Saveology
Information Security Policy

Table of Contents

1. Purpose

The purpose of this document is to provide standards and guidelines for Information Security at Saveology. These standards and guidelines are designed to protect Saveology's infrastructure, technology and the employees of Saveology from security breaches, hackers, and system vulnerabilities.

2. Scope

This policy covers all security standards and guidelines for Saveology. This includes but is not limited to all computer and communication devices owned or operated by Saveology. These policies also cover any computer and communication devices that are presented on Saveology premises, but which may not be owned or operated by Saveology. This Information Security policy is reviewed and updated annually by the IT Director. It is also communicated to the organization to review for any changes via the Saveology Intranet (http://www.saveologycentral.com).

3. Corporate Information Security

3.1 Acceptable Use Policy

3.1.1 Overview & Purpose

Information Technology's (IT) intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Saveology's established culture of openness, trust and integrity. IT is committed to protecting Saveology's employees, partners and the company from illegal or damaging actions.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are considered the property of Saveology. These systems are to be used for business purposes in serving the interests of the company, clients, and customers.

Effective security is a team effort involving the participation and support of every Saveology employee who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

3.1.2 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Saveology, including all personnel affiliated with third parties.

3.1.3 Policy

3.1.3.1 General Use and Ownership

1. While IT desires to provide a reasonable level of privacy, all the data created on the corporate systems remains the property of Saveology.
2. Employees are responsible for exercising good judgment regarding the extent of personal use. If there is any uncertainty, please check with your Supervisor, Management or the Information Technology Group.
3. IT recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see *Information Sensitivity Policy*.
4. IT may monitor and audit equipment, systems and network traffic at any time, Refer to the *Audit Policy*.
5. Users may only use software and/or operation systems that are approved by IT department.

3.1.3.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality.
2. Keep passwords secure and do not share accounts. System level passwords must be changed quarterly; user level passwords should be changed every (3) three months. For guidelines and information on password standards refer to the *Password Policy*.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the host will be unattended.
4. Use encrypted information in compliance the *Acceptable Encryption Use policy*.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised when using portable computers out of the office and/or traveling.
6. Postings by employees from a Saveology e-mail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Saveology, unless posting is in the course of business duties.
7. All computers that are connected to the Saveology Internet/Intranet/Extranet shall be continually executing approved virus-scanning software with a current virus database.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders which may contain viruses or other code harmful to Saveology.

3.1.3.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. The IT Security team, Network Engineering or System administration staff may have a need to disable the network access of a host if it is disrupting production services.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Saveology.
2. Unauthorized copying of copyrighted materials including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted

music, and the installation of any copyrighted software for which Saveology or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.
4. Introduction of malicious programs into the Saveology network or systems.
5. Revealing your account password to others or allowing use of your account by others
6. Using an Saveology computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
7. Making fraudulent offers of products, items, or services originating from any Saveology account.
8. Making statements about warranty, expressed or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning unless prior notification to IT is made and approved.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with availability or denying service to any users system (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Saveology employees to parties outside Saveology or any other unauthorized person or group.

E-mail and Communications Activities

1. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
2. Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of e-mail header information.
4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies or any other inappropriate reason.
5. Creating or forwarding chain letters or other pyramid schemes.
6. Posting the same or similar non-business-related messages to large numbers of Usernets newsgroups (newsgroup spam).

3.2 Audit Policy

3.2.1 Purpose

To provide the authority for IT authorized personnel to conduct security audits on any system at Saveology or connected to Saveology's network.

Audits may be conducted to:

- Ensure confidentiality, integrity and availability of information and resources
- Investigate possible security incidents to ensure conformity of Saveology security policies
- Monitor any corporate network user or system (s) activity.
- Monitor Internet usage

3.2.2 Scope

This policy covers all computers and communication devices owned or operated by Saveology and any computer and communications device that are present on Saveology's premises, but which may not be owned or operated by Saveology.

3.2.3 Policy

When requested, and for the purpose of performing an audit, access to computing resources will provided to appropriate personnel.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information that may be produced transmitted or stored on Saveology equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on Saveology networks

3.3 Password Policy

3.3.1 Overview

Passwords are the front line of protection for user accounts and are an important aspect of computer security. A poorly chosen password may result in the compromise of Saveology's entire corporate network. As such, all Saveology employees are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3.3.2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.3.3 Scope

The scope of this policy includes all personnel who have or are responsible for an account on any system that resides at any Saveology facility, has access to the Saveology network, or stores any non-public Saveology information.

3.3.4 Policy

General

- Only the IT Security Team & System Administrators will have the password to the Administrator's account for each domain.

- All system-level passwords: root, enable, domain admin, supervisor, SQL (s.a.), service accounts, application administration and other evaluated privilege accounts must be changed on at least a quarterly basis or if any knowledgeable personnel is terminated.
- All production system-level passwords must be part of the IT administered global password management database.
- All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every quarter.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively.
- All password changes / resets need authorization from a Manager of each department.
- Group and shared policies and user accounts are explicitly prohibited.
- All user-level and system-level passwords must conform to the guidelines described below.

3.3.5 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at Saveology. Some of the more common uses include: user level accounts, web accounts, e-mail accounts, screen saver protection, voice-mail password, and local router logins. Since very few systems have support for one-time tokens, all passwords should conform to the Strong Password characteristics. Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least (8) eight alphanumeric characters long.
- Is not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

B. Password Protection Standards

- Where possible, don't use the same password for various Saveology access needs. For example, select one password for the engineering systems and a separate password for IT systems.

- Do not share Saveology passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Saveology information.

- Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger, Firefox, MS Internet Explorer).

- Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions:

- Support authentication of individual users, not groups.
- Not store passwords in clear text or in any easily reversible form.
- Provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.
- Removal of any maintenance hooks or backdoors to code running in production.

D. Saveology Password Requirements

Below are the standards for creating passwords at Saveology and must be followed at all times when supported.

Passwords must have the following characteristics:

- 8 characters in length
- Must contain three of the following
- English lower case letters (a,b,c, … z)
- English upper case letters (A, B, C, … Z)
- Non-alphanumeric special characters (~, !, *, ., ?)
- Numeric characters (0 – 9)
- Passwords may not contain your user name or any part of your full name

3.4 Anti-Virus Policy

3.4.1 Purpose

Anti-virus software is used to stop the penetration of viruses and hacker programs to damage or gain access to information on your computer and or network resources. Viruses are continually created and distributed and can be transmitted thought e-mails, transferring infected files.

3.4.2 Scope

The scope of this policy includes all personnel, either by contract or permanent employment, who has access and/or connects to any of Saveology's network resources. Any form of access which includes physical connections, remote access, and wireless connection.

3.4.3 Policy

1. Guidelines

Systems that are connected to Saveology's network resources must be running the corporate standard Anti-Virus Application.

- Always run the corporate standard, supported anti-virus which is installed by IT before you receive your computer and the anti-virus software will be automatically updated, along with the virus definitions as they become available thought the use of a local or remote network connection.

- Never open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access.
- Always scan a floppy diskette, CD or USB device from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store it in a safe place.

2. Anti-Virus Standards – Servers

Servers must be set up with the following standards.

- Saveology will audit all servers connected to the network 24x 7x 365 by the use of Anti-Virus Management Servers located on the network.
- A full system scan is executed on a system when it has been installed with the Operating System and there-after is protected by Real-time scanning. Users will not be able to disable the real-time protect virus protection.
- If any file exclusions need to be setup for a system, that user needs to open a ticket in the Saveology Helpdesk. The request will be sent to IT for approval. Then if approved, it will be implemented in the Anti-Virus Policy for that group.

3. Anti-Virus Standards - Employee Workstations

Employees must follow these standards.

- Users will not be able to disable the real-time protect virus protection
- Systems that are not rebuilt by IT the owner of that system must call the Saveology Helpdesk to have an IT personnel update that system before that systems is connected to the network permanently.
- Saveology will audit all systems connected to the network 24 x 7 x 365 by the use of Anti-Virus Management Servers located on the network.
- If any file exclusions need to be setup for a system, that user needs to open a ticket in the Saveology Helpdesk. The request will be sent to IT for approval. Then if approved it will be implemented in the Anti-Virus Policy for that group.

3.5 Remote Access Policy

3.5.1 Purpose

The purpose of this policy is to define standards for connecting to Saveology's network from any host. These standards are designed to minimize the potential exposure to Saveology from damages which may result from unauthorized use of Saveology resources.

3.5.2 Scope

This policy applies to all Saveology employees, contractors, vendors and agents with a Saveology-owned or personally-owned computer or workstation used to connect to the Saveology network. This policy applies to remote access connections used to do work on behalf of Saveology, including reading or sending e-mail and viewing intranet web resources.

3.5.3 Policy

3.5.3.1 General

1. Remote access privileges to Saveology's corporate network must be given the same consideration as the on-site connection to Saveology.
2. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Saveology's network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*

3.5.3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any Saveology employee provide their login or e-mail password to anyone.
3. Ensure that Saveology-owned personal computer or workstation, which is remotely connected to Saveology's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Saveology employees and contractors with remote access privileges to Saveology's corporate network must not use non-Saveology e-mail accounts (i.e., Gmail, Hotmail, Yahoo, AOL), or other external resources to conduct Saveology business.
5. All hosts that are connected to Saveology internal networks via remote access technologies must use the most up-to-date anti-virus software.
6. Personal equipment that is used to connect to Saveology networks must meet the requirements of Saveology-owned equipment for remote access.
7. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Saveology production network must obtain prior approval from IT.

3.6 Dial-In Access Policy

3.6.1 Purpose

The purpose of this policy is to protect Saveology’s electronic information from being inadvertently compromised by authorized personnel using a dial-in connection.

3.6.2 Scope

The scope of this policy is to define appropriate dial-in access and its use by authorized personnel.

3.6.3 Policy

Saveology employees and authorized third parties (customers, vendors, etc.) can use dial-in connections to gain access to the corporate network. Dial-in access should be strictly controlled, using one-time password authentication. Any requests to get dial-in rights needs to be process by the Saveology Helpdesk.

Dial-in connections are literal extensions of Saveology's corporate network and provide a potential path to the company's most sensitive information. It is the responsibility of employees with dial-in access privileges to ensure a dial-in connection to Saveology is secure. The employee and/or authorized third party individual must take every reasonable measure to protect this service.

Analog and non-GSM digital cellular phones cannot be used to connect to Saveology's corporate network, as their signals can be readily scanned and/or hijacked by unauthorized individuals. Only GSM standard digital cellular phones are considered secure enough for connection to Saveology's network. For additional information on wireless access to the Saveology network, consult the *Wireless Communications Policy*.

Note: Dial-in accounts are considered 'as needed' accounts. Account activity is monitored, and if a dial-in account is not used for a period of six months the account will expire and no longer function. If dial-in access is subsequently required, the individual must request a new account as described above.

3.7 Virtual Private Networking (VPN) Policy

3.7.1 Purpose

The purpose of this policy is to provide guidelines for remote access via Virtual Private Network (VPN) connections to the Saveology corporate network.

3.7.2 Scope

This policy applies to all Saveology employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Saveology network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

3.7.3 Policy

Approved Saveology employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Saveology internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.
4. VPN gateways will be set up and managed by IT.
5. VPN users will be automatically disconnected from Saveology's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
6. The VPN concentrator is limited to an absolute connection time of 24 hours.
7. Users of computers that are not Saveology-owned equipment must configure the equipment to comply with Saveology's VPN and Network policies.
8. Only IT-approved VPN clients may be used.

9. By using VPN technology with personal equipment, users must understand that their machines are an extension of Saveology's network, and as such are subject to the same rules and regulations that apply to Saveology owned equipment.

Note: VPN accounts are considered 'as needed' accounts. Account activity is monitored, and if a VPN account is not used for a period of six months the account will expire and no longer function. If VPN access is subsequently required, the individual must request a new account as described above.

3.8 Server Security Policy

3.8.1 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Saveology.

3.8.2 Scope

This policy applies to server equipment owned and/or operated by Saveology, and to servers registered under any Saveology internal network domain. This policy is specifically for equipment on the internal Saveology network. For secure configuration of equipment external to Saveology on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.8.3 Policy

A. Ownership and Responsibilities

All internal servers deployed at Saveology must be owned by an operational group that is responsible for system administration. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides.

B. General Configuration Guidelines

- Operating System configuration (versions) should be in accordance with approved IT guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods.
- Security patches must be installed on the system as directed by IT or sooner.
- System patches are deployed on a monthly basis if applicable when released by Microsoft and various technology vendors.
- Do not use Administrator account when a non-privileged account will do.
- Group and shared policies and user accounts are explicitly prohibited.
- Production servers should be physically located in an access-controlled environment.

C. Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 month.
- Daily differential tape backups will be retained for at least 2 month.
- Weekly full tape backups will be done every Friday and retained for at least 2 month.
- Archive full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to IT by calling the Saveology Helpdesk. They will inform Information Security personnel which will review the incident and report to IT management. Corrective measures will be prescribed as needed.

D. Compliance

- Audits should be performed on a regular basis by authorized organizations in accordance with the *Audit Policy*.

3.9 Wireless Communication Policy

3.9.1 Purpose

This policy prohibits unauthorized wireless access to Saveology networks.

3.9.2 Scope

This policy covers any wireless data communication device including but not limited to a personal computer, Access point, laptop computer, cellular phone, PDA, or any other device with wireless capabilities connected to any of Saveology's data networks. This includes any form of wireless communication device capable of transmitting or receiving packet data. Wireless devices and/or networks without any connectivity to Saveology networks (such as cellular phones or Bluetooth devices connected only to their provider's voice and data networks or for personal use) do not fall under the purview of this policy. Any effort to circumvent Saveology's wireless security policy is prohibited.

3.9.3 Policy

Saveology will provide best-effort Wireless connectivity to Saveology network resources as a productivity aid for Saveology employees only. Unauthorized (Rogue) access points are prohibited and are subject to removal or rendering unusable. The employee responsible for or found using the unauthorized access point will be reported to their superior as well as HR. This includes Ad-Hoc or infrastructure access points. Only IT approved devices that support the Enterprise versions of WPA (Wi-Fi Protected Access) or WPA2 (Wi-Fi Protected Access2) will be supported and allowed to connect to the Saveology wireless infrastructure if configured and installed by authorized IT employees.

3.10 Information Sensitivity Policy

3.10.1 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Saveology without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Saveology Confidential information. Saveology Confidential information should not be left unattended in conference rooms or common areas.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to IT.

3.10.2 Scope

All Saveology information is categorized into two main classifications:

- Public – Information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage or harm to Saveology.
- Confidential – All other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information:
    - That should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company.
    - That is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.
    - That is Third Party Information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Saveology by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Saveology's network to support our operations.

3.10.3 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Saveology Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Saveology Confidential information in question.

3.10.3.1 Minimal Sensitivity: General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form:

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Saveology Confidential" may be written or designated in a conspicuous place on or in the

information in question. Other labels that may be used include "Saveology Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, Saveology information is presumed to be "Saveology Confidential" unless expressly determined to be Saveology Public information by a Saveology employee with authority to do so.

Access: Saveology employees, contractors, people with a business need to know.
Distribution within Saveology: Standard interoffice mail, approved electronic mail, and electronic file transmission methods.
Distribution outside of Saveology internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it is sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Saveology premises or shred documents; electronic data should be expunged / cleared. Reliably erase or physically destroy media.

3.10.3.2 More Sensitive: Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Saveology Confidential" or "Saveology Proprietary", wish to label the information "Saveology Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Saveology employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within Saveology: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Saveology internal mail: Sent via U.S. mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within Saveology, but should be encrypted or sent via a private link to approved recipients outside of Saveology premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on Saveology premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

3.10.3.3 Most Sensitive: Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Saveology Confidential information is very sensitive, you may should label the information "Saveology Internal: Registered and Restricted", "Saveology Eyes Only", "Saveology Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Saveology Confidential information need not be marked,

but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Saveology employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within Saveology: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of Saveology internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restriction to approved recipients within Saveology, but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Saveology premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

3.11 Internet DMZ Equipment Policy

3.11.1 Purpose

The purpose of this policy is to define standards to be met by all equipment owned and/or operated by Saveology located outside Saveology's corporate Internet firewalls. These standards are designed to minimize the potential exposure to Saveology from the loss of sensitive or company confidential data, intellectual property, damage to public image etc., which may follow from unauthorized use of Saveology resources.

Devices that are Internet facing and outside the Saveology firewall are considered part of the "de-militarized zone" (DMZ) and are subject to this policy. These devices (network and host) are particularly vulnerable to attacks from the Internet since they reside outside the corporate firewalls.

3.11.2 Scope

All equipment or devices deployed in a DMZ owned and/or operated by Saveology (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by Saveology, must follow this policy. This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the "Saveology.com" domain or appears to be owned by Saveology. All new equipment which falls under the scope of this policy must be configured according to the referenced configuration documents, unless a waiver is obtained from IT. All existing and future equipment deployed on Saveology's un-trusted networks must comply with this policy.

3.11.3 Policy

3.11.3.1 Ownership and Responsibilities

Equipment and applications within the scope of this policy must be administered by support groups approved by IT for DMZ system, application, and/or network management. Support groups will be responsible for the following:

- Equipment must be documented in the corporate wide enterprise management system. At a minimum, the following information is required:
    - Host contacts and location.
    - Hardware and operating system/version.
    - Main functions and applications.
    - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the corporate wide password management system/process.
- Changes to existing equipment and deployment of new equipment must follow and corporate governance or change management processes/procedures.

3.11.3.2 General System Configuration Policy

All equipment must comply with the following configuration policy:

- Hardware, operating systems, services and applications must be approved by IT as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards
- All patches/hot-fixes recommended by the equipment vendor and IT must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hot fixes.
- Services and applications not serving business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements and must be documented.
- Services and applications not for general access must be restricted by access control lists.
- Insecure services or protocols must be replaced with more secure equivalents whenever such exist.
- Remote administration must be performed over secure channels or console access independent from the DMZ networks. Where a methodology for secure channel connections is not available, one-time passwords must be used for all access levels.
- All host content updates must occur over secure channels.
- Security-related events must be logged and audit trails saved. Security-related events include the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access policy violations.

3.11.3.3 Firewall Configuration Policy

All firewall configuration changes must comply with the following configuration policy:

- All application ports that need to be opened for any servers or services must be in compliance with the IT Security Teams policy.
- Any application ports that are not within the IT Security Team Ports Policy and considered an exception must be reviewed prior and pre-approved by the Information Technology Groups Security Team before any changes can be made.
- Configuration changes are made by the IT Network Engineering Team.
- All configuration changes must be made during the maintenance window with the exceptions of

emergencies or incidents.

3.11.3.4 New Installations and Change Management Procedures

All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be done via the *DMZ Equipment Deployment Process*.
- Configuration changes must follow the Corporate Change Management (CM) Procedures.
- IT must be engaged to approve all new deployments and configuration changes.

3.11.3.5 Equipment Outsourced to External Service Providers

The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

3.12 Acceptable Encryption Policy

3.12.1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

3.12.2 Scope

This policy applies to all Saveology employees and affiliates.

3.12.3 Policy

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hillman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Saveology's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by IT. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

3.13 Visitor Domain Network Access Policy

3.13.1 Purpose

The purpose of this policy is to provide guidelines for enabling, managing, and auditing data network access for any personnel that are not Saveology employees. These "Non Saveology employees" will be referred to as "visitor personnel" for the remainder of this policy.

3.13.2 Scope

This policy applies to all Saveology business partners, contractors, consultants, customers, vendors and visitors utilizing the Saveology data network in any way. This policy applies to both onsite and remote visitor personnel.

3.13.3 Policy

Visiting personnel may be able to obtain approval to the data network using the visitor domain access and the approval of both the requesting department's manager and the Security Team. Approved visiting personnel granted access to the Saveology data network must adhere to the Saveology Information Security Policy and all of its sub policies, specifically the Acceptable Use Policy, Information Sensitivity Policy, Audit Policy, Antivirus Policy and the Visitor Domain Access Policy.
Data network access will only be granted once a non disclosure agreement (NDA) or Mutual non disclosure agreement (MNDA) has been signed between Saveology and the visitor's organization.

Data network access types:
Internet Access - Including but not limited to Web, Email, and FTP access
Virtual Private Network – Only to the network of an NDA signed corporation
HQ Server backbone – Connection to the Saveology servers
DMZ Servers – Connections to the Saveology web or externally accessible servers

- Hosted Co-location Servers – Must have approval from Director of Security Services

Approval process

1. Requesting department asks visiting vendor to sign an NDA or MNDA (if applicable)
2. Requesting department fills out visitor domain access form and obtains manager's signature
3. Help desk get request from department and sends it to Security Team
4. Security Team reviews and returns to help desk if approved or contacts department manager if not approved
5. Help desk creates account within the guidelines of the Visitor Domain Network Access Policy
6. Help desk audits quarterly to ensure access is renewed or removed

Limitations of Access

Time Limit - Three month per request or renewals
Approvers - Requesting group's manager and Security Team
Requirements - Must have signed MNDA or NDA & read and sign Saveology Security Policy
Servers - Only servers that are on the visitor domain access form
Prohibitions - Wireless data network access
Passwords - Passwords must be reset every 42 days even if access renewed
User IDs - All visitor personnel MUST be in the NON Saveology domain group

All visitor domain accounts will be subject to audit by both the help desk and the security team. The Security Team reserves the right to audit any device attached directly into the Saveology LAN or the WAN and/or is using a Saveology IP address within the Public or Private IP range.

3.14 Information Storage and Retention Policy

3.14.1 Purpose

The purpose of this policy is to provide guidelines for information data retention and the records management schedules associated to all critical business data in Saveology's enterprise.

All employees should recognize the importance of ensuring that all critical files are stored on the Saveology network (i.e., in the employees home directory). Employees are not responsible for backing up their own network directories and all the critical data files that physically reside there.

3.14.2 Scope

This policy applies to all Saveology employees that use the corporate email system, request, listen or distribute call (voice) recording containing sensitive data and facility personnel responsible for video surveillance management. This policy applies to both onsite and remote personnel.

Periodic backups of all critical business information and software on Saveology Information Technology resources will be performed. Business Owners / System owners are responsible for identifying the scope of the information and backups scheduled.

Retention of old outdated, or incorrect information can cause business complications and confusion. Inadvertent disclosure of retained unneeded information can place Saveology at risk for liabilities. Therefore, Saveology employees should not retain data that is no longer relevant to Saveology business operations unless retention is required for some other reason such as financial information for audits.

E-mail messages as well as other electronic and hard copy material may contain old, outdated or invalid information and take up storage space.

Please refer to the Saveology Records Management and Retention schedule for specific requirements.

3.14.3 Policy: Records management and retention schedules

Item:	Accessible On-line	Archived:
Corporate Email	Hosted solution with Rackspace	7 years
Call recordings	30 immediately \ on-line	7 years
Video Surveillance	90day online	1 year archive
Anti-Virus Software Logs	30 Days online	1 year archive

3.15 Employee Security Education

3.15.1 Purpose

The Purpose of this policy is to educate and raise awareness of corporate information security guidelines and responsibilities.

3.15.2 Scope

This policy applies to all Saveology employees.

3.15.3 Policy

A formal security awareness program will be implemented to make all employees aware of the importance of cardholder data security.

All employees will be educated upon hiring process and once annually. .

All employees will be required to acknowledge in writing that they have read and understand the company's security policies guidelines and procedures.

3.16 Employee Background procedures

3.16.1 Purpose

The purpose of this policy is to provide guidelines for employment background checks.

3.16.2 Scope

This policy applies to all Saveology employees.

3.16.3 Policy

All new employees will be subject to a background check as limited by law, during the hiring process by Human Resources Department.

4. Appendix A – IT Security Incident Procedure

Saveology Security Incident Procedure

Purpose

This procedure is for the escalation of reporting Security Incidents that happen and/or directly/indirectly affect Saveology's Networks and Systems.
This procedure should be used during the following conditions:

- Security Breach
- Virus Attack
- New Virus Discovery Alerts
- Systems Vulnerability Alerts
- Suspicion of illicit activity
- Knowledge or suspicion of malicious use of system resources, or any kind of damage to a system, or networks

IMPORTANT CONSIDERATIONS

A computer security incident can occur at anytime of the day or night. Although most hacker/cracker incidents occur during the off hours when hackers do not expect system managers to be watching their flocks. However, worm and virus incidents can occur any time during the day. Thus, time and distance considerations in responding to the incident are very important. If the first person on the call list to be notified can not respond within a reasonable time frame, then the second person must be called in addition to the first. It will be the responsibility of the people on the call list to determine if they can respond within an acceptable time frame.

Providing information to the wrong people could have undesirable side effects.

Scope

This policy covers all the steps necessary to notify the IT Security Team that there has been a form of a security breach, compromise, issue or general concern regarding a security situation.

Procedure

1. Once a security problem has been discovered the Saveology Helpdesk needs to be called to notify the IT Security Team and/or IT management.
2. Once the Helpdesk has been called, the Helpdesk will need to fill out the Saveology Security Alert Form with the information about the Security problem. Then E-Mail the Security alert Form document to the Information Security Team.
3. The Information Security Office and IT Management needs to be notified about the incident, by calling Help Desk, Cell Phones, Paging, or E-Mail.

4. Someone needs to be assigned to the Incident to monitor the progress of the resolution and that person needs to be entered in the Security Alert form with all his or her contact Information
5. Research then needs to be done on what the problem is and how it can be resolved. Then filling out the security alert form with the information that you find.
6. Every process that is completed need to be documented in the security alert form in the *Progress Log/notes* area.
7. Once the problem has been fixed. Enter in all the information on how the problem was resolved and the select Closed in the Case status field. Also enter in the date of completion in the *Closed Date* field.
8. Then save a copy of the security alert form and send to the Information Security Team for them to archive.

5. Appendix B – IT Security Alert Process Flow Chart

6. Appendix A – IT Supported Applications

Application Name	Vendor	Department	Type

7. Supported Forms