

# INFORMATION SECURITY POLICY

# S H ! F T

LAST REVISION DATE

April 27th, 2022

DOCUMENT OWNER

Silvia Rojas

## TABLE OF CONTENTS

1	Introduction.....	4
1.1	Purpose.....	4
1.2	Scope.....	4
1.3	Acronyms / Definitions.....	4
1.4	Applicable Statutes / Regulations.....	5
1.5	Privacy Officer.....	6
1.6	Confidentiality / Security Team (CST).....	6
2	Employee Responsibilities.....	7
2.1	Employee Requirements.....	7
2.2	Prohibited Activities.....	7
2.3	Electronic Communication, Email, Internet Usage.....	8
2.4	Internet Access.....	9
2.5	Reporting Software Malfunctions.....	9
2.6	Report Security Incidents.....	10
2.7	Transfer of Sensitive/Confidential Information.....	10
2.8	Transferring Software and Files between Home and Work.....	10
2.9	Internet Considerations.....	11
3	Identification and Authentication.....	12
3.1	User Login IDs.....	12
3.2	Passwords.....	12
3.3	Confidentiality Agreement.....	13
3.4	Access Control.....	13
3.5	User Login Entitlement Reviews.....	13
3.6	Termination of User Login Account.....	14
4	Network Connectivity.....	15
4.1	Permanent Connections.....	15
4.2	Emphasis on Security in Third Party Contracts.....	15
5	Malicious Code.....	17
5.1	Retention of Ownership.....	17
6	Encryption.....	18
6.1	Definition.....	18
6.2	Encryption Key.....	18
6.3	Installation of authentication and encryption certificates on the email system.....	18
6.4	File Transfer Protocol (FTP).....	18
6.5	Secure Socket Layer (SSL) Web Interface.....	18

7	Telecommuting .....	20
7.1	General Requirements .....	20
7.2	Required Equipment.....	20
7.3	Hardware Security Protections.....	21
7.4	Data Security Protection.....	21
7.5	Disposal of Paper and/or External Media .....	22
8	Specific Protocols and Devices .....	23
8.1	Use of Transportable Media .....	23
9	Retention / Destruction of Paper Based Information .....	25
10	Disposal of External Media / Hardware .....	26
10.1	Disposal of External Media.....	26
10.2	Requirements Regarding Equipment .....	26
10.3	Disposition of Excess Equipment .....	26
11	Change Management .....	27
12	Audit Controls .....	28
13	Information System Activity Review .....	29
14	Data Integrity .....	31
15	Contingency Plan .....	32
16	Security Awareness and Training.....	35
17	Security Management Process.....	37
18	Emergency Operations Procedures .....	40
19	Sanction Policy .....	41
20	Employee Background Checks .....	44
21	E-Discovery Policy: Production and Disclosure.....	46
22	E-Discovery Policy: Retention .....	52
23	Breach Notification Procedures .....	58
	Appendix A – Network Access Request Form .....	62
	Appendix B – Confidentiality Form.....	64
	Appendix C – Approved Software.....	65
	Appendix D – Approved Vendors.....	66
	Appendix E – Incident Response Tools .....	67
	Appendix F – Background Check Authorization .....	68
	Appendix G – Change Management Tracking Log.....	70
	Appendix H – Employee Hiring and Termination Checklist .....	71

<b>SHIFT</b>		<b>Policy and Procedure</b>	
<b>Title: INTRODUCTION</b>		<b>P&amp;P #: IS-1.0</b>	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology (TVS001)</b>	

# 1 Introduction

---

## 1.1 PURPOSE

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at SHIFT, hereinafter, referred to as the **Company**. It serves as a central policy document with which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Company with policies and guidelines concerning the acceptable use of Company technology equipment, e-mail, Internet connections, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Company employees or temporary workers at all locations and by contractors working with the Company as subcontractors.

## 1.2 SCOPE

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

## 1.3 ACRONYMS / DEFINITIONS

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

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

**CTO** – The Chief Technology Officer is responsible for annual security training of all staff on confidentiality issues and for International Information Security Policy and Privacy compliance issues

**CPO** – The Chief Privacy Officer is responsible for information security compliance issues.

**CST** – Confidentiality and Security Team

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

**External Media –i.e.** DVDs, flash drives, USB keys, thumb drives, tapes

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

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

**FTP** – File Transfer Protocol

**IT** - Information Technology

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

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

**System:** internal technologies developed by the Company

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

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

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

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

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

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

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

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

## 1.4 APPLICABLE STATUTES / REGULATIONS

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

- The 1999 Gramm-Leach-Bliley Act
- the 2002 Homeland Security Act, which included the Federal Information Security Management Act (FISMA)
- the 2016 EU General Data Protection Regulation (GDPR)
- the 1995 Law of personal protection against the treatment of their personal data. Law N° 8968" of Costa Rica

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

## 1.5 PRIVACY OFFICER

The Company has established a Privacy Officer as required by international security regulations. This Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of the Company privacy policies in accordance with applicable laws. The current Privacy Officer for the Company is:

Adrián Murillo - 604 836 0360 – amurillo@aurainteractiva.com

## 1.6 CONFIDENTIALITY / SECURITY TEAM (CST)

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

All members identified within this policy are assigned to their positions by the CEO. The term of each member assigned is at the discretion of the CEO, but generally it is expected that the term will be one year. The current members of the CST are:

COO- Juan Carlos Vidal  
VP Sales – Andrés Cabezas  
CTO – Adrián Murillo  
CSO – Silvia Rojas

The CST will meet quarterly to discuss security issues and to review concerns that arose during the quarter. The CST will identify areas that should be addressed during annual training 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 the Company and act as the first line of defense in enhancing the security posture of the Company.

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 quarterly meetings.

The 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 the Company. This log will also be reviewed during the quarterly meetings.

<b>SHIFT</b>		<b>Policy and Procedure</b>	
<b>Title: EMPLOYEE RESPONSIBILITIES</b>		<b>P&amp;P #: IS-1.1</b>	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology (TVS002, TVS003)</b>	

## 2 Employee Responsibilities

### 2.1 EMPLOYEE REQUIREMENTS

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

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

Unattended Computers - Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Company 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 Company Corporate Assets - Only computer hardware and software owned by and installed by the Company is permitted to be connected to or installed on Company equipment. Only software that has been approved for corporate use by the Company may be installed on Company equipment. Personal computers supplied by the Company 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 the Company for home use.

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

### 2.2 PROHIBITED ACTIVITIES

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

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred 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 the Company 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. The Company has access to client information which is protected by international regulations 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 Company computers must be approved by the Company.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the Company 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 the Company is strictly prohibited.

### 2.3 ELECTRONIC COMMUNICATION, EMAIL, INTERNET USAGE

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

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

- 1) it does not consume more than a trivial amount of employee time or resources,
- 2) it does not interfere with staff productivity,
- 3) it does not preempt any business activity,
- 4) it does not violate any of the following:
  - 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 Company 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 Company information resources for personal or commercial profit is strictly prohibited.
  - d) Political Activities – All political activities are strictly prohibited on Company premises. The Company encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Company assets or resources.



- e) Harassment – The Company strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Company prohibits the use of computers, e-mail, 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 includes, 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. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

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

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

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

## 2.4 INTERNET ACCESS

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, among others, have already been blocked by the Company 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 should inform the appropriate Company 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, the Company 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 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 appropriate personnel should monitor the resolution of the malfunction or incident, and report to the CST 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 Company employee or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the Privacy Officer. Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of the Company CST. Members of the CST are specified above in this document.

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

Security breaches shall be promptly investigated. If criminal action is suspected, the Company Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately.

## 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 the Company and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Company policy and will result in personnel action and may result in legal action.

## 2.8 TRANSFERRING SOFTWARE AND FILES BETWEEN HOME AND WORK

Company proprietary data, including but not limited to technology development information, IT Systems information, financial information, or human resource data, shall not be placed on any computer that is not authorized by the Company or on any online storage units that are not property or authorized by the Company. It is crucial to the Company to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer Company data to a non-Company Computer System or Online Data Repository, the

supervisor or department head should notify the Privacy Officer or appropriate personnel of the intentions and the need for such a transfer of data.

## 2.9 INTERNET CONSIDERATIONS

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

The following security and administration issues shall govern Internet usage.

Prior approval of the Company Privacy Officer or appropriate personnel authorized by the Company shall be obtained before:

- Company information (including notices, memoranda, documentation, and software) is made available on any web-based repository that is not provided by the Company (Dropbox, Google Drive)
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor
- 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
- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with the Company Privacy Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

<b>SHIFT</b>		<b>Policy and Procedure</b>	
<b>Title: IDENTIFICATION and AUTHENTICATION</b>		<b>P&amp;P #: IS-1.2</b>	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology (TVS008, TVS015, TVS016, TVS023)</b>	

## 3 Identification and Authentication

### 3.1 USER LOGIN IDS

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

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

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

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

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

### 3.2 PASSWORDS

#### User Account Passwords

User IDs and passwords are required in order to gain access to all Company systems and workstations. 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 in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

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

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

Change Frequency – Passwords must be changed every 90 days. Compromised passwords shall be changed immediately.

Reuse - The previous twelve passwords cannot be reused.

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

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

### 3.3 CONFIDENTIALITY AGREEMENT

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

*I understand that any unauthorized use or disclosure of information residing on the Company information resource systems may result in disciplinary action consistent with the policies and procedures of the competent agencies.*

Temporary workers and third-party employees shall also sign a confidentiality agreement prior to accessing Company information and technological 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 the Company.

### 3.4 ACCESS CONTROL

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e. passwords, access control lists, constrained user interfaces, etc.) and external (i.e. firewalls, two factor authentication, etc.).

Rules for access to resources (including all internal technologies developed and third-party systems) have been established by the information/application owner or manager responsible for the resources. Access is granted only by the completion of a Technology Access Request Form (Appendix C). This form can only be initiated by the appropriate department head, and must be signed by the department head and the Security Officer or appropriate personnel.

This guideline satisfies the "need to know" requirement of the regulations, 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, technology, or external system **only** upon the signature of the Security Officer or appropriate personnel who is 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.

#### Identification and Authentication Requirements

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

### 3.5 USER LOGIN ENTITLEMENT REVIEWS

If an employee changes positions at the Company, employee's new supervisor or department head shall promptly notify the Information Technology ("IT") Department of the change of roles by indicating on the Network Access Request Form (Appendix C) both the roles or access that need to be added and the

roles or access that need to be removed so that employee has access to the minimum necessary data to effectively perform their new job functions. The effective date of the position change should also be noted on the Form so that the IT Department can ensure that the employee will have appropriate roles, access, and applications for their new job responsibilities. For a limited training period, it may be necessary for the employee who is changing positions to maintain their previous access as well as adding the roles and access necessary for their new job responsibilities.

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

### 3.6 TERMINATION OF USER LOGIN ACCOUNT

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the IT Department by indicating "Remove Access" on the employee's Network Access Request Form (Appendix C) and submitting the Form to 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 workday so that their user account(s) can be configured to expire.

The employee's department head shall be responsible for ensuring that all access to internal technologies developed and third-party systems as well as Company equipment and property is returned to the Company prior to the employee leaving the Company on their final day of employment.

No less than quarterly, the IT Manager or their designee shall provide a list of active user accounts for both network and application access, including access to the internal technologies developed and third-party systems to department heads for review.

Department heads shall review the employee access lists within five (5) business days of receipt. If any of the employees on the list are no longer employed by the Company, the department head will immediately notify the IT Department of the employee's termination status and submit the updated Network Access Request Form (Appendix C).

<b>SHIFT</b>		<b>Policy and Procedure</b>	
<b>Title: NETWORK CONNECTIVITY</b>		<b>P&amp;P #: IS-1.3</b>	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology</b>	

## 4 Network Connectivity

### 4.1 PERMANENT CONNECTIONS

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

### 4.2 EMPHASIS ON SECURITY IN THIRD PARTY CONTRACTS

Access to Company internal technologies developed and third-party systems should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the Company Information Security Policy have been reviewed and considered.
- Policies and standards established in the Company 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 in order to meet the covenants of the International Information Security Regulations.
- 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 detailed list of users that have access to Company 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 agreement 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 authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- Because annual confidentiality training is required under International Information Security Regulations, 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.



<b>SH!FT</b>		<b>Policy and Procedure</b>	
<b>Title: MALICIOUS CODE</b>		<b>P&amp;P #: IS-1.4</b>	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology (TVS018)</b>	

## 5 Malicious Code

---

### 5.1 RETENTION OF OWNERSHIP

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

<b>SHIFT</b>		<b>Policy and Procedure</b>	
<b>Title: ENCRYPTION</b>		<b>P&amp;P #: IS-1.5</b>	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology (TVS012, TVS015)</b>	

## 6 Encryption

### 6.1 DEFINITION

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read <http://www.webopedia.com/TERM/e/read.html> 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 ENCRYPTION KEY

An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, the Company shall establish the criteria in conjunction with the Privacy Officer or appropriate personnel. The Company employs several methods of secure data transmission.

### 6.3 INSTALLATION OF AUTHENTICATION AND ENCRYPTION CERTIFICATES ON THE EMAIL SYSTEM

Any user desiring to transfer secure email with a specific identified external user may request to exchange public keys with the external user by contacting the Privacy Officer or appropriate personnel. Once verified, the certificate is installed on each recipient workstation, and the two may safely exchange secure email.

### 6.4 FILE TRANSFER PROTOCOL (FTP)

Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the Privacy Officer or appropriate personnel.

### 6.5 SECURE SOCKET LAYER (SSL) WEB INTERFACE

Any EHR hosted (ASP) system, if applicable, will require access to a secure SSL website. Any such access must be requested using the Network Access Request Form (found in Appendix A) and have

appropriate approval from the supervisor or department head as well as the Privacy Officer or appropriate personnel before any access is granted.

<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title: TELECOMMUTING</b>	<b>P&amp;P #: IS-1.7</b>	
<b>Approval Date:</b>	<b>Review: Annual</b>	
<b>Effective Date:</b>	<b>Information Technology</b>	

## 7 Telecommuting

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. The Company considers telecommuting to be an acceptable work arrangement.

This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of the Company office environment. It applies to users who work from their home full time to employees on temporary travel, to users who work from a remote office location, and to any user who connects to the Company internal technologies developed and third-party systems, 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 the Company’s network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate as well as client data to risks not present in the traditional work environment.

### 7.1 GENERAL REQUIREMENTS

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

- **Need to Know:** Telecommuting Users will have the access based on the same ‘need to know’ as they have when in the office.
- **Password Use:** The use of a strong password, changed at least every 60 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
- **Training:** Personnel who telecommute must complete the same annual privacy training as all other employees.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

### 7.2 REQUIRED EQUIPMENT

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

**Company Provided:**

- Company supplied workstation (applied to certain workers).
- If using VPN, a Company issued hardware firewall is required.
- If printing, a Company supplied printer.
- If approved by your supervisor, a Company supplied phone.

**Employee Provided:**

- Broadband connection and fees,
- Paper shredder,
- Secure office environment isolated from visitors and family,
- A lockable file cabinet or safe to secure documents when away from the home office.

### 7.3 HARDWARE SECURITY PROTECTIONS

Virus Protection: Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all Company personal computers and is set to update the virus pattern on 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 Company information of any type via a VPN. The Company requires the use of VPN software and a firewall device, when stated and required. 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 or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 15 minutes of inactivity.

### 7.4 DATA SECURITY PROTECTION

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

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

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

Email: Do not send any individual-identifiable information via email unless it is encrypted. If you need assistance with this, contact the Privacy Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through email.

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

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of client level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted workspaces. If your laptop has not been set up with an encrypted workspace, contact the Privacy Officer or appropriate personnel for assistance.

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

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive 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 the Company: All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any client level information to anyone outside the Company without the written approval of your supervisor.

## 7.5 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-Company work environment, that need to develop paper based information, MUST have direct access to a shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with International Information Security Regulations compliant procedures.

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

<p><b>SHIFT</b></p>		<p><b>Policy and Procedure</b></p>	
<p><b>Title: SPECIFIC PROTOCOLS AND DEVICES</b></p>		<p><b>P&amp;P #: IS-1.8</b></p>	
<p><b>Approval Date:</b></p>		<p><b>Review: Annual</b></p>	
<p><b>Effective Date:</b></p>		<p><b>Information Technology (TVS009)</b></p>	

## 8 Specific Protocols and Devices

### 8.1 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 key devices.

The purpose of this policy is to guide employees/contractors of the Company in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Company networks. Every workstation or server that has been used by either Company 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 Company 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 Company within the Company. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Company networks. Transportable media received from an external source could potentially pose a threat to Company networks. **Sensitive data** includes all human resource data, financial data, Company 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 a rugged titanium format which connects to any 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 data** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB keys used to store Company data or sensitive data must be an encrypted USB key issued by the Privacy Officer or appropriate personnel. The use of a personal USB key to store sensitive data is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by the Company.
- Non-Company workstations and laptops may not have the same security protection standards required by the Company, and accordingly virus patterns could potentially be

transferred from the non-Company device to the media and then back to the Company workstation.

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

Examples of necessary data exchange include:

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 Company workstations or servers as long as the source of the media is on the Company Approved Vendor list (Appendix D).
- 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 the Company, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for data erasure that conforms to the established standards for data elimination.

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

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



<b>SH!FT</b>		<b>Policy and Procedure</b>	
<b>Title: RETENTION / DESTRUCTION of PAPER DOCUMENTS</b>		<b>P&amp;P #: IS-1.9</b>	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology (TVS020, TVS021)</b>	

## 9 Retention / Destruction of Paper Based Information

---

Many laws regulate the retention and destruction of paper based, sensitive information. The Company actively conforms to these laws and follows the strictest regulation if/when a conflict occurs.

Record Retention - Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information Company, client contracts, among others of a similar nature, are maintained for a period of 6 years.

Record Destruction - All hardcopy records that require destruction are shredded using NIST 800-88 guidelines.

<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title: DISPOSAL OF EXTERNAL MEDIA / HARDWARE</b>	<b>P&amp;P #: IS-1.10</b>	
<b>Approval Date:</b>	<b>Review: Annual</b>	
<b>Effective Date:</b>	<b>Information Technology (TVS020, TVS021)</b>	

## 10 Disposal of External Media / Hardware

### 10.1 DISPOSAL OF EXTERNAL MEDIA

It must be assumed that any external media in the possession of an employee is likely to contain either protected confidential information or other sensitive information. Accordingly, external media (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 Privacy Officer or appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.

### 10.2 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.

### 10.3 DISPOSITION OF EXCESS EQUIPMENT

As the older Company 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.
- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title: CHANGE MANAGEMENT</b>	<b>P&amp;P #: IS-1.11</b>	
<b>Approval Date:</b>	<b>Review: Annual</b>	
<b>Effective Date:</b>	<b>Information Technology (TVS024)</b>	

## 11 Change Management

---

### Statement of Policy

To ensure that Company is tracking changes to systems, and workstations including software releases and software vulnerability patching in internal technologies developed and third-party systems. Change tracking allows the Information Technology (“IT”) Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

### Procedure

1. The IT staff or other designated Company employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
  - a. When changes are tracked within a system, i.e. Windows updates in the Add or Remove Programs component or iOS updates performed and logged by the vendor, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
  - b. When changes are performed within an internal technology developed by the Company, they will be logged and tracked by the Information Technology (“IT”) Department in the appropriate web-based systems designated by the CTO.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. 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.

<b>SH!FT</b>		<b>Policy and Procedure</b>	
<b>Title: AUDIT CONTROLS</b>		<b>P&amp;P #: IS-1.12</b>	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology (TVS013, TVS014, TVS019)</b>	

## 12 Audit Controls

---

### Statement of Policy

To ensure that Company implements hardware, software, and/or procedural mechanisms that record and examine activity in the internal technologies developed.

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.

The Company is committed to routinely auditing users' activities to continually assess potential risks and vulnerabilities to the internal technologies developed. As such, the Company will continually assess potential risks and vulnerabilities and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with International Information Security Rules.

### Procedure

1. See policy entitled Information System Activity Review for the administrative safeguards for auditing system activities.
2. The Information Technology Services shall enable event auditing on all the internal technologies developed that process, transmit, and/or store client's data for purposes of generating audit logs. Each audit log shall include, at a minimum: user ID, login time and date.
3. The Company shall utilize appropriate tracking systems for the matter, and it shall be responsible for installing, maintaining, and updating such systems.

<b>SHIFT</b>		<b>Policy and Procedure</b>	
<b>Title: INFORMATION SYSTEM ACTIVITY REVIEW</b>		<b>P&amp;P #: IS-1.13</b>	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology (TVS014, TVS017, TVS019)</b>	

## 13 Information System Activity Review

**Statement of 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, file access, security incidents, audit logs, and access reports. Company shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

**Procedure**

1. See policy entitled Audit Controls for a description of the technical mechanisms that track and record activities on Company’s information systems that contain or use client information.
2. The Information Technology Services shall be responsible for conducting reviews of Company’s 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.
3. The Security 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.
4. Such reviews shall be conducted annually. Audits also shall be conducted if Company has reason to suspect wrongdoing. In conducting these reviews, the Information Technology Services shall examine audit logs for security-significant events including, but not limited to, the following:
  - a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
  - b. 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.
  - c. 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 the report format referred to in Section 2 of this policy and procedure.

1. The Information Technology Services shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the Security Officer for review. The Security Officer shall be responsible for maintaining such reports. The Security Officer shall consider such reports and recommendations in determining whether to make changes to Company's administrative, physical, and technical safeguards.

<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title: DATA INTEGRITY</b>	<b>P&amp;P #: IS-1.14</b>	
<b>Approval Date:</b>	<b>Review: Annual</b>	
<b>Effective Date:</b>	<b>Information Technology (TVS012, TVS013)</b>	

## 14 Data Integrity

---

### Statement of Policy

Company shall implement and maintain appropriate electronic mechanisms to corroborate that client data has not been altered or destroyed in an unauthorized manner.

The purpose of this policy is to protect the data stored from Company's clients in all internal technologies developed, from improper alteration or destruction.

### Procedure

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

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

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

Company 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, Company will test its systems for accuracy and functionality before clients start to use them. Regarding third party systems used by personnel, the Company will update them when IT vendors release fixes to address known bugs or problems.

1. Company will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.
2. 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 hot summer months.

<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title: CONTINGENCY PLAN</b>	<b>P&amp;P #: IS-1.15</b>	
<b>Approval Date:</b>	<b>Review: Annual</b>	
<b>Effective Date:</b>	<b>Information Technology (TVS026)</b>	

## 15 Contingency Plan

### Statement of 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 clients` data.

Company is committed to maintaining formal Company's for responding to an emergency or other occurrence that damages systems containing clients `data. Company shall continually assess potential risks and vulnerabilities to protect the information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the International Security Rules.

### Procedure

1. Data Backup Plan

- a. Company, under the direction of the Security Officer, shall implement a data backup plan to create and maintain retrievable exact copies of client`s information in case of
- b. At the conclusion of each day, Monday through Friday, an incremental backup of all servers containing clients` data shall be backed. On Saturday, a full backup of all servers containing client`s data shall be backed up. The backup tapes are taken each week off site by the IS Manager or his/her designee to ensure safeguard of Company's data. One month of backup data will be maintained at all times in a remote location. Backup media that is no longer in service will be disposed of in accordance with the Disposal of External Media/Hardware policy.
- c. The Security Officer shall monitor storage and removal of backups and ensure all applicable access controls are enforced.
- d. The Security Officer shall test backup procedures on an annual basis to ensure that exact copies of clients` data can be retrieved and made available. Such testing shall be documented by the Security Officer. To the extent such testing indicates need for improvement in backup procedures, the Security Officer shall identify and implement such improvements in a timely manner.

2. Disaster Recovery and Emergency Mode Operations Plan

- a. The Security Officer shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:
  - i. Restoring or recovering any loss of data and/or systems necessary to make all technologies available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and



- ii. 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.
- b. The disaster recovery and emergency mode operation plan shall include the following:
  - i. Current copies of the information systems inventory and network configuration developed and updated as part of Company's risk analysis.
  - ii. Current copy of the backup procedures developed and updated pursuant to this policy.
  - iii. Identification of an emergency response team. Members of such team shall be responsible for the following:
    - 1. Determining the impact of a disaster and/or system unavailability on Company's operations.
    - 2. In the event of a disaster, securing the site and providing ongoing physical security.
    - 3. Retrieving lost data.
    - 4. Identifying and implementing appropriate "work-arounds" during such time information systems are unavailable.
    - 5. Taking such steps necessary to restore operations.
  - iv. Procedures for responding to loss of 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 Company's risk analysis
  - v. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:
    - 1. Members of the immediate response team,
    - 2. Facilities at which backup data is stored,
    - 3. Information systems vendors, and
    - 4. All current workforce members.
- c. The disaster recovery team shall meet on at least an annual basis to:
  - i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by Company;
  - ii. 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

- iii. Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

<b>SH!FT</b>		<b>Policy and Procedure</b>
<b>Title: SECURITY AWARENESS AND TRAINING</b>	<b>P&amp;P #: IS-1.16</b>	
<b>Approval Date:</b>	<b>Review: Annual</b>	
<b>Effective Date:</b>	<b>Information Technology (TVS006)</b>	

## 16 Security Awareness and Training

### Statement of Policy

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

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

### Procedure

- a. Security Training Program
  - i. The Security Officer shall have responsibility for the development and delivery of initial security training. All workforce members shall receive such initial training addressing the requirements of the International Security Rules. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation of all training activities.
  - ii. The Security 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 the data.
- b. Security Reminders
  - i. The Security Officer shall generate and distribute to all workforce members 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 may provide such reminders through formal training, e-mail messages, discussions during staff meetings, newsletters, etc. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.
  - ii. The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.
- c. Protection from Malicious Software

- i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:
  - a) Guidance on opening suspicious email attachments, email from unfamiliar senders, and hoax email,
  - b) The importance of checking a workstation or other device to determine if all protection is current,
  - c) Instructions to never download files from unknown or suspicious sources,
  - d) Recognizing signs of a potential threats that could sneak past protections established,
  - e) The importance of backing up critical data on a regular basis and storing the data in a safe place,
  
- d. Password Management
  - i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords:
    - a) Passwords must be changed every 60 days.
    - b) A user cannot reuse the last 12 passwords.
    - c) Passwords must be at least eight characters and contain upper case letters, lower case letters, numbers, and special characters.
    - d) Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.
    - e) A password must be promptly changed if it is suspected of being disclosed or known to have been disclosed.
    - f) Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to “fix” a computer or handle an emergency situation) or individuals, including family members.
    - g) Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
    - h) Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
    - i) Any employee who is directed by the Security Officer to change his/her password to conform to the aforementioned standards shall do so immediately.

<b>SH!FT</b>		<b>Policy and Procedure</b>	
<b>Title: SECURITY MANAGEMENT PROCESS</b>		<b>P&amp;P #: IS-1.17</b>	
<b>Approval Date:</b>		<b>Review: Annual</b>	
<b>Effective Date:</b>		<b>Information Technology</b>	

## 17 Security Management Process

### Statement of Policy

To ensure Company conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of clients’ data held by Company.

Company shall conduct an accurate and thorough risk analysis to serve as the basis for Company’s Information Security Rule compliance efforts. Company shall re-assess the security risks to its data management and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business Company’s and technological advancements.

### Procedure

- a. The Security Officer shall be responsible for coordinating Company’s risk analysis. The Security Officer shall identify the appropriate people within the organization to assist with the risk analysis.
- b. The risk analysis shall proceed in the following manner:
  - i. Document Company’s current information systems.
    - a) Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces, virtual workstations): date acquired, location, vendor, licenses, maintenance schedule, and function.
    - b) 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:
      - i) Describe the data associated with that application.
      - ii) Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.
      - iii) Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.
      - iv) Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period of time.

- v) Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.
  - vi) For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.
- e) Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of data created, received, maintained, or transmitted by Company. Consider the following:
- i) Natural threats, e.g., earthquakes, storm damage.
  - ii) Environmental threats, e.g., fire and smoke damage, power outage, utility problems.
  - iii) Human threats
    - a. Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls
    - b. Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment
    - c. Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail
    - d. External attacks, e.g., malicious cracking, scanning, demon dialing
  - iv) Identify and document vulnerabilities in Company's information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in unauthorized access to data, modification of data, 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.
- f) Determine and document probability and criticality of identified risks.
- i) Assign probability level, *i.e.*, likelihood of a security incident involving identified risk.
    - a. "Very Likely" (3) is defined as having a probable chance of occurrence.
    - b. "Likely" (2) is defined as having a significant chance of occurrence.
    - c. "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.
  - ii) Assign criticality level.
    - a. "High" (3) is defined as having a catastrophic impact on the Company including a significant number of data records which may have been lost or compromised.

- b. "Medium" (2) is defined as having a significant impact including a moderate number of data records within the Company which may have been lost or compromised.
      - c. "Low" (1) is defined as a modest or insignificant impact including the loss or compromise of some data records.
    - iii) 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.
  - g) 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.
  - h) 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 shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The Security 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 International Information Security Regulations; new governmental, or local laws or regulations affecting the security of data; changes in technology, environmental processes, or business processes that may affect International Information 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 virtual 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, Company shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement

<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title:</b> Emergency Operations Procedures (EHR outage)	<b>P&amp;P #:</b> IS-2.0	
<b>Approval Date:</b>	<b>Review:</b> Annual	
<b>Effective Date:</b>	<b>Information Technology</b> (TVS026)	

## 18 Emergency Operations Procedures

---

### Purpose

To provide procedures for managing data storage when systems are unavailable due to planned or unexpected outages.

### Definitions

SHIFT2: (Content Development System)

SHIFT SUAS: (User and Content Management System)

SHIFT Deploy (Mobile App)

SHIFT Reporter (Reports and Analytics System)

### Procedures

#### Notification:

The Information Systems or Technology Manager shall notify Company management as soon as practicable in the event of:

- planned downtime of all SHIFT Technologies and systems,
- unexpected outage of SHIFT Technologies and systems, and
- resumption of SHIFT Technologies and following an outage such that normal operations may resume.

#### Scheduling:

If any of the SHIFT Technologies systems is not operational or otherwise unavailable, the schedule printed the previous day is retrieved. The center manager is tasked with maintaining a copy of this schedule or assigning this duty as appropriate.

If phones are operational, client appointments may not be made. The operator should ask for pertinent contact information and record a message using the paper telephone encounter form.

#### System Restoration:

System restoration of all SHIFT Technologies to its corresponding client users, should undergo a procedure described in a specific document.



<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title: Sanction Policy</b> Security Violations and Disciplinary Action		<b>P&amp;P #:</b> IS-4.0
<b>Approval Date:</b>		<b>Review: Annual</b>
<b>Effective Date:</b>		<b>Human Resources</b> (TVS001)

## 19 Sanction Policy

### Policy

It is the policy of the Company that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Company will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization. The Company will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Company’s information security and privacy policies or confidentiality laws or regulations, including International Information Security regulations.

### Purpose

To ensure that there are appropriate sanctions that will be applied to workforce members who violate the requirements of the Company’s Information Security Policy, Directives, and/or any other governmental regulatory requirements.

### Definitions

*Workforce member* means employees, volunteers, and other people 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:

- Protected Client Information – Individually identifiable personal information that is in any form or media, whether electronic, paper, or oral.
- Electronic Protected Client Information – Electronic records generated from clients’ use of SHIFT Technologies.
- Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by the Company.
- Payroll data – Any information related to the compensation of an individual during that individuals’ employment with the Company.
- Financial/accounting records – Any records related to the accounting Company’s or financial statements of the Company.
- Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.

*Availability* refers to data or information is accessible and useable upon demand by an authorized person. *Confidentiality* refers to data or information 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.

### 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	<ul style="list-style-type: none"> <li>• Accessing information that you do not need to know to do your job.</li> <li>• Sharing SHIFT Technologies' access codes (username &amp; password).</li> <li>• Leaving computer unattended while being able to access sensitive information.</li> <li>• Disclosing sensitive information with unauthorized persons.</li> <li>• Copying sensitive information without authorization.</li> <li>• Changing sensitive information without authorization.</li> <li>• Discussing sensitive information in a public area or in an area where the public could overhear the conversation.</li> <li>• Discussing sensitive information with an unauthorized person.</li> <li>• Failing/refusing to cooperate with the Information Security Officer, Privacy Officer, Chief Information Officer, and/or authorized designee.</li> </ul>
2	<ul style="list-style-type: none"> <li>• Second occurrence of any Level 1 offense (does not have to be the same offense).</li> <li>• Unauthorized use or disclosure of sensitive information.</li> <li>• Using another person's access code (username &amp; password) for any of SHIFT Technologies' systems</li> <li>• Failing/refusing to comply with a remediation resolution or recommendation.</li> </ul>
3	<ul style="list-style-type: none"> <li>• Third occurrence of any Level 1 offense (does not have to be the same offense).</li> <li>• Second occurrence of any Level 2 offense (does not have to be the same offense).</li> <li>• Obtaining sensitive information under false pretenses.</li> <li>• Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.</li> </ul>

**Recommended Disciplinary Actions**

In the event that a workforce member violates the Company's privacy and security policies and/or violates International Information Security Regulations established in this policy or related governmental laws governing the protection of sensitive and client identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	<ul style="list-style-type: none"> <li>• Verbal or written reprimand</li> <li>• Retraining on privacy/security awareness</li> <li>• Retraining on the Company's privacy and security policies</li> </ul>

Violation Level	Recommended Disciplinary Action
	<ul style="list-style-type: none"> <li>• Retraining on the proper use of internal or required forms</li> </ul>
2	<ul style="list-style-type: none"> <li>• Letter of Reprimand*; or suspension</li> <li>• Retraining on privacy/security awareness</li> <li>• Retraining on the Company's privacy and security policies</li> <li>• Retraining on the proper use of internal or required forms</li> </ul>
3	<ul style="list-style-type: none"> <li>• Termination of employment or contract</li> <li>• Civil penalties as provided under applicable International Information Security Regulations and current governmental law</li> <li>• Criminal penalties as provided under applicable International Information Security Regulations and current governmental law</li> </ul>

**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, the Company 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 the Company.

**Related Policies**

Information Security Policy

**Acknowledgment**

I, the undersigned employee or contractor, hereby acknowledges receipt of a copy of the Sanction Policy for SHIFT Technologies (Aura Interactiva).

Dated this \_\_\_\_\_ day of \_\_\_\_\_, 20\_\_\_\_.

\_\_\_\_\_  
Signature of Employee/Contractor

<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title: EMPLOYEE BACKGROUND CHECKS</b>	<b>P&amp;P #: IS-4.1</b>	
<b>Approval Date:</b>	<b>Review: Annual</b>	
<b>Effective Date:</b>	<b>Human Resources (TVS007)</b>	

## 20 Employee Background Checks

The Company will conduct employment reference checks, investigative consumer reports and background investigations on all candidates for employment prior to making a final offer of employment and may use a third party to conduct these background checks. The Company will obtain written consent from applicants and employees prior to ordering reports from third-party providers and will provide a description of applicant and employee rights and all other documentation as required by law to each applicant or candidate in accordance with governmental and other applicable international regulations (Appendix G). All background checks are subject to these notice and consent requirements.

An investigative consumer report compiles information on a candidate's general reputation, personal characteristics, or mode of living. This information may be gathered online including social networking sites, through public or educational records, or through interviews with employers, friends, neighbors, associates, or anyone else who may have information about the employee or potential employee. In the pre-employment process, investigative consumer reports typically include such things as criminal records checks, education verification checks, and employment verification checks.

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

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

This information may also be sought out at other times during employment, such as during reassignment or promotional periods, and following safety infractions or other incidents.

The Company will conduct background checks in compliance with all applicable local, and international laws and regulations. Applicants and employees may request and receive a copy of requested "investigative consumer reports."

A reported criminal offense conviction will not necessarily disqualify a candidate from employment. The nature and seriousness of the offense, the date of the offense, the surrounding circumstances,

rehabilitation, the relevance of the offense to the specific position(s), and whether hiring, transferring, or promoting the applicant would pose an unreasonable risk to the business may be considered before a final decision is reached. The Company will follow international requirements, other applicable statutes, and Company procedures for providing information and reports, making decisions, and responding to applicants and employees regarding potentially adverse actions to an investigative report.

The Company reserves the right to withdraw any offer of employment or consideration for employment, or discharge an employee, upon finding falsification, misrepresentation, or omission of fact on an employment application, resume, or other attachments, as well as in verbal statements, regardless of when it is discovered.

Background check reports shall be maintained in separate, confidential files and retained in accordance with the Company's document retention procedures.

<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title: e-Discovery Policy</b> Production and Disclosure of Clients' Information and Records for e-Discovery		<b>P&amp;P #:</b> IS-5.0
<b>Approval Date:</b>		<b>Review: Annual</b>
<b>Effective Date:</b>		<b>Information Technology</b>

## 21 E-Discovery Policy: Production and Disclosure

### Policy

It is the policy of this organization to produce and disclose relevant information and records in compliance with applicable laws, court procedures, and agreements made during the litigation process.

### Purpose

The purpose of this policy is to outline the steps in the production and disclosure process for clients' information and records related to discovery for pending litigation.

### Scope

This policy addresses discovery production and disclosure procedures related to the pertinent rules and regulations. Client information and records include both paper and electronic data related to relevant records and enterprise sources.

### Procedure

#### Accurate Client Identification

Responsible	Action
HIM	For litigation involving an individual's records, verify the user's identity in the master client index, including demographic information and identifiers including the medical record number. <i>[Note: When conducting searches, it is critical to accurately identify the correct client and relevant information.]</i>
HIM	Note multiple medical record numbers, identifiers, aliases, etc., that will be used during the search process to find relevant information.

#### Subpoena Receipt and Response

Responsible	Action
Litigation Response Team	Upon receipt, subpoenas should be reviewed to determine that all elements are contained, the parties and the purpose are clearly identified, and the scope of information requested is clear. <ul style="list-style-type: none"> <li>• Validate the served subpoenas before official acceptance. The validation process includes at a minimum:</li> </ul>

Responsible	Action
Litigation Response Team, continued	<ul style="list-style-type: none"> <li>• Verification of appropriate service of the subpoena and that the organization is under legal obligation to comply with it, and</li> <li>• Verification that the seal and clerk of the court signature are present and valid</li> </ul> <p>Review of the venue and jurisdiction of the court for the case and verification that the court is located within legal distance/mileage requirements.</p>
HIM	Notify the Litigation Response Team that subpoena has been received and determine if a legal hold is in place. If not, the Litigation Response Team should determine whether a legal hold should be applied.
HIM	<p>If the subpoena requests “any and all records,” HIM and/or Legal Services should work with the judge and/or plaintiff’s attorney to clarify the scope and type of information being requested.</p> <p><i>[Note: The e-discovery process will identify vast volumes of data which can overwhelm a case; the parties should identify information that is necessary and relevant rather than providing all information.]</i></p>
Litigation Response Team/Legal Services	Provide direction to HIM in the processing of the subpoena, including the specific information to produce, agreed upon file formats and forms of production, whether an objection will be filed, timeframe to produce and disclose, and whether on-site testing/sampling will be conducted by the requesting party.
Litigation Response Team/Legal Services	If an outside firm is retained, such as outside counsel or discovery/litigation consultants, perform an analysis to determine if the contracted firm will have access to personal information and will need to sign a Business Associate Agreement with this organization. Execute Business Associate Agreement as appropriate.

**Search and Retrieve Process**

Responsible	Action
Litigation Response Team	<p>Identify the potential sources of information which may hold potentially relevant information, such as:</p> <ul style="list-style-type: none"> <li>• Local area servers for the office</li> <li>• Personal shares or personal folders on servers</li> <li>• Dedicated servers for the organization</li> <li>• Laptop and/or department computers</li> <li>• Home computers, PDAs, SmartPhones</li> <li>• E-mail, including archived e-mail and sent e-mail</li> <li>• E-mail trash bin, desktop recycle bin</li> </ul>
Litigation Response Team, continued	<ul style="list-style-type: none"> <li>• Text/instant message archives</li> <li>• Removable storage media (e.g., disks, tapes, CDs, DVDs, memory sticks and thumb drives)</li> <li>• Department/office files such as financial records</li> <li>• Personal desk files</li> <li>• Files of administrative personnel in department/office</li> <li>• Files located in department/office staff home</li> <li>• Web site archives</li> </ul>

Responsible	Action
HIM, Data Owners	Based on direction from the litigation response team on the potential locations of relevant information and the information agreed upon in the discovery plan and/or subpoena, establish search parameters (client identifiers, search terms, key words, etc.) and conduct the search process. Maintain a record of the systems searched, search methodology, search parameters (terms), and search results.
IT	Provide assistance to HIM and Data Owners in the search and retrieval process for various systems and data sources.
HIM, Data Owners	Screen or filter the search results, eliminating inappropriate information (e.g., wrong client, outside the timeframe, not relevant to the proceeding, etc.).
Legal Services	Review the content of the data/data sets found to determine relevancy to the proceeding and identify information that is considered privileged.
Legal Services, HIM, Data Owners	Determine the final list of relevant data/data sets, location, and search methodology.

**Production of Records/Data**

Responsible	Action
HIM, Data Owners, IT	Determine the format the information will be disclosed, such as: paper, ASCII, PDF, TIF, screen shot, mirror copy of data file, or review of material on-line. The format will vary depending on data, source, and agreement made in the Discovery Plan/Form 35.
HIM, Data Owners, IT	Produce the information in the agreed-upon format as outlined in the discovery plan/Form 35.
Legal Services, HIM, Data Owners, IT	Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different client) as appropriate.
Legal Services	Conduct final review of information before disclosing to requesting party.
Legal Services	Retain a duplicate of information disclosed to requesting party.

**Charges for Copying and Disclosure**

Responsible	Action
HIM, Data Owners, IT	For the information searched and disclosed, calculate the costs for search, retrieval, and disclosure methods using the organization's established formula and governmental formulas for reproduction charges.
HIM	Invoice requesting parties for allowable charges related to the reproduction of information and records.
Legal Services	Determine whether other expenses may be charged in accordance with the discovery plan or negotiation with litigants and/or judge.

**Testing and Sampling**



Responsible	Action
Legal Services	A party to the legal proceeding may request to test and sample the search and retrieve methodology. Testing and sampling should be discussed and agreed upon during the pretrial conference and part of the discovery plan, including whether an external party will test and sample the search and retrieve methodologies. The costs and charges should also be determined and negotiated.
HIM, Data Owners	Retain information on all searches; including methodology, key words, and systems used in case the methodology has to be recreated for testing purposes and to determine if the sample was statistically valid.
Litigation Response Team, HIM	Assign a monitor for the outside party during their testing protocols.

**Attorney/Third Party Request to Review Electronic Data**

Responsible	Action
Litigation Response Team	Determine the procedures for allowing an attorney or third party to review the electronic records and search results on-line. This includes where the review will occur, system access controls, monitoring during the review session, and the charges, if any.
Legal Services, IT, HIM, Data Owners	Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different client) as appropriate.
HIM, Data Owners	Verify the outside party is allowed access to the record and systems by reviewing all supporting documentation (e.g., signed consent, credentials from retained firm, etc.).
HIM, Data Owners	Prepare for access by identifying the types of information that party is allowed to access. If an authorization has been signed by a client or legal representative, allow access to legal medical records and/or other information as outlined in the authorization. If other types of information will be reviewed, access is allowed based on the subpoena, court order, state/federal statutes, or agreed-upon discovery plan.

**Responding to Interrogatories, Deposition, Court Procedures**

Responsible	Action
Legal Services	Legal Services manages the process for completion of the interrogatories and will coordinate processes related to depositions and testifying in court.
HIM (official record custodian)	HIM may provide information for an interrogatory, be deposed, or testify in court. HIM is the official custodian of the record and can testify whether the records were kept in the normal course of business and the authenticity of the records. In addition, HIM also addresses the good faith operations related to records management, retention/destruction, and the search and retrieval process/parameters.
IT (official system custodian)	IT may provide information for an interrogatory, be deposed, or testify in court. IT is the official custodian of the information system and may testify about the technical infrastructure, system architecture, security, source applications, and the good faith operations from a technical infrastructure perspective.

Responsible	Action
Data Owners	Data owners may provide information for an interrogatory, be deposed, or testify in court. The data owners may testify about the specific issues related to their department/business process area.
Primary/Direct Custodian	Primary/direct custodians may provide information for an interrogatory, be deposed, or testify in court. The primary/direct custodians are those person(s) who work with the data directly or have direct involvement/knowledge of the events the litigation. For example, a staff nurse who has made an entry into the medical record and is knowledgeable about the events of a case in litigation.
Business Associates/Third Parties	Business Associates/Third Parties may provide information for an interrogatory, be deposed, or testify in court. These include contractors and others who serve a variety of functions associated with a party's information but who themselves are not parties to the litigation. Examples include Internet service providers, application service providers such as a claims clearinghouse, and other providers who provide services ranging from off-site data storage to complete outsourcing of the IT Department.

**APPROVALS:**

Legal Department Approval:		Date:	
HIM Department Approval:		Date:	
IT Department Approval:		Date:	
		Date:	

<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title: e-Discovery Policy</b> Production and Disclosure of Clients' Information and Records for e-Discovery		<b>P&amp;P #:</b> IS-5.1
<b>Approval Date:</b>		<b>Review: Annual</b>
<b>Effective Date:</b>		<b>Information Technology</b>

## 22 E-Discovery Policy: Retention

---

### Policy

It is the policy of this organization to maintain and retain enterprise information and records in compliance with applicable governmental and regulatory requirements. This organization will adhere to retention schedules and destruction procedures in compliance with regulatory, business, and legal requirements.

### Purpose

The purpose of this policy is to achieve a complete and accurate accounting of all relevant records within the organization; to establish the conditions and time periods for which paper based and electronic information and records will be stored, retained, and destroyed after they are no longer active for business purposes; and to ensure appropriate availability of inactive records.

### Scope

This policy applies to all enterprise information and records whether the information is paper based or electronic.

### Definitions

*Data Owners:* Each department or unit that maintains client records, either in electronic or paper form, is required to designate a records management coordinator who will ensure that records in his or her area are preserved, maintained, and retained in compliance with records management policies and retention schedules established.

*Property Rights:* All enterprise information and records generated and received are the property of the organization. No employee, by virtue of his or her position, has any personal or property right to such records even though he or she may have developed or compiled them.

*Workforce Responsibility:* All employees and subcontractors are responsible for ensuring that enterprise information and records are created, used, maintained, preserved, and destroyed in accordance with this policy.

*Destruction of Enterprise Information and Records:* At the end of a 7-day period, each information and record retained as an encrypted backup, will be destroyed in accordance with the procedures in this policy unless a legal hold/preservation order exists or is anticipated.

*Unauthorized Destruction:* The unauthorized destruction, removal, alteration, or use of any information and records is prohibited. People who destroy, remove, alter or use information and records in an unauthorized manner will be disciplined in accordance with the organization's Sanction Policy.

### Procedure

Responsible	Action
Data Owner/Departments	Data owners/departments will designate records coordinator for their areas and report that designation to the Records Committee and Litigation Response Team.
Record Committee	The record committee's role is under the Information Security Officer's duties, where he/she is entitled to authorize any changes to the Retention, Storage, and Destruction policies and procedures; review and approve retention schedules and revisions to current retention schedules; address compliance audit findings; and review and approve control forms relating to business records.
HIM	<p>HIM will convene the Record Committee as needed and maintain responsibility for the following:</p> <ul style="list-style-type: none"> <li>● Review, maintain, publish, and distribute retention schedules and records management policies.</li> <li>● Audit compliance with records management policies and retention schedules and report findings to Record Committee.</li> <li>● Serve as point of contact for Records Coordinators.</li> <li>● Provide training for Records Coordinators. Training will be provided on an individual basis to Records Coordinators and any individual or department that needs assistance.</li> <li>● Oversee operation of designated offsite record storage center(s) for archival storage of information and records or serve as contract administrator for such services.</li> <li>● Contract for destruction of paper and electronic records and certification thereof.</li> </ul>
IT/HIM/Data Owners	IT/HIM/Data Owners will ensure that electronic storage of enterprise information and records is carried out in conjunction with archiving and retention policies.
Records Coordinators	<p>Records coordinators are responsible for implementing and maintaining records management programs for their designated areas.</p> <p>They will organize and manage online records management control forms relating to enterprise records and information in their areas of responsibility to accomplish the following:</p> <ul style="list-style-type: none"> <li>● Transfer records to storage</li> <li>● Identify, control, and maintain records in storage</li> <li>● Retrieve and/or return records from/to storage</li> <li>● Document the destruction of records and the deletion of records from the records inventory</li> <li>● Monitor the records management process</li> </ul> <p>Record coordinators will obtain (if not already trained) and maintain records management skills.</p>
Legal Services	<p>Legal Services serves as subject matter expert and provides counsel regarding records designations and legal and statutory requirements for records retention and pending legal matters.</p> <p>It ensures that access to or ownership of records is appropriately protected in all divestitures of property or lines of business or facility closures.</p>

**Guidelines for Retention of Records/Information and Schedules:**

Record Retention	Unless otherwise stipulated, retention schedules apply to all records. Records will only be discarded when the maximum specified retention period has expired, the record is approved for destruction by the record owner.
Non-record Retention	Non-records are maintained for as long as administratively needed, and retention schedules do not apply. Non-records may and should be discarded when the business use has terminated. For example, when the non-record information, such as an employee's personal notes, is transferred to a record, such as an incident report, the notes are no longer useful and should be discarded. Preliminary working papers and superseded drafts should be discarded, particularly after subsequent versions are finalized. Instances where an author or recipient of a document is unsure whether a document is a record as covered or described in this policy should be referred to the Compliance Officer for determination of its status and retention period.
Email Communication Retention	Depending on content, email messages between clients and the Company's staff as well as documents transmitted by email may be considered records and are subject to this policy. If an email message would be considered a record based on its content, the retention period for that email message would be the same for similar content in any other format. The originator/sender of the email message (or the recipient of a message if the sender is outside Organization) is the person responsible for retaining the message if that message is considered a record. Users must save email messages in a manner consistent with departmental procedures for retaining other information of similar content.

<p>Development of Records Retention Schedules</p>	<p>Retention Schedule Determined by Law: All records will be maintained and retained in accordance with national and international laws and regulations that apply to the nature of the Company’s work. <i>[Note: minimum retention schedules are attached to this policy]</i>. Electronic records must follow the same retention schedule as physical records, acknowledging the format and consolidated nature of records within an application or database.</p> <p>Changes to Retention Schedule: Proposed changes to the record retention schedules will be submitted to the Records Committee for initial review. The Records Committee, in consultation with the Legal Services Department, will research the legal, fiscal, administrative, and historical value of the records to determine the appropriate length of time the records will be maintained and provide an identifying code. The proposed revisions will be submitted to the Records Committee for review and approval. The approved changes will be published and communicated to the designated Records Coordinators.</p> <p>Retention of Electronic Records: Retention of records implies the inherent ability to retrieve and view a record within a reasonable time. Retained electronic data must follow guidelines established by the CTO and the Records Committee.</p> <p>Retention of Records in Large Applications: Retention of data for large-scale applications, typically those that reside in the data center and are accessed by a larger audience, shall be the responsibility of the CTO and the Technology department.</p> <p>Retention of Records on Individual Virtual Workstations: Primary responsibility for retention of data created at the virtual desktop level—typically with e-mail, Microsoft “Office” applications such as Word, Excel, PowerPoint, Access, or other specialized but virtually and saved in the cloud—shall be with the corresponding profile of the user/author. The user/author will ensure that the documents are properly named and saved to be recognizable by the user in the future.</p>
---------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Storage and Destruction Guidelines**

<p>Active/Inactive Records</p>	<p>Records are to be reviewed periodically by the Data Owner to determine if they are in the active, inactive, or destruction stage. Records that are no longer active will be stored in the designated off-site storage facility. Active stage is that period when reference is frequent and immediate access is important. Records should be retained in the office or close to the users. Data Owners, through their Records Coordinator, are responsible for maintaining the records in an orderly, secure, and auditable manner throughout this phase of the record life-cycle.</p>
<p>Active/Inactive Records, continued</p>	<p>Inactive stage is that period when records are retained for occasional reference and for legal reasons. Inactive records for which scheduled retention periods have not expired or records scheduled for permanent retention will be cataloged and moved to the designated off-site storage facility. Destruction stage is that period after records have served their full purpose, their mandated retention period, and finally are no longer needed.</p>
<p>Storage of Inactive Records</p>	<p>All inactive records identified for storage will be delivered with the appropriate Records Management Forms to the designated off-site storage facility where the records will be protected, stored, and will remain accessible and cataloged for easy retrieval. Except for emergencies, the designated off-site storage facility will provide access to records during normal business hours.</p>



Records Destruction	<p>General Rule: Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the Records Retention Schedules.</p> <p>Permanent Records: Records that cannot be destroyed include records of matters in litigation or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the record may be destroyed in accordance with the Records Retention Schedules but in no case shall records used in evidence to litigation be destroyed earlier than a specified number of years from the date of the settlement of litigation.</p> <p>Destruction of Records Containing Confidential Information: Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information unrecognizable. The approved methods to destroy records include: A Certificate of Destruction form must be approved and signed by the appropriate management staff prior to the destruction of records. The Certificate of Destruction shall be retained by the off-site storage facility manager.</p> <p>Destruction of Non-Records Containing Confidential Information: Destruction Non-Records containing personal information or other forms of confidential corporate, employee, member, or client information of any kind shall be rendered unrecognizable for both source and content by means of shredding, pulping, etc., regardless of media. This material shall be deposited in on-site, locked shred collection bins or boxed, sealed, and marked for destruction.</p> <p>Disposal of Electronic Storage Media: Electronic storage media must be assumed to contain confidential or other sensitive information and must not leave the possession of the organization until confirmation that the media is unreadable or until the media is physically destroyed.</p>
Records Destruction, continued	<p>Disposal of Electronic Media: Electronic storage media, such as CD-ROMs, DVDs, tapes, tape reels, USB thumb drives, disk drives or floppy disks containing confidential or sensitive information may only be disposed of by approved destruction methods. These methods include: CD-ROMs, DVDs, magneto-optical cartridges and other storage media that do not use traditional magnetic recording approaches must be physically destroyed.</p> <p>Disposal of IT Assets: Department managers must coordinate with the IT Department on disposing surplus property that is no longer needed for business activities according to the Disposal of IT Assets Policy. Disposal of information system equipment, including the irreversible removal of information and software, must occur in accordance with approved procedures and will be coordinated by IT personnel.</p>

**APPROVALS:**

Legal Department Approval:		Date:	
HIM Department Approval:		Date:	
IT Department Approval:		Date:	

<b>SHIFT</b>		<b>Policy and Procedure</b>
<b>Title: Reporting and Managing a Privacy Breach Procedure</b>	<b>P&amp;P #: IS-6.0</b>	
<b>Approval Date:</b>	<b>Review: Annual</b>	
<b>Effective Date:</b>	<b>Information Technology (TVS025)</b>	

## 23 Breach Notification Procedures

**Purpose**

To outline the process for notifying affected individuals of a breach of protected information under International Information Security rules and regulations.

**Scope**

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

**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.

Personally Identifiable Information – Information in any form that consists of a combination of an individual’s name and one or more of the following: Government identification number, driver’s license, personal code, security code, password, personal ID number, photograph, or other information which could be used to identify an 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.

**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 the Company 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 contact the Privacy Officer directly at his email or his Teams account
  - 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 the Company's 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 Company
    - 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 Company's
    - 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 the Company's 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 the Company's 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 – the Company's 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*

1. The Privacy Officer will work with the department(s) involved, the Company's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
2. 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 clients' data 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.
3. The required elements of notification vary depending on the type of breach and which law is implicated. As a result, the Company's Privacy Officer and Legal Counsel should work closely to draft any notification that is distributed.
  4. 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, the Company 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.
  5. Using multiple methods of notification in certain cases may be the most effective approach.

Business associates must notify the Company if they incur or discover a breach of unsecured client data.

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 the Company in investigating and mitigating the breach.
- 
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, the Company will be required to keep track of all breaches and to notify the privacy officer 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.

**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 the Company's Sanction Policy.

**Attachments**

Appendix E: Privacy Breach Assessment

**Related Policies**

IS-2.0 Sanction Policy

# Appendix A – Network Access Request Form

## Employee or Contractor Request for Network Access

EMPLOYEE/CONTRACTOR INFORMATION	
<input type="checkbox"/> New Employee <input type="checkbox"/> New Contractor <input type="checkbox"/> Existing User	Today's Date:
<input type="checkbox"/> Temporary	
First Name:	Last Name: <span style="float: right;">*MI:</span>
Position:	Department: Supervisor:
<input type="checkbox"/> Full-time <input type="checkbox"/> Part-time	Start date or Requested due date: Temporary or Contractor end date, if known:
SECURITY & EMAIL	
New Account:	
<input type="checkbox"/> Network Account <input type="checkbox"/> Email	
<input type="checkbox"/> Security/Email similar to what existing user:	
<input type="checkbox"/> Include in which E-mail Group(s):	<input type="checkbox"/> Remove from which E-mail Group(s):
<input type="checkbox"/> Include in which Security Group(s):	<input type="checkbox"/> Remove from which Security Group(s):
<input type="checkbox"/> Permit access to the following network location(s):	
Drive	Path      Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
Drive	Path      Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
Drive	Path      Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Miscellaneous Needs ( <i>Enter any other requests</i> ):	
EHR ACCESS	
<input type="checkbox"/> EHR Account	
Roles & Access:	
<input type="checkbox"/> Front Office	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Clinician	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Physician	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Accounting	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Records Management	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Reporting	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Administrator	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Other: Specify	Access: <input type="checkbox"/> Read-only <input type="checkbox"/> Read/write <input type="checkbox"/> Full Access <input type="checkbox"/> Remove Access
<input type="checkbox"/> Miscellaneous Needs ( <i>Enter any other requests</i> ):	
HARDWARE & SOFTWARE	
Hardware:	
<input type="checkbox"/> Laptop <input type="checkbox"/> Desktop <input type="checkbox"/> Either Laptop or Desktop	
<input type="checkbox"/> Screen protector	<input type="checkbox"/> Laptop bag <input type="checkbox"/> Cable lock
<input type="checkbox"/> Multifunction printer	<input type="checkbox"/> Netgear Router <input type="checkbox"/> Numeric keypad
<input type="checkbox"/> Standard inkjet printer	<input type="checkbox"/> Dual monitors <input type="checkbox"/> Docking station
<input type="checkbox"/> iPhone <input type="checkbox"/> iPad <input type="checkbox"/> Windows Mobile Device	
Software:	
<input type="checkbox"/> Adobe Acrobat (full version)	<input type="checkbox"/> Email Encryption

Nombre del Colaborador: \_\_\_\_\_ ID del Colaborador: \_\_\_\_\_

Firma: \_\_\_\_\_

Microsoft Office Professional 2003     Microsoft Office Professional 2007  
 MS Project 2007     MS Visio 2007     MS OneNote 2007  
 Fax Server - *Specify level of access:*  
 Miscellaneous Needs (*Enter any other requests*):

**TELEPHONY**

Telephone:  
 Desk Phone     Softphone (IP Communicator)  
 Desk phone currently exist at location. Current extension is:  
 Accessories:  
 Wireless headset                       Wired headset

**CELL PHONE / AIR CARD**

Cell phone     Air Card  
 Accessories:  
 Cell Phone Case/Holder     Car Charger  
 Miscellaneous Needs (*Enter any other requests*):

**BUILDING ACCESS**

Access Requested for the following location(s):  
 Medical Records Room               Server Room  
 Lobby                                               Other, *Specify:*  
 Additional Access Restriction:  
 After-Hours Access, *Specify Hours:*  
 Other Restrictions (be specific):

**SPECIAL INSTRUCTIONS**

Manager Checklist/Reminder:  
 - Signature below can be of the Department Head or the Data Owner if new network access is requested.  
 - Ensure employee badge is requested  
 - Schedule new employee orientation, if applicable  
 - Ensure name appears on any appropriate sign-in/out sheets  
 - Remember to have all new employees/contractors read and sign appropriate forms, i.e. Confidentiality Form (Appendix B)  
 - Request appropriate training/background:  
     o HR Background Investigation  
     o Security Training  
     o Any additional training and/or background check

NAME	SIGNATURE	DATE
<b>Department Head (Print Name)</b>		
<b>Privacy Officer / Appropriate Authority</b>		

## Appendix B – Confidentiality Form

---

### RESPONSIBILITY OF CONFIDENTIALITY

I understand and agree to maintain and safeguard the confidentiality of privileged information of SHIFT Technologies and Aura Interactiva. Further, I understand that any unauthorized use or disclosure of information residing on the Company information resource system may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Company/Firm

\_\_\_\_\_  
Date





\_\_\_\_\_  
Signature of Company  
Privacy Officer







## Appendix E – Incident Response Tools

Tool	Attached Form/Worksheet	Description
Security Incident Report	 Security_Incident-Report-Confidential.doc	Security incident report utilized by the reporting employee or witness to an incident or potential incident.
Security Incident Investigation	 Security_Incident-Investigation-Confident	Security incident investigation report that that allows for further investigation of a potential incident upon receipt of the initial security incident report.
Security Incident Log	 Security_Incident-Logging-Confidential.xls	Security incident log to ensure incidents are tracked for further analysis and follow-up.
Security Breach Assessment Tool	 Security_Incident-Breach Assessment-Cor	Privacy breach assessment tool which can assist in determining the severity of a breach.

## Appendix F – Background Check Authorization

### AUTHORIZATION AND RELEASE TO OBTAIN INFORMATION

Under all applicable international information security laws and regulations, I hereby authorize and permit to obtain a consumer report and/or an investigative consumer report which may include the following:

1. My employment records;
2. Records concerning any driving, criminal history, credit history, civil record, workers' compensation (post-offer only), and drug testing;
3. Verification of my academic and/or professional credentials; and
4. Information and/or copies of documents from any military service records.

I understand that an "investigative consumer report" may include information as to my character, general reputation, personal characteristics, and mode of living, which may be obtained by interviews with individuals with whom I am acquainted or who may have knowledge concerning any such items of information.

I agree that a copy of this authorization has the same effect as an original.

I understand that information obtained in this authorized investigative consumer report and background investigation may result in not being offered a position of employment. I hereby release and hold harmless any person, firm, or entity that discloses information in accordance with this authorization, as well as from liability that might otherwise result from the request for use of and/or disclosure of any or all of the foregoing information except with respect to a violation of the Act. I authorize SHIFT Technologies and Aura Interactiva ("Company") and its designated agent and all associated entities to receive any criminal history information or credit report pertaining to me in the files of any state or local criminal justice agency. I authorize all corporations; companies; former employers; supervisors; credit agencies; educational institutions; law enforcement/ criminal justice agencies; city, state, county and federal courts; state motor vehicle bureaus; and other persons and entities to release information they may have about me to the Company or their designated agent.

I hereby authorize the Company to obtain and prepare an investigative consumer report and background investigation as set forth above, as part of its investigation of my employment application. This authorization shall remain in effect over the course of my employment. Reports may be ordered periodically during the course of my employment such as during reassignment or promotional periods and following safety infractions or other incidents.

I understand and acknowledge that I may request a copy of any consumer report from the consumer reporting agency that compiled the report, after I have provided proper identification. As part of a routine background investigation, we may request a consumer credit report from a consumer credit reporting agency or one of its associated companies. If we do so and you wish them to send you a free copy of this consumer credit report, please check here: \_\_\_\_\_.

My signature below also indicates that I have received a [Summary of Rights](#) in accordance with the Fair Credit Reporting Act.

Date \_\_\_\_\_

Applicant's Signature \_\_\_\_\_

Applicant's Printed Name \_\_\_\_\_

Other Names Used \_\_\_\_\_

Social Security Number \_\_\_\_/\_\_\_\_/\_\_\_\_ Date of Birth \_\_\_\_\_

Driver's License # \_\_\_\_\_ State \_\_\_\_\_

Current Address \_\_\_\_\_

City/Town \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_

Previous address \_\_\_\_\_

City/Town \_\_\_\_\_ State \_\_\_\_\_ Zip Code \_\_\_\_\_



# Appendix H – Employee Hiring and Termination Checklist

Employee Hiring and Termination Checklist							
Company:				Starting Date of Employment:			
Employee Name:				Ending Date of Employment:			
Type of Termination:							
System/Device	System/Device Description <i>(Examples in Italics)</i>	Access Type	Access Granted?	Access Granted By:	Date Access or Device Provided	Access Removed By:	Date Access or Device Removed
Facility	<i>Physical Access to Building and List of Accessible Areas</i>						
Network	<i>Windows Active Directory, Novell, Unix, etc.</i>						
Email	<i>Outlook, Google, AT&amp;T, etc.</i>						
Clinical Documentation	<i>EHR Vendor and Application</i>						
Practice Management	<i>Vendor and Application</i>						
Office Software	<i>Product, Version, and Components (i.e. Microsoft Word, Excel, Outlook, etc.)</i>						
Laptop/Tablet	<i>Manufacturer and Model No.</i>						
Cellular/Smart Phone	<i>Manufacturer and Model No.</i>						
PDA	<i>Manufacturer and Model No.</i>						
Flash Drive	<i>Manufacturer, Size and Encryption</i>						
Comments:							



Hire&TerminationChecklist.xls