Title	Acceptable Use of Information Systems Policy
Policy Number	ORG.1030.000.000
Initiating Authority	Information Technology Department
Approved By	Compliance Committee 2-23-22
Origin Date	January 2022
Revision Date	
Effective Date	March 1, 2022
Next Review Date	August
Associated Policies	
Associated Procedures	
Associated Documents	

I. POLICY STATEMENT

Information systems are a growing and important resource for Shadowfax staff members, one that can provide critical competitive advantage to Shadowfax in the form of information gathering, improved external communications, and increased customer responsiveness. As more and more of our staff members use information systems to connect with our individuals, customers, suppliers and other key organizations, it is important that Shadowfax staff members understand and agree on the appropriate procedures to protect Shadowfax's assets.

II. PURPOSE

This policy provides useful guidelines and techniques to promote effective use of Shadowfax's information systems. It applies to all Shadowfax systems located on or accessed from Shadowfax property and systems provided by Shadowfax for use in Shadowfax business.

III. SCOPE

This policy applies to all Shadowfax staff members that have access to Shadowfax's information resources.

Note: The term "Individual" is synonymous with resident, client, patient, consumer, or participant.

IV. GENERAL

Shadowfax utilizes sophisticated computer and communications systems to assist staff members in performing their job functions. These technologies support our business activities by enabling closer, more effective and timely communications among personnel within Shadowfax and with our individuals, customers, partners and vendors worldwide. These guidelines advise all users regarding the access to and the disclosure of information systems. These guidelines establish Shadowfax's expectations for all staff members concerning the disclosure of information via Shadowfax's information systems.

V. POLICY

Shadowfax maintains and uses many facilities, equipment, and communication systems, such as telephones, regular mail, electronic-mail, voice mail, fax machines, computers, etc., designed to make Shadowfax's operations effective and efficient. Shadowfax's information systems are provided to staff members at Shadowfax expense to assist staff members in carrying out Shadowfax business. Some of these systems permit staff members to communicate with each other internally and with other parties externally. As with all Shadowfax assets, Shadowfax's information systems are for official Shadowfax business only. Access to Shadowfax information systems is provided in conjunction with the official Shadowfax business and individual job responsibilities. Use of Shadowfax's information systems is subject to these policies and guidelines and other relevant Shadowfax policies and procedures.

A. INFORMATION ACCESS, CONTENT, AND USE

Shadowfax makes every effort to provide its staff members with the best technology available to conduct Shadowfax's official business. Shadowfax has installed information Resources to conduct its official business.

This document addresses general information systems policies and guidelines, specific issues related to appropriate content, and staff members use of Shadowfax's information systems. All departments and staff members are required to follow these general policies and guidelines. All Shadowfax staff members with access to Shadowfax's information systems are required to read, understand and comply with Shadowfax's policies.

Shadowfax's information systems are owned by Shadowfax and are to be used for business purposes only in serving the interests of Shadowfax's individuals, customers and in the course of normal business operations.

The use of Shadowfax facilities, property, equipment, and/or communication systems is limited to Acceptable Use as defined in these policies and guidelines. No Shadowfax equipment or communications systems, including all hardware and software, may be removed from Shadowfax property without prior expressed consent of a Shadowfax Director and/or Manager. Laptops and cell phones given to Shadowfax staff for business purposes may be taken from Shadowfax property for business use.

Personal equipment, including all computer hardware and software, may not be brought onto Shadowfax premises or be used for Shadowfax's official business without the prior expressed consent of a Shadowfax Director and/or Manager. Staff members are not to use their personal accounts during work hours or use Shadowfax equipment to reach personal sites unless it is for legitimate business purposes, as determined solely by Shadowfax.

Shadowfax encourages the use of Shadowfax's information systems for business when such business can be accomplished consistent with the following policies and guidelines identified in this document. When using information systems, staff members shall conduct official Shadowfax business consistent with Shadowfax's mission statement. Official Shadowfax business shall comply with all federal and state statutory requirements as well as standards for integrity, accountability, and legal sufficiency. Thus, official Shadowfax business conducted via the internet should meet or exceed the standards of performance for traditional methods (i.e., meetings, use of telephone).

Staff members shall base decisions to use Shadowfax's information systems on sound business practices. The conduct of business using Shadowfax's information systems is particularly compelling where costs are reduced and/or the services provided by Shadowfax are improved in measurable ways. When using Shadowfax's information systems, Shadowfax staff members shall promote and maintain a professional image.

Shadowfax staff members shall disseminate information that is current, accurate, complete, and consistent with Shadowfax policy. Information released via Shadowfax's information systems is subject to the same official Shadowfax policies for

Note: The term "Individual" is synonymous with resident, client, patient, consumer, or participant.

the release of information via other media (such as printed documents), so that the information disclosed avoids potential problems with copyrights, trademarks, and trade secrets. Information accuracy is particularly important.

Shadowfax staff members shall protect confidential and proprietary information entrusted to Shadowfax. Questions regarding confidential or proprietary information should be directed to Shadowfax management or their designee.

B. PROTECTING CONFIDENTIAL INFORMATION

Maintaining the confidentiality of sensitive information is crucial to Shadowfax's success. Confidential information stored on or carried over Shadowfax's information systems could become the subject of accidental or intentional interception, mis-delivery, hacking or even unauthorized internal review, unless staff members take the necessary precautions outlined in these guidelines.

Shadowfax has developed specific procedures to ensure the protection of confidential information. Staff members should exercise care when communicating any potentially confidential information outside of Shadowfax, as no electronic communications facility is completely secure.

All confidential data should be marked with "Confidential," "Do not reproduce," "Not to be reproduced without approval," or "Do not forward." All external email messages containing confidential information should be encrypted and contain "Secure" in the subject header.

Some directories in Shadowfax's information systems contain sensitive or confidential data. Access to these directories shall be restricted. Unauthorized attempts to circumvent such access restrictions are violations of these guidelines and may result in disciplinary action, up to and including termination of employment, and legal action.

Staff members must refrain from entering into discussions with third parties regarding Shadowfax's business prospects or financial condition. Staff members should not discuss future products, services, features or functionality unless Shadowfax has previously disclosed such information in a press release or through some other public disclosure. Such information is proprietary to Shadowfax and constitutes valuable information that should be protected as a trade secret. The release of such information could become the subject of criminal prosecution.

Staff members are asked to respect the privacy of individuals who send them messages. Staff members should protect voice mail, and email accounts from unauthorized access. Appropriate protection procedures include ensuring proper password protection to these accounts, closing email messages after reading them and deleting all messages when they are no longer needed.

Staff members shall not place Shadowfax material (e.g., copyrighted software, internal correspondence) on any publicly accessible internet computer without prior permission.

The internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the internet may be at risk of detection by a third-party. Staff members must exercise caution and care when transferring such material in any form.

C. COPYRIGHTED INFORMATION

Shadowfax respects the intellectual property rights of other companies and individuals. Use of all copyrighted material, including literature, software, and graphics shall comply with relevant, valid license terms. Shadowfax's information systems may provide access to materials protected by copyright, trademark, patent and trade secret and even export laws. Staff members should not assume that merely because information is available on an electronic information system such as the internet, that it may be downloaded or further disseminated. No copyrighted material should be copied, transmitted, posted, or otherwise distributed without such compliance. If a question arises as to the propriety of downloading information, Shadowfax management should be consulted.

All material trademarked or copyrighted by Shadowfax should be marked with the appropriate trademark or copyright designation. No Shadowfax staff member should remove trademark and copyright notices from third party material.

Shadowfax's license to use software is carefully set forth in legal agreements that Shadowfax has with the developers and distributors of the software. Staff members' use of software must be in compliance with those agreements. If Shadowfax gives staff members the opportunity to use certain software, copying of that software is strictly prohibited. Loading of software of a personal interest is prohibited unless staff members are given prior expressed consent by Shadowfax management. When staff members leave Shadowfax, all Shadowfax owned software, licenses, and media will remain with Shadowfax.

Note: The term "Individual" is synonymous with resident, client, patient, consumer, or participant.

Unless otherwise noted, all software on the internet should be considered copyrighted work. Therefore, staff members are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.

D. Privacy Statement

This policy is intended to guide staff members in the performance of their duties. It is also intended to place staff members on notice that staff members should not expect Shadowfax's information systems and their contents to be confidential or private. All data, including any that is stored or printed as a document, is subject to audit and review.

No staff members should have a reasonable expectation of personal privacy with respect to the use of any of the Shadowfax's facilities, property, equipment or communications systems. This includes anything created or received on Shadowfax's information systems even if used for business purposes and in the normal course of Shadowfax operations.

Shadowfax reserves the right, but not the obligation, to monitor use of Shadowfax's information systems including the internet, email, computer transmissions, and electronically stored information created or received by Shadowfax staff members with the Shadowfax's information systems. All computer applications, programs, work-related information created or stored by staff members on Shadowfax's information systems are Shadowfax property.

E. Monitoring and Inspecting Information Systems

Shadowfax's information systems are provided for official Shadowfax business. Shadowfax's information systems are owned and controlled by Shadowfax and are accessible at all times by Shadowfax for maintenance, upgrades and other business or legal purposes.

All information systems, including the messages and data stored on the systems, are and remain at all times the property of Shadowfax, subject to applicable third-party intellectual property rights such as copyrights. By virtue of continued employment and use of Shadowfax systems, all staff members are considered to have consented to monitoring and other access by authorized Shadowfax personnel. Shadowfax reserves the right to inspect a staff member's computer system for violations of Shadowfax policies.

Shadowfax reserves the right to access and conduct an inspection or search all directories, indices, diskettes, files, databases, faxes, Shadowfax computer hardware and software, voice mail, email and communication systems or deliveries sent to any Shadowfax location, no matter to whom it is addressed, with no prior notice. Shadowfax may also cancel or restrict any staff member's privilege to use any or all of its facilities, equipment, property, or communication systems.

If a staff member refuses to cooperate with a search or inspection for legitimate business purposes that is based on reasonable suspicion that the staff member is in possession of prohibited materials, Human Resources (HR) may take that refusal into consideration in determining appropriate disciplinary action. A staff member's refusal to provide their password to Shadowfax management will be considered additional grounds for discipline. Discipline, including termination, will be based on all available information, including the information giving rise to the inspection or search.

Access to on-line services, the internet, bulletin board services or other communications networks is prohibited unless Shadowfax has provided prior expressed consent. As such, no Shadowfax equipment, telephone lines, or on-line services may be used to view or download offensive, discriminatory or pornographic material. Staff member use of these services may be monitored to include numbers called and the amount of time spent using the services. Shadowfax reserves the right to inspect computer systems for viruses, offensive, discriminatory or pornographic material, personal software, etc.

Shadowfax management may examine staff member communications or files and such examination should be expected to occur in various circumstances when necessary, including, but not limited to:

- Ensuring that Shadowfax systems are not being used to transmit discriminatory, harassing or offensive messages of any kind.
- Determining the presence of illegal material or unlicensed software.
- Ensuring that communication tools are not being used for unauthorized, disruptive, or improper uses.
- Investigating allegations or indications of impropriety.
- Locating, accessing and/or retrieving information in staff members absence.
- Responding to legal proceedings and court orders in the preservation or production of evidence.

Note: The term "Individual" is synonymous with resident, client, patient, consumer, or participant.

- Shadowfax reserves the right to review the staff members use of and to inspect all material created by or stored on Shadowfax information systems. Shadowfax reserves the right to monitor all use of information systems to access, review, copy, delete, or disclose messages and data derived from any use. All messages or data become property of Shadowfax, subject to access, review, duplication, deletion, or disclosure by Shadowfax management or by other personnel authorized by Shadowfax. Staff members should be aware that billing practices, firewall protections, and traffic flow monitoring programs often maintain detailed audit logs setting forth addresses, times, durations, etc. of communications both within and external to the Shadowfax. Staff members should treat Shadowfax's information systems with the expectation that communications will be available for review by authorized personnel of Shadowfax for legitimate business purposes at any time.

Shadowfax reserves the right to access, review, duplicate, delete or disclose for legitimate business purposes any communications, messages or data derived from use of Shadowfax's information systems.

F. Storing and Archiving Information

Shadowfax has developed specific archival procedures to ensure the safe retention of electronic data. Most files are subject to routine back-up procedures. Copies of documents and electronic messages may be retained for long periods of time. By virtue of various archival practices employed at Shadowfax, any messages or data stored, even temporarily, on Shadowfax information systems may be copied to magnetic or other storage media without the specific knowledge of the individual creating the messages or data. Such archives are and remain Shadowfax property and may be used by Shadowfax for any business purpose. Simply deleting messages or data from these information systems does not provide privacy with regard to such messages or data. The length of time that such archives may be maintained can be almost indefinite. Staff members may be required to preserve their electronic data based on pending litigation and/or investigations by the Shadowfax. Refer to the Information Technologies (IT) department for additional information on storing and archiving information.

G. Employee Usage

Each staff member has the responsibility of complying with Shadowfax's policies and guidelines provided in this document. Failure to do so may result in disciplinary action, up to and including termination of employment and legal action.

The use of information systems is restricted to official Shadowfax business. Personal use of or time spent for personal gain is strictly prohibited unless Shadowfax gives prior express consent. Inappropriate personal use includes the creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials, materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited. In addition, any internet use that could cause congestion, disruption of normal service, or general additional Shadowfax expense is prohibited.

Hacking or unauthorized attempts or entry into any other computer is forbidden. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.

Sending threatening, slanderous, racially and/or sexually harassing messages is strictly prohibited. The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited.

Staff members should be aware that Shadowfax's information systems and the World Wide Web are not censored and contain information some users may find offensive. Shadowfax cannot accept responsibility for what the staff member accesses; however, if offensive material is accessed, staff members shall disengage from the material immediately.

Staff members shall not copy or transfer electronic files without prior Shadowfax permission. Almost all software is subject to Federal copyright laws. Care should be exercised whenever accessing or copying any information that does not belong to staff members. When in doubt, consult Shadowfax management. Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on Shadowfax's information systems in a manner inconsistent with relevant license terms or other intellectual property rights.

Downloading a file from the internet can infect Shadowfax's systems with a virus. Staff members shall not circumvent or disable Shadowfax standard virus prevention software and/or information Resource security mechanisms.

Staff members shall not send, post or provide access to any confidential Shadowfax materials or information to anyone outside of Shadowfax.

Staff members are obligated to cooperate with any investigation regarding the use of staff member's computer equipment and for which Shadowfax management has authorized.

Alternate internet Service Provider connections to Shadowfax's internal network are not permitted unless prior express consent has been given by Shadowfax management and properly protected by a firewall or other appropriate security device(s).

If staff members are using information from an internet site for strategic official Shadowfax business decisions, staff members should verify the integrity of that information. Staff members should verify whether the site is updated on a regular basis (the lack of revision date might indicate out-of-date information) and that it is a valid provider of the information.

Shadowfax has no control or responsibility for content on an external server not under the control of the Shadowfax. Information may be offensive and/or unsuitable for dissemination.

Do not upload or download large files during prime hours due to the network impact on other users. Information systems may have limits regarding disk space usage. Documents take up space; therefore, staff members should regularly delete and/or archive any files they wish to save.

Staff members using Shadowfax's accounts are acting as representatives of Shadowfax. As such, staff members should act accordingly so as not to damage the reputation of Shadowfax.

In order to maintain confidentiality of all information and records, no person, including but not limited to, Shadowfax employees, visitors, individuals, customers, vendors,

should record conversations of another without his or her prior knowledge and consent. Recordings include audio and/or video by any means, including smart phones.

The devices used to record via audio or video that are prohibited are inclusive of, but are not limited to, phones, smart phones, voice recorders of any kind, video cameras of any kind, and microphones.

Any staff member requesting to record via audio or video any interaction with any employee of Shadowfax will need to inform Human Resources of their intention and obtain authorization. Shadowfax reserves the right to refuse such request, at their sole discretion.

Phone and Voice Mail

Shadowfax IT department provides and maintains the phone system, including voice mail to assist you in the conduct of business within the company. All telephone hardware is company property. All communication messages composed, sent or received on the telephone are and will remain the property of Shadowfax. They are not private property of the employee.

Shadowfax approves limited, occasional or incidental non-business use of the telephone if done in a professional manner that does not interfere with business use, does not incur any additional cost to the company, and complies with the rest of the Acceptable Use Policy.

Prohibited actions include, but are not limited to, any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability or any other legal activity.

Each user is required to setup, maintain and use a pass code for secure voice mail access.

Shadowfax reserves the right to review, audit, intercept, access, and disclose all messages created, received or sent over the voice mail system for any purpose. The contents of the voice mail may be disclosed within Shadowfax without the permission of the staff member.

Internet and Network Security

Shadowfax provides and maintains access to the internet to assist you in the conduct of business within the organization. All messages/data received through the internet are Shadowfax property.

Shadowfax approves limited, occasional or incidental non-business use of the internet if done in a professional manner that does not interfere with business use, does not incur any additional cost to the company, and complies with the rest of the Acceptable Use Policy.

Prohibited actions include, but are not limited to, any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability or any other legal activity.

Without proper prior authorization, the internet shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary business, financial information or similar materials.

Shadowfax reserves the right to review, audit, intercept, access and disclose all internet transactions created, received, or sent over the internet. The contents of the voicemail may be disclosed within Shadowfax without the permission of the staff member.

Information Technology (IT) requires each user to setup, maintain and use personal and confidential passwords to protect files, retrieved stored information, and "lock down" workstations.

No staff member should attempt to gain access to another staff member's passwords or documents without permission or authorization.

H. Information Systems Awareness

The use of information systems is the responsibility of each staff member. The practices listed below are not inclusive, but rather designed to remind each staff member of the need to raise their information systems awareness.

- Protect equipment. Keep it in a secure environment and keep food and drink from electronic systems. Know where the fire suppression equipment is located and how to use it in an emergency.
- Protect areas. Keep unauthorized people away from equipment and data. Challenge strangers in the area
- Protect passwords. Never write it down or give it to anyone. Don't use names, numbers or dates that are personally identified with the staff members. Change the password often and change it immediately if it has been compromised.
- Protect files. Don't allow unauthorized access to staff members' files and data. Never leave equipment unattended with the password activated – log off.
- Backing up data. Keep duplicates of critical data in a safe place.
- Report security violations. staff members should tell their supervisor or Shadowfax management if they notice any unauthorized changes to their data. Immediately report any loss of data or programs, whether automated or hard copy.

I. ELECTRONIC MAIL (EMAIL)

Email may be sent through each staff member's computer. Email will be sent for official Shadowfax business only. No personal email shall be sent or received via Shadowfax internet accounts.

Shadowfax provides and maintains an email system to assist you in the conduct of business within the organization. Messages/data composed, sent or received on the email system are and will remain the property of Shadowfax regardless of means or transmission. The messages and data are not private property of the staff member.

Shadowfax approves limited, occasional or incidental non-business use of the email system if done in a professional manner that does not interfere with business use, does not incur any additional cost to Shadowfax and complies with the rest of this Acceptable Use Policy.

The email system may not be used at any time to solicit or promote commercial ventures, religious or political causes, outside organizations, or other non-company approved solicitations. No company-wide distribution of non-company business information or chain letters is permitted.

Email should present an image to promote and maintain the ethical standards of the Shadowfax's mission statement

Note: The term "Individual" is synonymous with resident, client, patient, consumer, or participant.

The email system is not to be used to create or repeat any harassment, offensive or disruptive messages or any other legal activities in the course of business or personal use.

Prohibited actions include, but are not limited to, any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability or any other legal activity.

Shadowfax reserves the right to review, audit, intercept, access and disclose messages/data created, received or sent over the email or data system for any purpose. The information may be disclosed within the organization without the permission of the staff member.

Staff members may not post information to electronic bulletin boards, social networking sites or similar public posting forums on the internet or create email that may be detrimental to Shadowfax or may damage the reputation of a staff member, Individual or the organization.

Encrypted – Email
Email encryption is the process of converting plain text (the original message and attachments) to cipher text and serves the function of maintaining confidentiality.

This is to secure sensitive data sent by email transmission outside the organization. Shadowfax has licensed the shadowfax.org domain with email Encryption software for all Shadowfax staff members ("Users"). This is to provide for the secure transmission of protected health information (PHI) and other sensitive data when Emailed to minimize the risk of a breach of confidentiality and the potential misuse, disclosure or theft of such information.

Shadowfax staff approved to share sensitive data and PHI externally shall be trained in the use of email Encryption Software and shall use the email Encryption Software when sending any email (with or without attachments) which contains Sensitive Data and Protected Health Information (below).

***Sensitive Data*:** protected health information, social security numbers, credit card numbers, financial account numbers, and other information protected by HIPAA.

Note: The term "Individual" is synonymous with resident, client, patient, consumer, or participant.

Protected Health Information: Protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service, such as diagnosis or treatment.

Violation of this policy will be reviewed on a case-by-case basis by the IT Department and Human Resources, with consequences recommended to management of the staff member, including termination of employment, additional penalties and charges to the full extent of the law applicable to the offense.

The following disclaimer shall be appended to all out-going email messages:

NOTICE OF CONFIDENTIAL INFORMATION
The information in this communication belongs to THE SHADOWFAX CORPORATION. It contains confidential, legally privileged information that is intended only for the use of the above-named addressee, who may not disclose it to any other person, except as allowed by law. If you are not the intended recipient, you are hereby informed that any use, disclosure, distribution, or copying of this communication or any part thereof is strictly prohibited and unlawful. If you have received this communication in error, please notify the sender immediately and remove it from your system.

Email users are to exercise good judgment and common sense when creating and distributing messages. Email is the property of Shadowfax and is to be used exclusively for official Shadowfax business. No staff member's email is considered private. Similarly, the accessing, reading or copying of email not intended for a staff member's eyes is prohibited. Staff members are strictly prohibited from sending email messages of a harassing, intimidating, offensive or discriminatory nature. Anonymous messages are not to be sent. Staff members are prohibited from using aliases while connected to services. Shadowfax retains the right to access a staff member's email at any time, for any reason, without notice to the staff member. Conduct in violation of this policy will subject the staff member to Shadowfax's disciplinary procedures.

J. SECURING INFORMATION SYSTEMS WITH PASSWORDS

Prior express consent for information systems access must be obtained through Shadowfax management. Contractors performing Shadowfax work shall only be given access to the network after written communication and approval by Shadowfax management. Once Shadowfax provides prior expressed consent, staff members shall be responsible for the security of their account password and will be held responsible

for all use or misuse of their account. No other password or security device shall be used without approval by Shadowfax management.

Each Shadowfax information System may allow staff members to set or change their password. If so, set the password and change it regularly. Guidelines for selecting and choosing passwords should be obtained from the IT department for password adherence standards. Periodic password changes keep undetected intruders from continuously using the password of a legitimate user. After logging on, the computer will attribute all activity to a staff member's User ID. Therefore, never leave workstations without logging off -- even for a few minutes. Always log off or otherwise inactivate the workstation so no one could perform any activity under staff member's User ID when away from the area. Staff members should safeguard sensitive information from disclosure to others.

If requested, staff members shall disclose their passwords (i.e., voice mail, email, relevant internet web site passwords) to their supervisor and/or manager. staff members must maintain secure passwords and never use an account assigned to another user.

Shadowfax reserves the right to override the user's password and other security features when it has a need to do so. Should a time come when staff members leave Shadowfax, or at any other appropriate time, Shadowfax may replace a staff member's password with another of Shadowfax's choosing.

K. Protecting Information Systems From Viruses

Shadowfax provides virus protection software to help safeguard information systems. These systems are not totally foolproof. As such, be particularly cautious when opening any email with an attachment.

Staff members shall not disable or remove anti-virus software. Viruses can infect executable files, disk boot sectors, documents, etc. If a virus is received from a sender, that sender should be notified that the file was infected and if possible, the type of virus should be identified.

L. Encrypting Data

Only authorized encryption tools (both software and hardware) may be used in connection with information systems. Except with the prior written consent of

Shadowfax management, all encryption tools must permit Shadowfax to access and recover all encrypted information.

M. SECURING MOBILE COMPUTING DEVICES

Staff members who use Shadowfax mobile computing resources (i.e., laptops, handheld devices, etc.) must take adequate precautions to ensure that proprietary information contained in such devices is secure and not available to third parties, particularly during travel. staff members are responsible for taking adequate precautions against theft of their mobile computing devices. Please discuss with IT on bringing your own device in regard to technology for additional information and standards.

N. ACCEPTABLE USE

- **Authorized Use.** The authorized use of Shadowfax systems is limited to Shadowfax's official business. Shadowfax provides information systems and communication tools to facilitate business communication and enhance personal productivity. Shadowfax reserves the right to prohibit or restrict use of Shadowfax systems for any other purpose and at any time.
- **Incidental Personal Use.** Personal use of Shadowfax systems is permitted so long as it is not excessive as determined by Shadowfax, does not interfere with job performance, consume significant resources, or interfere with the activities of other staff members.

O. UNACCEPTABLE USE

- **Unauthorized Use.** Excessive personal and other use of information systems inconsistent with this or any other Shadowfax policy is unauthorized. Under no circumstances are Shadowfax's information systems to be used for personal financial gain or to solicit others for activities unrelated to official Shadowfax business, such as solicitations for personal, political, or religious causes. Installation of software without approval from Shadowfax management is unauthorized.
- **Disruptive Use.** Use that may reasonably be considered offensive or disruptive to any individual or organization, or to harmony within the workplace is prohibited. Such disruptive use includes, but is not limited to, transmission, retrieval, storage, or display of defamatory, obscene, offensive, politically motivated, slanderous,

harassing, or illegal data, or messages that disclose personal information without authorization. Grossly indiscriminate or "broad band" distribution of email would clearly constitute a disruptive use.

- **Prohibited Use.** Unauthorized or illegal use of third-party intellectual property is prohibited. Such use includes, but is not limited to, downloading or using copyrighted or patented software, video and audio clips or documents on information systems in a manner inconsistent with relevant license terms or other intellectual property rights. When in doubt about the existence or scope of a license or about appropriate use of copyrighted, patented, or otherwise proprietary third-party data or software code, staff members should contact Shadowfax management. staff members are expressly prohibited from using Shadowfax's information systems to store or access pornography.

Only the IT Department is authorized to install software on servers, storage, and other related information resources.

VI. **ENFORCEMENT**

Any staff members member found to have violated this policy, in whole or in part, will be subject to disciplinary action, up to and including termination.

VII. **OVERSIGHT**

Shadowfax Compliance Committee or their designee(s) (the "Approved By") will be in charge of the administration of this Policy. The Approved By responsibilities include:

1. Identifying the action steps to come into compliance and directives to maintain compliance and implement the action steps.

2. Periodically reviewing this Policy and monitoring compliance to it.

3. Training responsible parties on their obligations under the Policy.

Revision History

Name	Date	Reason for Changes	Version

Note: The term “Individual” is synonymous with resident, client, patient, consumer, or participant.