­­

Attention: IIAV Member Agencies

Virginia Statute 38.2-613.2 requires that each insurance institution, agent, and insurance-support organization will have a written information security program that includes administrative, technical, and physical safeguards for the protection of policy information.

As an IIAV member benefit, the attached Information Security Program template was developed specifically for IIAV member agencies. This includes an addendum for PCI compliance requirements, and a HIPPA Rule Addendum for those who need it.

Don’t get caught being out of compliance and having to pay a potential fine. Make sure your agency is in compliance by implementing your written security program.

If you have any question/comments contact Linda Loving.

**Linda S. Loving, CIC, AISM, AIAO** | IIAV Chief Operating Officer and VFSC Executive Vice President

Phone 804-747-9300 / 800-288-4428:

Email: [lloving@iiav.com](mailto:lloving@iiav.com)

Disclaimer: This document is for use as a baseline template and will need to be modified based on an agency’s specific requirements. Agencies may wish to consult with their own outside experts. It is not intended to be an exhaustive treatment of the topic but should be used in conjunction with other policies. It is not intended to constitute legal advice to individual agencies.

Authorized by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

  Version \_\_\_\_\_\_\_\_

Information Security PROGRAM



010218 ed.

Table of Contents

[Document Revision History 3](#_Toc510173512)

[Executive Summary 3](#_Toc510173513)

[Program Objectives 3](#_Toc510173514)

[General System Description 3](#_Toc510173515)

[Administration 4](#_Toc510173516)

[General responsibilities 4](#_Toc510173517)

[Staff Manager responsibilities 4](#_Toc510173518)

[IT Manager responsibilities 5](#_Toc510173519)

[The Internet and E-mail 6](#_Toc510173520)

[Employee Responsibilities for Internet and Email Use 6](#_Toc510173521)

[Unacceptable Internet and Email Use 7](#_Toc510173522)

[Downloads 7](#_Toc510173523)

[Monitoring 8](#_Toc510173524)

[Computer Viruses 8](#_Toc510173525)

[Information Technology Department Responsibilities 8](#_Toc510173526)

[Employee responsibilities 9](#_Toc510173527)

[Account passwords 10](#_Toc510173528)

[IT Manager Responsibilities 10](#_Toc510173529)

[Employee responsibilities 10](#_Toc510173530)

[Supervisor Responsibilities 11](#_Toc510173531)

[Physical Security 11](#_Toc510173532)

[Staff Manager Responsibilities 11](#_Toc510173533)

[IT Manager Responsibilities 12](#_Toc510173534)

[Employee Responsibilities 12](#_Toc510173535)

[Telephone Use 13](#_Toc510173536)

[Intellectual Property and License Agreements 13](#_Toc510173537)

[IT Manager responsibilities 13](#_Toc510173538)

[Employee responsibilities 13](#_Toc510173539)

[Sensitive Information 14](#_Toc510173540)

[Personally Identifiable Information (PII) 14](#_Toc510173541)

[Personal Information Under Va. Code. § 18.2-186.6 14](#_Toc510173542)

[Medical Information Under Va. Code. § 32.1-127.1:05 15](#_Toc510173543)

[Medical Record Information and Protected Health Information 15](#_Toc510173544)

[Payment Card Industry Data Security Standard (PCI DSS) 16](#_Toc510173545)

[Incident Response Plan (Data Breach) 17](#_Toc510173546)

[Updates 18](#_Toc510173547)

# Document Revision History

| Date | Author | Version | Change Reference |
| --- | --- | --- | --- |
|  |  |  |  |
| 03/xx/18 | Name | xx | xx |

## Executive Summary

Computer information systems and networks are an integral part of business at Insurance Agency Name Here (the “Agency”). Threats from both the intentional and unintentional actions of people make the challenge of ensuring the confidentiality, integrity, and availability of sensitive information an ongoing, critical part of our daily business. This Information Security Program (ISP) identifies the administrative, technical, and physical safeguards implemented by the Agency to help protect all Agency computing systems and the data that resides in those systems from unauthorized access, use and disclosure.

## Program Objectives

The following polices are established to:

1. Ensure the security confidentiality, integrity and availability of policyholder information;
2. Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of policyholder information;
3. Protect against unauthorized access to or use of policyholder information that could result in substantial harm or inconvenience to any policyholder;
4. Reduce business and legal risk to the Agency;
5. Protect the good name of our Industry;
6. Protect the good name of the Agency; and
7. **Protect our clients**.

## General System Description

Include a brief description of the Insurance Agency Information System here.

*[Optional. May also include system diagram]*

## Administration

The Information Technology Manager (IT Manager) is responsible for the technical components of this policy. The Staff Manager (Owners, Managers or Supervisors) is responsible for the administrative components of the policy. These roles may be assigned to existing staff positions or third-party contracted services without re-designation.

Subjects covered in this document include:

1. General responsibilities
2. Staff Manager responsibilities
3. IT Manager responsibilities
4. The Internet and email
5. Computer viruses
6. Account passwords
7. Physical security
8. Copyrights and license agreements
9. Sensitive Information
10. Personally Identifiable Information (PII)
11. Medical Record Information and Protected Health Information (PHI)
12. Payment Card Industry Data Security Standard (PCI DSS)
13. Incident Response Plan (Data Breach)

Additional topics referenced in this ISP will be covered by other Agency policies.

## General responsibilities

This policy specifies general responsibilities for which all employees are responsible, except where specific responsibilities are assigned to specific categories of employees.

## Staff Manager responsibilities

Owners, Managers and Supervisors:

1. Ensure that **ALL** employees and third-party contractors who have access to Agency systems are aware of, and comply with, this policy.
2. Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.
3. Ensure all staff complete information security training on an annual basis.
4. Coordinate with the IT Manager to ensure all policies and procedures are regularly reviewed, updated, and enforced for the security of the Agency.

## IT Manager responsibilities

The IT Manager:

1. In collaboration with Staff Managers, develops and maintains written standards and procedures necessary to ensure the implementation of, and compliance with, information security policy directives. This should include ongoing risk assessments as well as establishing and maintaining baseline configurations and inventories of Agency systems to enforce appropriate security settings as well as regular security scans and other information security enforcement mechanisms to maintain adequate system security across the Agency
2. Limits system access to only authorized users.
3. Grants system access based on least privilege principles.
4. Employs the principle of least functionality by configuring systems to provide only essential capabilities.
5. Provides appropriate support and guidance to assist employees in fulfilling their responsibilities in accordance with Agency information security policies.
6. Ensures every information system has password protected logon screens.
7. Enforces strong password, password resets, and screen lockout policies.
8. Ensures computer logon screens remind users of information security policies and contain the following banner or similar notification upon login:

*“Attention: You are about to access a(n) (Insurance Agency Name Here) information system. The information system and data contained herein are the property of (Insurance Agency Name Here). There is no expectation of privacy when using this information system. All activities on this information system are subject to monitoring by (Insurance Agency Name Here).”*

1. Ensures automated regularly scheduled backup services run normally.
2. Ensures user level encryption is available and utilized for email, files, and removable media and enforces policies regarding encryption of removable/portable media. *[Removable/portable media policies are good practice.]*
3. Ensures enterprise level encryption is utilized for all file servers and backup services.
4. Ensures physical security for all local servers and systems.
5. Ensures network and personal firewall devices and software are installed, securely configured and operational.
6. In collaboration with Staff Managers, develops and delivers information security training to staff on an annual basis. *[Good practice. Topics should include: phishing scams, password security, social media training, data identification, categorization, and privacy (such as what constitutes PII, PHI, FTI and how these types of information should be treated), physical security training, insider threat training (disgruntled employees), etc.]*
7. Authorizes and monitors all access to Agency information systems and prohibits access when appropriate, in consultation with Staff Managers and Agency policy.
8. Develops and maintains the Agency’s disaster recovery/work continuity plan in consultation with Staff Managers.
9. Develops and maintains the Agency’s breach/incident response plan in consultation with Staff Managers.
10. Develops and maintains the Agency’s other information security policies in consultation with Staff Managers. *[These may include policies such as bring your own device policies (BYOD) and social media policies]*

## The Internet and E-mail

The Internet is a worldwide, publicly accessible, interconnected network accessed by billions of individual users and organizations daily. Access to the Internet is provided to employees for the benefit of the Agency and its policyholders. Employees can connect to a variety of business information resources through the Internet. Although incredibly beneficial, use of the Internet poses substantial risks, including the risk of unauthorized access to sensitive information maintained by the Agency. The following rules are designed to mitigate those risks and to protect the Agency by promoting and enforcing responsible Internet use.

## Employee Responsibilities for Internet and Email Use

1. [Email use shall be limited to Agency business.] **or** [Any personal use of email should be minimal and not interfere with the employee’s productivity.] *[Choose policy most appropriate for your agency.]*
2. Employees shall not utilize social media accounts for work purposes under any circumstances.
3. Employees shall be responsible for the content of all text, audio, or images that the employee stores or transmits over the Internet. All communications should be identifiable as from the employee and reflect the professionalism of the Agency. (Such as email signature blocks, fax cover sheets, etc.)
4. Employees shall ensure that Agency approved confidentiality banners are attached to all emails.
5. Employees shall be familiar with and follow all applicable Agency policies, including dealing with security and confidentiality of Agency records.
6. External storage devices of any kind, (including USB (“thumb”) drives, external hard drives, CDs/DVDs, flash drives, etc.) shall not be utilized with any Agency information system without IT Manager authorization. All external storage devices shall be security scanned by the IT Manager or designee before introduction into any Agency information system. Employees shall run virus scans on all files received via the Internet prior to opening. *[OPTIONAL]*
7. Transmission of information protected under state and federal laws such as HIPAA Gramm-Leach-Bliley or any other applicable laws (confidential policyholder information) over the Internet, except in a manner specifically approved by Agency procedures is prohibited. Under no circumstances shall employees transmit Sensitive Information via the Internet or by any other means, including fax or by telephone without appropriate security safeguards, as directed by Agency policies.
8. When the Agency permits the transmission of non-confidential, non-public personal information via the Internet or by any other means, employees are required to take reasonable steps, in accordance with Agency policies, to ensure that information is delivered to the appropriate person who is authorized to receive such information for a legitimate use.

**Acceptable Internet and Email Use**

Employees using the Internet are representing the Agency. Employees are responsible for ensuring that the Internet is used in an effective and lawful manner. Examples of acceptable uses are:

1. Using Web browsers to obtain business information from commercial Web sites for Agency business.
2. Accessing databases for information as needed for Agency business
3. Using email for business communications
4. Customer research, marketing and prospecting
5. Accessing personal email, eCommerce shopping, Higher education

*[Depending on Agency Management]*

## Unacceptable Internet and Email Use

Employees shall not use the Internet for purposes that are illegal, harmful to the Agency, or nonproductive. Examples of unacceptable use are:

1. Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
2. Conducting personal business using Agency resources unless specifically authorized to do so.
3. Transmitting any content that is offensive, harassing, or fraudulent
4. Online gambling, pornography, or accessing social media accounts
5. Utilization of the Internet and Email for any use that is prohibited by Agency policies

## Downloads

It is common practice to download files such as resource documents from the Internet for business purposes. Binary or “executable content” **SHALL NOT** be downloaded unless specifically authorized in writing in advance by the IT Manager. The risk introduced by downloading this type of content is high. Binaries or executable content can be identified by their file extensions, some of which are, .exe, .bat, .com, .link., .run, .dll.

Employees should ask the IT Manager or designee if they have any concerns about a file prior to downloading the file.

## Monitoring

All Agency information systems, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for specified business uses within the application provided. These information systems may be monitored for all lawful purposes, including ensuring that their use is authorized by the Agency, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes, but is not limited to, active simulated attacks by authorized Agency entities to test or verify the security of Agency systems. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, stored or transmitted utilizing the Agency information system, may be monitored. Employees have no expectation of privacy in Agency information systems and networks or the data residing therein.

Unauthorized use of Agency information systems and networks may subject the unauthorized user to criminal prosecution or disciplinary action up to and including termination from employment. Evidence of unauthorized use collected may be used for administrative, criminal, disciplinary actions and all other lawful purposes as necessary.

Attempts to upload, access, modify, or transmit information on Agency information systems without authorization are strictly prohibited, and may be punishable under the Computer Fraud and Abuse Act of 1986, the National Information Infrastructure Protection Act of 1996 and other federal or state laws.

## Computer Viruses

A computer virus is a malicious software program capable of replicating itself and causing harm to information systems including making unauthorized changes to programs or data and causing the destruction of agency resources and records. It is important to know that:

1. Computer viruses are much easier to prevent than cure.

2. Defenses against computer viruses include: protection against unauthorized access to information systems (both at the network and desktop levels), using only trusted sources for data and programs, and maintaining antivirus software.

## Information Technology Department Responsibilities

The Agency’s Information Technology Department, under the direction of the IT Manager shall:

1. Install and maintain appropriate versions of antivirus/antimalware software on all Agency information systems.
2. Ensure that all antivirus software data/definition files are automatically and routinely updated.
3. Respond to all virus detections or attacks, remove any viruses detected, and document each incident.

## Employee responsibilities

1. Employees shall not knowingly introduce a computer virus into an Agency information system.
2. Employees shall not open any attachment from an unknown source or from a known source with an unusual title or e-mail message. If an employee is unsure whether an email or attachment is safe, the employee shall contact the IT Manager for guidance prior to opening any questionable email or attachment.
3. Employees shall not load removable media (CD/DVD/USB/External Hard Drive) of unknown origin into Agency information systems.
4. Employees shall not download non-business files (e.g., music or video files) without permission from the IT Manager.
5. Incoming removable media shall be scanned for viruses before being introduced into Agency information systems.
6. Any employee who suspects that his/her workstation has been infected by a virus shall **IMMEDIATELY DISCONNECT THE WORKSTATION FROM THE INTERNET** and notify the IT Manager.
7. Employees shall not access Agency information systems from a remote location, including home computers, without written authorization from the IT Manager. If employees are authorized to access the Agency’s information system from a remote location, including home computers, it shall only be through a Virtual Private Network (VPN) or other secure means approved by the IT Manager. The requirements of this ISP and any other information security policies shall apply to employees remotely accessing Agency information systems.

*[Recommended. Mobile devices includes laptops and tablets as well as mobile phones. If employees have access to the network from remote locations, they should only be accessing it through secure means, such as a VPN. Ideally, they should also use a dedicated computer to access the network from a remote location, but this will depend on agency resources; some agencies may not have the resources to provide separate mobile devices.*]

1. Employees accessing Agency information systems from a remote location, including home computers, shall do so in accordance with Agency policies and are required to have the security software approved by the IT Manager installed and running on their device with automatic updates activated.
2. Employees are prohibited from accessing Agency information systems remotely utilizing unsecured wireless networks (open networks/guest networks/free Wi-Fi locations, etc.). Employees shall only access Agency information systems remotely utilizing securely encrypted wireless networks utilizing encryption methodology approved by the IT Manager.
3. Employees are prohibited from accessing Agency information systems utilizing mobile phones.

## Account passwords

The confidentiality and integrity of data stored on Agency information systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee’s job duties utilizing principles of least privilege and least functionality.

## IT Manager Responsibilities

The IT Manager shall:

1. Be responsible for the administration of user access to all Agency information systems.

2. Process user additions, deletions, and changes upon receipt of a written request from the employee user’s supervisor, although the IT Manager may process user deletions/deactivations in response to an oral request from a supervisor prior to receiving a written request.

3. Maintain a list of administrative access codes and passwords and keep this list in a secure area.

4. Enforce Agency wide, a minimum password complexity and change of characters when passwords are created.

5. Prohibit password reuse for a specified number of generations.

6. Allow temporary password use for system logons with an immediate change to a permanent password.

7. Authenticate or verify the identity of users, processes, or devices prior to allowing access to organizational systems.

8. Employ the principles of least privilege and least functionality when granting access and configuring organizational systems.

9. Limit system access to only authorized users.

10. Utilize non-privileged accounts or roles when accessing non-security functions and prevent non-privileged users from executing privileged functions.

11. Monitor and control all remote access sessions.

12. Protect wireless access using authentication and encryption and monitor all wireless access.

13. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

## Employee responsibilities

Each employee:

1. SHALL be responsible for all computer transactions that are made by him/her.
2. SHALL NOT disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained. Passwords should always be kept out of view and not be placed on the monitor or be visible on the desk area. Passwords should not be saved onto a USB drive, PDA or smart phone type device.
3. SHALL change passwords according to Agency policy. (at least every 90 days.)
4. SHALL use strong passwords that contain a combination of all four of the following: upper and lower-case letters, numbers and special characters and any other password policy requirements.
5. SHALL lock their workstation any time they leave their workstation unattended for any reason, e.g. for meetings, breaks, lunch, or at the end of the day. This includes activating the lockout screen saver on all computers.
6. SHALL NOT USE PASSWORDS FOR ANY PURPOSE OR ATTEMPT TO ACCESS AGENCY INFORMATION SYSTEMS AFTER TERMINATION FROM THE AGENCY.

## Supervisor Responsibilities

1. Managers and supervisors SHALL notify the IT Manager immediately, preferably in advance, if possible, whenever an employee leaves the Agency or transfers to another department so that his/her access can be revoked or adjusted, as appropriate.
2. Employee terminations SHALL be reported concurrently with, or prior to, the termination to ensure that the IT Manager can revoke user permissions as soon as possible.

## Physical Security

It is Agency policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards. Physical security will vary depending on the size and complexity of an organization.

## Staff Manager Responsibilities

The Staff Manager will ensure the physical security of the office spaces and be responsible for physical access controls which safeguard Sensitive Information.

Staff Managers shall, at a minimum:

1. Use lockable cabinets, desks or credenzas to store all files containing Sensitive Information.
2. Remove all Sensitive Information from office spaces shared with other companies when leaving for the day.
3. Ensure cleaning crews will be bonded, no open Sensitive Information containers shall be permitted after hours. All Sensitive Information containers shall be secure.
4. Ensure visitors will be logged and escorted at all times while in areas processing Sensitive Information.
5. Ensure that all documents containing Sensitive Information that are no longer used or needed for record retention purposes are shredded or otherwise destroyed or rendered unreadable in accordance with methods authorized by the Agency.
6. Ensure Sensitive Information is secured and protected against unauthorized access anytime staff are out of the office.
7. Establish document retention guidelines which ensure documents are retained and destroyed in a timely fashion when no longer required by policy or statute.
8. Monitor visitor activity and maintain logs of physical access.

## IT Manager Responsibilities

1. Servers and network equipment shall be installed in a locked cabinet, closet or room. Access shall be restricted to IT technical staff.
2. Ensure all laptop computers have a firewall, full hard drive encryption and strong passwords installed.
3. Ensure all requests for equipment installations, disconnections, modifications, and relocations occur in a timely manner. (This reduces the likelihood that staff will do it)
4. Critical computer equipment, e.g., file servers, should be protected by an uninterruptible power supply (UPS); all other computer equipment should be protected by a surge suppressor.
5. Ensure removable media have encryption capabilities and control the use of removeable media in accordance with Agency policies.
6. Track removable media when in use and ensure secure storage of removable media when not in use.

## Employee Responsibilities

1. Laptops or other Agency computing devices shall not be removed from Agency premises by the employee without advanced authorization by the department manager. All Agency laptops or other mobile computing devices removed from the Agency will have full hard drive encryption and be password protected.
2. Employees should exercise care to safeguard the equipment assigned to them.
3. Removable Media (CD’s, DVD’s, USB drives, etc.) shall be kept out of view and will be locked up when not in use. Removable media shall not be taken off premises without department manager approval, and then only in accordance with Agency policies.
4. Hardware and media should be kept away from environmental hazards such as water, heat, direct sunlight, and magnetic fields.
5. All Agency guests shall be logged in at the receptionist’s location or other authorized entry point and be escorted at all times while on Agency premises. Guests shall not be permitted to access secure areas without management authorization.

## Telephone Use

1. Employees shall confirm the identities of callers pursuant to Agency procedures before disclosing non-public and other sensitive Agency information to the caller.
2. Employees shall follow Agency procedures regarding what types of information they may disclose to various categories of caller.
3. Any suspected Phishing or probing shall be reported to the Office Manager and IT Manager immediately.
4. Employees shall ensure that mobile phones and other devices (such as tablets and laptops) with camera or video capability do not take video or photographs of Sensitive Information.

## Intellectual Property and License Agreements

It is Agency policy to comply with all laws respecting the ownership rights of others in intellectual property (e.g., software, web content, books and reports), including, but not limited to, United States copyright and trademark laws. There are severe civil and criminal penalties that can result from the violation of these laws.

## IT Manager responsibilities

The IT Manager shall:

1. Maintain records of software licenses executed by, or on behalf of the Agency.
2. Periodically inventory Agency computers to verify that only authorized software is installed.
3. Report **ALL** violations of Agency policy or licensing issues to management.
4. Not permit users to install software without authorization.

## Employee responsibilities

Employees shall **NOT**:

1. Copy, download or install software (unless authorized in advance by IT Manager). Only software that is licensed to or owned by the Agency may be installed on Agency computers.
2. Copy, incorporate, or transmit the information contained on web sites without securing the permission of the owner of that information in advance.
3. Create or produce any written work, display, website or presentation for the Agency without ensuring that proper permissions have been provided for the use of any material subject to copyright, trademark, patent, or other intellectual property rights.

## Sensitive Information

Sensitive Information is any information that is not generally available to the public that could be used to damage our employees, insureds/members of our clients, or our business. It includes any information that must be protected from unauthorized access. This information includes but is not limited to the following information types:

## Personally Identifiable Information (PII)

According to the National Institute of Standards and Technology (NIST) Special Publication 800-122, PII is any information about an individual maintained by an Agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. PII can be used to commit identity theft and similar crimes, and includes but is not limited to information such as a person’s name, and any of the following:

1. Personal identification, including a number or other identifying information from social security, state ID card, driver’s license, passport or employee ID.

2. Financial account identification, including bank account number or credit card number.

3. Other identifying information to access financial accounts or non-public records.

4. Employee records including payroll, pension and insurance.

5. Business-private information for legitimate business purposes, including business plans, vendor and customer lists, contracts, and account information of vendors, clients, and customers.

6. Financial transactions with our clients, employees and vendors including checks and ACH transfers.

## Personal Information Under Va. Code. § 18.2-186.6

The Code of Virginia § 38.2-602 defines “personal information” as:

The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

1. Social security number;

2. Driver's license number or state identification card number issued in lieu of a driver's license number; or

3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.

The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

## Medical Information Under Va. Code. § 32.1-127.1:05

The Code of Virginia § 32.1-127.1:05 defines “medical information” as:

The first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

1. Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

2. An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

## Medical Record Information and Protected Health Information

The Code of Virginia § 38.2-602 defines “medical record information” as personal information that:

1. Relates to an individual's physical or mental condition, medical history, or medical

treatment; and

2. Is obtained from a medical professional or medical-care institution, from the individual, or from the individual's spouse, parent, or legal guardian.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) defines protected health information (PHI) as individually identifiable health information that is:

1.     Transmitted by electronic media;

2.   Maintained in electronic media; or

3. Transmitted or maintained in any other form or medium.

It excludes individually identifiable health information in:

1.     Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

2.   Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and

3.   Employment records held by a covered entity in its role as employer.

## Payment Card Industry Data Security Standard (PCI DSS)

Another type of Sensitive Information is PCI data. The PCI DSS is a set of comprehensive requirements for enhancing payment account data security and was developed by the founding payment brands of the PCI Security Standards Council (PCI SSC): American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. It applies to all entities involved in payment card processing and all other entities that store, process, or transmit Cardholder Data and/or Sensitive Authentication Data.

Cardholder Data includes:

1. Primary Account Number (PAN)
2. Cardholder name
3. Expiration date
4. Service code

Sensitive Authentication Data includes:

1. Full track data (magnetic-stripe data or equivalent on a chip)
2. CAV2/CVC2/CVV2/CID
3. PINs/PIN blocks

\* *See* Payment Card Industry (PCI) Data Security Standard v. 3.2

Essential compliance with PCI requires:

1. In general, full Credit Card account information **SHOULD NOT** be transmitted via email. The account name and last four digits of the card number may be transmitted for reference, as in a receipt of payment.

2. Web payments must be processed using a PCI-compliant service provider approved by the IT Manager. Credit card numbers **SHOULD NOT** be entered into a web page or database of a server hosted on the Agency network, unless specifically designated for such a purpose by the IT Manager.

Any paper documents containing credit card information should be:

1. Limited to only information required to transact business,

2. Limited to only those individuals with a business need to have access,

3. Should be in a secure location and must be destroyed via approved methods once business needs no longer require retention.

\*See the PCI DSS addendum for more information on PCI DSS.

## Incident Response Plan (Data Breach)

A security breach occurs when an unauthorized access to the system occurs that bypasses or contravenes security policies, practices, or procedures which results in the compromise or potential compromise of sensitive data. If a breach occurs internally, it is called a security violation. Each employee shall be responsible for notifying the Staff Manager and IT Manager whenever he or she learns that there has been or may have been a security breach or security violation that may have compromised Sensitive Information or other Agency information about clients, employees or Agency business.

**IF A SECURITY BREACH OR SECURITY VIOLATION THAT COMPROMISES OR HAS THE POTENTIAL TO COMPROMISE SENSITIVE INFORMATION OCCURS OR IS SUSPECTED, THE AGENCY WILL TAKE THE FOLLOWING ACTIONS IMMEDIATELY:**

* 1. Notify management immediately (without delay);
  2. Investigate immediately (under management direction);
  3. SEVER the data connection (under management direction); (isolate suspect systems)
  4. CALL the Sera-Brynn Incident Response Hotline: (855) 514-6048
  5. Consult legal counsel
  6. Review the requirements of applicable state laws and regulations
* Review provisions of Virginia Code § [18.2-186.6](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-186.6). “Breach of personal information notification” for additional specific actions required.
* If medical information or HIPAA information may be compromised, Review provisions of Virginia Code § [32.1-127.1:05](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+32.1-127.1C05). “Breach of medical information notification” and the Health Insurance Portability and Accountability Act of 1996 (42 USC § 17937)

# Updates

This policy will be reviewed and updated annually to ensure compliance with Code of Virginia § 38.2-613.2 and other applicable laws. See Document Revision History on Page 3 of this Document.

Code of Virginia § 38.2-613.2. Information security program.

1. Each insurance institution, agent, and insurance-support organization shall implement a comprehensive ***written information security program*** that includes *administrative*, *technical*, and *physical safeguards* for the protection of policyholder information. The administrative, technical, and physical safeguards included in the information security program shall be appropriate to the size and complexity of the insurance institution, agent, or insurance-support organization and the nature and scope of its activities.
2. The information security program shall be designed to:

1. Ensure the security and confidentiality of policyholder information;

2. Protect against any anticipated threats or hazards to the security or integrity of the information; and

3. Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any policyholder.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

**EMPLOYEE ACKNOWLEDGEMENT**

This form is used to acknowledge receipt of, and compliance with, the Insurance Agency Name Here Information Security Program.

Each employee shall complete the following steps:

1. Read the Information Security Program.
2. Sign and date in the spaces provided below.
3. Return this page along with the signature page only to the Staff Manager.

By signing below, I agree to the following terms:

1. I have received and read a copy of the “Information Security Program.” I understand it and agree to abide by this policy in its entirety;
2. I understand and agree that any computers, software, storage media, and documents provided to me by Insurance Agency Name Here contain proprietary and confidential and Sensitive Information about Insurance Agency Name Here and its customers or its vendors, and that this is and remains the sole property of the Insurance Agency Name Here at all times;
3. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at Insurance Agency Name Here), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;
4. I agree to use special care to safeguard the privacy of “Protected Health Information” (HIPAA) and other Sensitive Information concerning customers and other individuals and to not disclose it to anyone, including fellow employees, except as necessary in the course of business and as specifically permitted by Agency procedures.
5. I agree to use special care to safeguard the confidentiality of my passwords, to not disclose them to fellow employees or other persons at **any time** and not to use these passwords for any purpose after termination from the Insurance Agency Name Here.
6. I agree that, if I leave Insurance Agency Name Here for any reason, I shall immediately return to the Insurance Agency Name Here all originals and any copies of all software, computer materials, computer equipment, data, files, documents, information, in whatever form, and any other Insurance Agency Name Here property that I may have received from Insurance Agency Name Here that is either in my possession or otherwise directly or indirectly under my control.
7. I agree to abide by all the provisions contained in the “Information Security Program,” or other information security policies even though they have not been singled out and repeated in this Acknowledgment form.
8. I understand and acknowledge that a violation of this Information Security Program by me may subject me to discipline, up to and including termination from employment or other legal action.

Employee signature:

Employee name:

Date:

Department: