutions. Third-party solutions are also available.

Method 2: Destroy the Media
Proper precautions and safety gear must be utilized when destroying storage media.

Hard disk drives: using a hammer and punch tool, multiple holes shall be punched through the body and platters or solid state storage component of the drive.
Flash Storage Drives: the solid state component of the drive will be smashed with a hammer.
Optical Disks: using a metal tool the data-bearing surfaces of the disk will be thoroughly scratched, then the disk will be snapped into more than one piece.
Floppy Disks: the magnetic film will be removed the body of the disk then cut into multiple pieces

12.7 Storage of Media until Time of Disposal or Re-Use

Before and during processing, re-usable media will be stored inside a locked area of the Service department. After processing, re-usable media will be returned to and checked into Inventory. Before, during and after processing, unusable media will be stored inside a locked area of the Service or Inventory departments until such time as it is sold, recycled or otherwise properly disposed of.

12.8 Steps to Follow When Disposing of Media

Proper maintenance of a chain of custody of the storage media is required, from the first decision to securely remove the data, to the receipt of the device by the technician who will handle the device, to the final step in the process whether that is placement on the shelf in Inventory or dropping it off at a recycling center. The steps outlined below must be followed.

When a storage device has been deemed in need of secure removal of data the Service Department Manager or their authorized delegate will create a CRM ticket for the device. The subject or title of the CRM ticket should follow this format: Secure Disposal of Storage Media – DEVICE TYPE. Examples:

- Secure Disposal of Storage Media – Hard Disk Drive
- Secure Disposal of Storage Media – Removable Flash Drive
- Secure Disposal of Storage Media – CD-ROM

The CRM ticket details should include the following when the ticket is created:

- User's name
- BIS serial number, if available
- Manufacturer's serial number, if available
- Device storage capacity
- Date of receipt of the device
- Description of the decision made for the disposition of the device. Examples:
    - "Service tech John Doe ran tests on this hard disk drive and determined that it is in an unusable condition. This device must be destroyed."

- "This hard disk drive was pulled from an unusable PC returned from customer X but the hard disk drive is in usable condition. We will securely remove the data and return the device to inventory."
- "This hard disk drive is in usable condition but is too small to be used in future operations. We will securely remove the data and return it to Inventory where they will attempt to sell the device."

At each step of the processing of this device the technician who completes the step will add a note the CRM ticket detailing what was done to the device.

13 Change Management

13.1 Statement of Policy

To ensure that BIS is tracking changes to networks, systems, and applications including software releases and software vulnerability patching in information systems. Change tracking allows teams to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

13.2 Procedure

- The DevOps, IT or other designated BIS staff who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
- The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
- The employee implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

14 Audit Controls

14.1 Policy

To ensure that BIS implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems. 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.

BIS is committed to routinely auditing users' activities to continually assess potential risks and vulnerabilities. As such, BIS will continually assess potential risks and vulnerabilities and develop, implement, and maintain appropriate administrative, physical, and technical security measures.

14.2 Procedure

- See policy below entitled Information System Activity Review for the administrative safeguards for auditing system activities.
- The DevOps Team or Information Technology Team shall enable event auditing on all computers that process, transmit, and/or store confidential information including PII for purposes of generating audit logs and meeting legal requirements relating to the monitoring of both authorized and unauthorized access. Each audit log shall include, at a minimum: user ID, login time and date, program or command used to access data, source and destination addresses, and scope of 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.
- BIS shall utilize appropriate automated network-based and host-based intrusion detection systems to monitor both inbound and outbound connections, and tools to perform file integrity monitoring. The DevOps Team or Information Technology Team shall be responsible for installing, maintaining, and updating such systems.
- Audit records will be retained for 90 days and older records will be archived for at least 365 days. Audit records can be automatically processed for events of interest based on selective criteria.
- BIS shall monitor systems to identify any irregularities or anomalies that are indicators of a potential system malfunction or compromise while helping to confirm all systems are operating in their optimal, secure state.
- BIS ensures that appropriate alerts are generated for DevOps or Information Technology teams to investigate any suspicious activity or suspected policy violations.
- BIS shall analyze and correlate audit logs across different repositories using a centralized SIEM (Security Information and Event Management) tool for log consolidation from multiple hosts. BIS shall use this tool to devise profiles of common events to reduce 'white-noise' false positives and enable the DevOps and Information Technology teams to focus on unusual activity rather than insignificant alerts.

15 Information System Activity Review

15.1 Policy

To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, management activities, system and application startup/shutdown/errors, file access, security incidents, audit logs, access reports and Internet activity. BIS shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

15.2 Procedure

- See policy above entitled Audit Controls for a description of the technical mechanisms that track and record activities on BIS' information systems that contain or use confidential information including PII.
- The Network Services Department shall be responsible for conducting reviews of BIS' information systems activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.
- The Security Officer or Privacy Officer shall develop a report format to capture the review findings. Such 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 report shall be in a checklist format.
- Such reviews shall be conducted regularly. Audits also shall be conducted if BIS 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:
  - Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
  - File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.
  - 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.
  - User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

All significant findings shall be recorded using a standard report format.

- The Information Security Team shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the Security Officer or Privacy Officer for review and shall be responsible for maintaining such reports. The Security Officer or Privacy Officer shall consider such reports and recommendations in determining whether to make changes to BIS' administrative, physical, and technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the policy entitled Employee Responsibilities (Report Security Incidents).

16 Wireless Detection / Remediation

16.1 Policy

To reduce the risks associated with the installation of unauthorized and/or improperly secured wireless networking devices that extend BIS network(s), the following procedures have been developed to facilitate the detection, analysis, and mitigation of unauthorized (rogue) wireless access points. The primary risk posed by such devices is exposure and possible interception of sensitive data.

16.2 Procedure

Detection:

1. BIS wireless (internet SSID) access point controllers will be configured to detect and report (create log records of) other Service Set identifiers (SSID) within their area of coverage.
2. On a regular basis, a program will gather the relevant log records from the wireless controllers, merge the information gathered with other network records, and write the resultant information into a database. The database will include fields to indicate:
    a) Known, registered wireless access point devices and their configured SSID
    b) Unknown/new devices
    c) Known devices that are in the process of being reviewed/mitigated
3. Wireless access point information will be collected and maintained on a continuous basis while the device is detected, and for 12 months after the last detection.

Analysis:

1. On a regular basis, or quarterly, the Information Security Oficer and/or Policy Officer will review the information in the log records for changes and initiate mitigation procedures for unknown devices.
2. Owner contact information, based on the network records available, will be obtained (if possible).

Mitigation:

1. The Information Security and Policy Office will send device details and a policy notice (via e-mail) regarding the unauthorized device to:
    a) The IT Director and/or Network Security Contact (NSC) of the appropriate University Organization where the device is installed.
    b) The owner or operator of the device, if known.
2. The Information Security and Policy Office will create a record (ticket) with the relevant information in their problem tracking system.
3. The Information Security and Policy Office will allow one week for a response detailing which remediation or mitigation steps have been taken:

    a) The device was removed. UI wireless service (eduroam) is or will be used in its place.

    b) The device was appropriately secured using current best practices. The device has been or will be registered (authorized) with ITS Network Services for continued use.

4. The Information Security and Policy Office will follow up with any non or unsatisfactory responses to determine the status of the mitigation. At the Information Security and Policy Office or ITS Network

Services discretion, any subsequent detection of the device, in any location, after one week from sending the notice will result in the wired network connection (or connections should the device be moved), being disconnected.

Notes:

- Authorization for keeping personal, research, or department-owned wireless access point devices connected to the University campus network will be determined on a case basis.
- The Information Security and Policy Office will obtain/facilitate assistance from the ITS Network Services group as necessary.
- Any device that is disrupting the operation of the University campus network, or the UI wireless network service (eduroam), will be subject to immediate shut down as defined in the University Network Citizenship Policy.

17 Data Integrity

17.1 Policy

BIS shall implement and maintain appropriate electronic mechanisms to corroborate that confidential information including PII has not been altered or destroyed in an unauthorized manner.

The purpose of this policy is to protect confidential information from improper alteration or destruction.

17.2 Procedure

- To the fullest extent possible, BIS shall utilize applications with built-in intelligence that automatically checks for human errors.
- BIS shall acquire appropriate network-based and host-based intrusion detection systems. The Security Officer or Privacy Officer shall be responsible for ensuring the installation, maintenance, and updates of such systems.
- BIS will implement host file and registry tracking to monitor for and alert on any unauthorized changes to system files or parameters.
- To prevent transmission errors as data passes from one computer to another, BIS will use encryption, as determined to be appropriate, to preserve the integrity of data.
- BIS 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, BIS will test its information systems for accuracy and functionality before it starts to use them. BIS will update its systems after IT vendors release fixes to address known bugs or problems.
- BIS will install and regularly update antivirus software on all workstations and servers to detect and prevent malicious code from altering or destroying data.
- To prevent exposing magnetic media to a strong magnetic field, workforce members shall keep magnetic media away from strong magnetic fields and heat. For example, computers should not be left in automobiles during the summer months.

17.3 Security of Privileged Data

Privileged information shall be defined as any information to which the employee has access but which other people who may contact the employee should not have access. Employees of the offices of our clients have the right to have access to the data pertaining to the transactions they are working on. Members of the public do not have the right to have access to the data pertaining to transactions performed by our clients.

Here are two examples for how to handle requests for access to privileged data.

1. A client asks you for credit card information beyond what is contained in the transaction table. Inform the client that you do not have access to that privileged information and pass the call to your supervisor who will inform the caller that we in Support do not have access to that information.

2. A member of the public asks you for any transaction or credit card information. Inform them that you are not authorized to divulge that information. Pass the call to your supervisor who will inform the caller that BIS will not divulge that information without a subpoena.

18 Contingency Plan

18.1 Policy

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain confidential information.

BIS is committed to maintaining formal practices for responding to an emergency or other occurrence that damages systems containing confidential information. BIS shall continually assess potential risks and vulnerabilities to protect confidential information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with all applicable statutes and regulations.

18.2 Procedure

- BIS, under the direction of the Security Officer or Data Privacy Officer, shall implement a data backup plan to create and maintain retrievable exact copies of confidential information.
- No less than daily incremental backups of confidential information will be performed and at least one full weekly backup. Backups will be completed using standard cloud hosting tools and stored offsite from the primary hosting facility. Backup media that is no longer in service will be disposed of in accordance with BIS' data retention policy.
- The Security Officer or Privacy Officer shall audit storage and removal of backups and ensure all applicable access controls are enforced.
- The Security Officer or Privacy Officer shall ensure backup procedures are tested no less than on an annual basis to safeguard that exact copies of confidential information can be retrieved and made available. Such testing shall be documented by the DevOps team. To the extent such testing indicates need for improvement in backup procedures, the Security Officer or Privacy Officer shall ensure such improvements are implemented in a timely manner.
- Disaster Recovery and Emergency Mode Operations Plan
- The Security Officer or Privacy Officer shall be responsible for ensuring the development and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:
    - Restoring or recovering any loss of confidential information and/or systems necessary to make confidential information available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and
    - Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained in a secure location.
- The disaster recovery and emergency mode operation plan shall include the following:
    - Current copies of the information systems inventory and network configuration developed and updated as part of BIS' risk analysis.
    - Current copy of the written backup procedures developed and updated pursuant to this policy.
    - Identification of an emergency response team. Members of such team shall be responsible for the following:
        - Determining the impact of a disaster and/or system unavailability on BIS' operations.
        - In the event of a disaster, securing the site and providing ongoing security.
        - Retrieving lost data.

        - Identifying and implementing appropriate “work-arounds” during such time information systems are unavailable.
        - Taking such steps necessary to restore operations.
    - Procedures for responding to loss of electronic data including, but not limited to retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of BIS’ risk analysis
    - Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:
        - Members of the immediate response team,
        - Where backup data is stored,
        - Information systems vendors, and
        - All current workforce members.

- The disaster recovery team shall meet on at least an annual basis to:
    - Review the effectiveness of the plan in responding to any disaster or emergency experienced by BIS;
    - In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills; and
    - Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer or Privacy Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer or Privacy Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

19 Security Awareness and Training

19.1 Policy

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

All workforce members shall receive appropriate training concerning BIS' security policies and procedures. Such training shall be repeated at least annually for all employees.

19.2 Procedure

- The Security Officer or Privacy Officer shall have responsibility for the development and delivery of initial security training. All workforce members shall receive such initial training addressing the requirements of confidential information including PII. 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 or Privacy Officer shall be responsible for maintaining appropriate documentation of all training activities.

- The Security Officer or Privacy Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of confidential information including PII, e.g., addition of new hardware or software, and increased threats.

- The Security Officer or Privacy Officer shall generate and distribute to all staff routine security reminders on a regular basis. Periodic reminders shall address password security, malicious software, incident identification and response, and access control. The Security Officer or Privacy 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, mouse pads, sticky notes, etc. The Security Officer or Privacy Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.

- The Security Officer or Privacy Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

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

    1. Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail,
    2. The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,
    3. Instructions to never download files from unknown or suspicious sources,
    4. Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software,
    5. The importance of backing up critical data on a regular basis and storing the data in a safe place,
    6. Damage caused by viruses and worms, and
    7. What to do if a virus or worm is detected.

- As part of the aforementioned Security Training Program and Security Reminders, the Security Officer or Privacy 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:

    1. Passwords change interval.
    2. Password re-use restrictions.
    3. Password complexity requirements.
    4. Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.
    5. A password must be promptly changed if it is suspected of being disclosed, or known to have been disclosed.
    6. Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to “fix” a computer or handle an emergency situation) or individuals, including family members.
    7. Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
    8. Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
    9. Any employee who is directed by the Security Officer or Privacy Officer to change his/her password to conform to the aforementioned standards shall do so immediately.

20 Security Management Process

20.1 Policy

To ensure BIS conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PII held by BIS.

BIS shall conduct an accurate and thorough risk analysis to serve as the basis for BIS' PII storage compliance efforts. BIS shall re-assess the security risks to its PII storage and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business practices and technological advancements.

20.2 Procedure

a. The Security Officer or Privacy Officer shall be responsible for coordinating BIS' risk analysis. The Security Officer or Privacy Officer shall identify appropriate persons within the organization to assist with the risk analysis.

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

    i. Document BIS' current information systems.

        1. Update/develop information systems inventory. Update/develop network diagram illustrating how organization's information system network is configured.

        2. Update/develop BIS owned facility layout(s) 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.

        3. For each application identified, identify each licensee (*i.e.,* authorized user) by job title and describe the manner in which authorization is granted.

d) For each application identified:

1. Describe the data associated with that application.

2. 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.

3. 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.

4. 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 a period of time.
    1. High – Application is critical in providing the service. Outage would cause severe problems.
    2. Medium – Application is needed but an outage would only minorly impact the service.
    3. Low – Application is optional. Outage would not impact the service.

5. Define the sensitivity classification of the data as Confidential, Restricted, Internal Use or Public. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.

    1. Confidential – Most private or sensitive information that must be controlled always. Disclosure may cause severe problems for BIS, its customer or business partners. Access to this information must be approved by the Executive information owner. Examples include client data, mergers and acquisitions, and legal information protected by attorney-client privilege.
    2. Restricted – This information is private and restricted to those with a legitimate business need. Disclosure may cause significant problems for BIS, its customers or business partners. Access to this information must be approved by an information owner that is typically a director level or higher. Examples are customer account information, billing and invoices.
    3. Internal Use Only – The information is intended for use within BIS, and in some cases business partners. Disclosure of this information to outsiders may cause problems for BIS, its customers, or business partners. This type of information is widely distributed within BIS or it could be distributed within the organization without advance permission. Examples are internal telephone book, most electronic messages, and incident or root cause analysis reports.
    4. Public – This information has been approved for public or prospect release. Disclosure of this information will not cause problems for BIS, its customers, or business partners. Examples are approved marketing brochures and material posted to the BIS web page.

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

    a. Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of PII and ePHI created, received, maintained, or transmitted by BIS. 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

    - 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

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

    - Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail

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

        - Identify and document vulnerabilities in BIS 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 PII or ePHI, modification of PII or 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.

- Determine and document probability and criticality of identified risks.

i) Assign probability level, i.e., likelihood of a security incident involving identified risk.

- "Very High" (4) is defined as having an extreme likelihood for risk to occur.
- "High" (3) is defined as having a high likelihood for risk to occur.
- "Medium" (2) is defined as a modest chance of occurrence.
- “Low” (1) is defined as unlikely to occur.
    - Assign impact level.
- "Very High" (4) is defined as having a catastrophic impact on the medical practice including a significant number of medical records which may have been lost or compromised.
- "High" (3) is defined as having a significant impact including a moderate number of medical records within BIS which may have been lost or compromised.
- "Medium" (2) is defined as a modest or insignificant impact including the loss or compromise of some medical records.
- “Low” (1) is defined as it would be minor to the service or business operations.
    - Determine risk score for each identified risk. Multiply the probability score and criticality score. Those risks with a higher risk score require more immediate attention.
        - Identify and document appropriate security measures and safeguards to address key vulnerabilities. To accomplish this task, review the vulnerabilities you have identified in relation to the standards and implementation specifications. Focus on those vulnerabilities with high risk scores, as well as specific security measures and safeguards required by the Security Rule.
        - Develop and document an implementation strategy for critical security measures and safeguards.

i) Determine timeline for implementation.

ii) Determine costs of such measures and safeguards and secure funding.

iii) Assign responsibility for implementing specific measures and safeguards to appropriate person(s).

iv) Make necessary adjustments based on implementation experiences.

v) Document actual completion dates.

i. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.

c. The Security Officer or Privacy Officer shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The Security Officer or Privacy Officer shall identify appropriate persons within the organization to assist with such evaluations. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the HIPAA Security Regulations; new federal, state, or local laws or regulations affecting the security of ePHI; changes in technology, environmental processes, or business processes that may affect HIPAA Security policies or procedures; or the occurrence of a serious security incident. Follow-up evaluations shall include the following:

i. Inspections, reviews, interviews, and analysis to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess employee compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., not posted), and workstation sessions terminated (i.e., employees logged out); review of latest security policies and procedures for correctness and completeness; and inspection and analysis of training, incident, and media logs for compliance.

ii. Analysis to assess adequacy of controls within the network, operating systems and applications. As appropriate, BIS shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement

iii.

iv.

20.3 Executive Quarterly Review

Executive management will ensure that quarterly reviews are conducted to confirm that designated security personnel are following policies and operational procedures. Results of the reviews will be documented and approved with signature of the Chief Information Officer.

Executive review will ensure that personnel delegated with responsibility for aspects of the PCI-DSS program are properly carrying out those duties. Review will include but is not limited to:

- Daily log reviews
- Firewall ruleset reviews
- Applying configuration standards to new systems
- Responding to security alerts
- Change management processes

21 Sanction Policy

21.1 Policy

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

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

21.2 Purpose

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

21.3 Definitions

Workforce member means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.
Sensitive information, includes, but not limited to, the following:

- Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by BIS.
- Payroll data – Any information related to the compensation of an individual during that individuals' employment with BIS.
- Financial/accounting records – Any records related to the accounting practices or financial statements of BIS.
- Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.

Availability refers to data or information which is accessible and useable upon demand by an authorized person.
Confidentiality refers to data or information which is not made available or disclosed to unauthorized persons or processes.
Integrity refers to data or information that have not been altered or destroyed in an unauthorized manner.

21.4 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 (user name & password). Leaving computer unattended while being able to access sensitive information. Disclosing sensitive information with unauthorized

Level	Description of Violation
	persons. Copying sensitive information without authorization. Changing sensitive information without authorization. Discussing sensitive information in a public area 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, Privacy 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 (user name & 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.

Recommended Disciplinary Actions
In the event that a workforce member violates BIS' privacy and security policies and/or violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or related state laws governing the protection of sensitive and patient identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	Verbal or written reprimand Retraining on privacy/security awareness Retraining on BIS' privacy and security policies Retraining on the proper use of internal or required forms
2	Letter of Reprimand*; or suspension Retraining on privacy/security awareness Retraining on BIS' privacy and security policies Retraining on the proper use of internal or required forms
3	Termination of employment or contract Civil penalties as provided under applicable Federal/State/Local law Criminal penalties as provided under applicable Federal/State/Local law

- Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, BIS shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

  *A Letter of Reprimand must be reviewed by Human Resources before given to the employee.

  Exceptions
  Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with BIS.

22 Breach Notification Procedures

22.1 Purpose

To outline the process for notifying affected individuals of a breach of protected information under the Privacy Act, unsecured protected health information (PHI) for the purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and/or state breach notification purposes.

22.2 Scope

This applies to all employees, volunteers, and other individuals working under contractual agreements with BIS.

22.3 Definitions

State Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of Personal Information that compromises the security, confidentiality, or integrity of the Personal Information.

Personal Information – Personal Information has many definitions including definitions by statute which may vary from state to state. Most generally, Personal Information is a combination of data elements which could uniquely identify an individual. Please review applicable state data breach statutes to determine what definition of Personal Information is applicable for purposes of the document.

HIPAA Breach – Unauthorized acquisition, access, use, or disclosure of unsecured PHI.

Personally Identifiable Information (PII) – Information in any form that consists of a combination of an individual's name and one or more of the following: Social Security Number, driver's license or state ID, account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or other information which could be used to identify an individual.

Individually Identifiable Health Information (IIHI) – PII which includes information related to the past, present or future condition, treatment, payment or provision of health care to the identified individual.

Privacy Act Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information protected by the Privacy Act. This information includes, but is not limited to Social Security Number, government issued ID numbers, financial account numbers or other information posing a risk of identity theft.

Private Information – Information protected by the Privacy Act, Personally Identifiable Information, Personal Information and Protected Health Information collectively.

Protected Health Information (PHI) – Individually identifiable health information except for education records covered by FERPA and employment records.

22.4 Procedure

Reporting a Possible Breach

1. Any employee who becomes aware of a possible breach of privacy involving Private Information in the custody or control of BIS will immediately inform their supervisor/manager, and the Privacy Officer.

2. Notification should occur immediately upon discovery of a possible breach or before the end of your shift if other duties interfere, however, in no case should notification occur later than twenty-four (24) hours after discovery.
    a. The supervisor/manager will verify the circumstances of the possible breach and inform the Privacy Officer and the division Administrator/Director within twenty-four (24) hours of the initial report.
3. You may call the Privacy Officer directly at 423-946-2182
    a. Provide the Privacy Officer with as much detail as possible.
    b. Be responsive to requests for additional information from the Privacy Officer.
    c. Be aware that the Privacy Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.
4. The Privacy Officer, in conjunction with BIS' Legal Counsel, will decide whether or not to notify the President/CEO as appropriate by taking into consideration the seriousness and scope of the breach.

Containing the Breach

1. The Privacy Officer will take the following steps to limit the scope and effect of the breach.
    a. Work with department(s) to immediately contain the breach. Examples include, but are not limited to:
        i. Stopping the unauthorized practice
        ii. Recovering the records, if possible
        iii. Shutting down the system that was breached
        iv. Mitigating the breach, if possible
        v. Correcting weaknesses in security practices
        vi. Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity

Investigating and Evaluating the Risks Associated with the Breach

1. To determine what other steps are immediately necessary, the Privacy Officer in collaboration with BIS' Legal Counsel and affected department(s) and administration, will investigate the circumstances of the breach.
    a. A team will review the results of the investigation to determine root cause(es), evaluate risks, and develop a resolution plan.
        i. The Privacy Breach Assessment tool will help aid the investigation.
    b. The Privacy Officer, in collaboration with BIS' Legal Counsel, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:
        i. Contractual obligations
        ii. Legal obligations – BIS' Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment to the Privacy Officer and the rest of the breach response team
        iii. Risk of identity theft or fraud because of the type of information lost such as social security number, banking information, identification numbers
        iv. Risk of physical harm if the loss puts an individual at risk of stalking or harassment
        v. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records
        vi. Number of individuals affected

Notification

- The Privacy Officer will work with the department(s) involved, BIS' Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
- If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach.

a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
    i. Notices must be in plain language and include basic information, including:
        1. What happened
        2. Types of PHI involved
        3. Steps individuals should take
        4. Steps covered entity is taking
        5. Contact Information

    ii. Notices should be sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.

b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.

- The required elements of notification vary depending on the type of breach and which law is implicated. As a result, BIS' Privacy Officer and Legal Counsel should work closely to draft any notification that is distributed.
- Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.
    a. If a breach affects five-hundred (500) or more individuals, or contact information is insufficient, BIS will notify a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.
- Using multiple methods of notification in certain cases may be the most effective approach.

Business associates must notify BIS if they incur or discover a breach of unsecured PHI.

1. Notices must be provided without reasonable delay and in no case later than sixty (60) days after discovery of the breach.
2. Business associates must cooperate with BIS in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If BIS' Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to HHS at the same time that notices to individuals are issued.
2. If a breach involves fewer than five-hundred (500) individuals, BIS will be required to keep track of all breaches and to notify HHS within sixty (60) days after the end of the calendar year.

Prevention

1. Once immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach.
    a. If necessary, this will include a security audit of physical, organizational, and technological measures.
    b. This may also include a review of any mitigating steps taken.
2. The Privacy Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

22.5 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 in accordance with BIS' Sanction Policy.

22.6 Attachments

Appendix E: Privacy Breach Assessment

22.7 Related Policies

IS-2.0 Sanction Policy

23 Approved Equipment

23.1 Policy

It is the policy of BIS to purchase and deploy only pre-approved network equipment and payment card handling devices. A request for equipment not listed below will need to be approved by the Chief Information Officer or their appointed delegate before a purchase order or requisition document can be signed or unauthorized equipment can be purchased.

23.2 Purpose

In order to prevent the purchase and use of insecure equipment in our offices or in those customer offices which we have a contractual obligation.

23.3 List of Approved Equipment

Payment Card Processing Devices

- Ingenico IPP320
- Ingenico ISC250
- Ingenico ISC480
- IDTech IDRE-335133B
- IDTech IDRE-335133BX

Routers

- Ubiquiti ERLite-3

Switches

- Cisco SG110D-08
- HP 1820-24G
- HP 1820-48G

24 Server, PC and Credit Card Device Configuration

24.1 Policy

It is the policy of BIS to follow documented procedures for the setup and configuration of servers, PCs and payment card handling devices.

24.2 Purpose

This section will provide the user a list of document locations. These documents define the policies and procedures which need to be followed when configuring a server, PC or credit card device.

24.3 Servers

In-House server
NOTE: Network Services always handles the setup of in-house servers so they would need to provide this process document.

Customer server
\\opserver\e\Service\Documents\Server - PC - CC Device Configuration\Server Setup Process.docx

24.4 PCs

In-House PC
\\opserver\e\Service\Documents\Server - PC - CC Device Configuration\In House PC setup.doc

Kiosk PC
\\opserver\e\Service\Documents\Server - PC - CC Device Configuration\Kiosk Setup and Configuration Guide.docx

Customer PC
\\opserver\e\Service\Documents\Server - PC - CC Device Configuration

24.5 Payment Card Processing Devices

Ingenico 480, 250 and 320
\\opserver\e\Service\Documents\Server - PC - CC Device Configuration\Ingenico Device Configuration.docx

IDTech
\\opserver\e\Service\Documents\Server - PC - CC Device Configuration

Appendix A

I, the undersigned, do hereby attest that the device described below has been destroyed per establish, written company policy.

Device Description

Device Serial Number, MAC or Other Identifier

Date of Destruction

Employee Signature

Date of Signature

Employee Printed Name

Supervisor Signature

Date of Signature

Supervisor Printed Name