ACCEPTABLE USE POLICY

1.0 Overview
Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the corporate network. This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using company resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

2.0 Purpose
Since inappropriate use of corporate systems exposes RETA to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of RETA information technology resources for the protection of all parties involved.

3.0 Scope
The scope of this policy includes any and all use of RETA IT resources, including but not limited to, computer systems, email, the network, and the corporate Internet connection.

4.0 Policy

4.1 E-mail Use
Personal usage of RETA email systems is permitted as long as A) such usage does not negatively impact the RETA computer network, and B) such usage does not negatively impact the user's job performance.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive but is included to provide a frame of reference for types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to RETA may not be sent via email, regardless of the recipient, without proper encryption.
- It is RETA policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Attachments should not exceed the maximum file size permitted by the email server(s) and/or policy being used by RETA at the time.

Please note that detailed information about the use of email may be covered in RETA's Email Policy.

4.2 Confidentiality
Confidential data must not be A) shared or disclosed in any manner to non-employees of the company, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in
any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.

4.3 Network Access
The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

4.4 Unacceptable Use
The following actions shall constitute unacceptable use of the RETA network. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the RETA network and/or systems to:

- Engage in activity that is illegal under local, state, federal, or international law.
- Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.
- Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- Engage in activities that cause an invasion of privacy.
- Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- Make fraudulent offers for products or services.
- Perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques when not part of employee's job function.
- Install or distribute unlicensed or "pirated" software.
- Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

4.5 Blogging and Social Networking
Blogging and social networking by RETA's employees are subject to the terms of this policy, whether performed from the RETA network or from personal systems. This policy defines LinkedIn as a business site for matters related to RETA. Personal blogging and social networking is never allowed from the RETA computer network. RETA staff are prohibited from offering negative comments about RETA business matters or material detrimental to RETA in any blog or website. The user assumes all risks associated with personal blogging and/or social networking.

RETA staff may be required to monitor and respond to social network comments and questions about RETA and its programs. All communication representing RETA in these sites and matters must be handled professionally and in a manner that is consistent with RETA objectives and policies regarding interaction with RETA members, board members, committees, applicants, candidates, certified persons and other interested parties.

4.6 Instant Messaging
Instant messaging is allowed such that it follows guidelines on disclosure of confidential data and does not negatively impact the user's job function.
4.7 **Overuse**
Actions detrimental to the computer network or other RETA resources, or that negatively affect job performance are not permitted.

4.8 **Web Browsing**
The Internet is a network of interconnected computers of which the company has very little control. The user should recognize this when using the Internet and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet at his or her own risk. RETA is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

Personal Use. RETA recognizes that the Internet can be a tool that is useful for both personal and professional purposes. Personal usage of RETA computer systems to access the Internet is permitted as long as such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on RETA or on the user's job performance.

4.9 **Copyright Infringement**
RETA's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

4.10 **Peer-to-Peer File Sharing**
Peer-to-Peer (P2P) networking is not allowed on the RETA network under any circumstance.

4.11 **Streaming Media**
Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media is allowed for job-related functions only.

4.12 **Monitoring and Privacy**
Users should expect no privacy when using the RETA network or RETA resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. RETA reserves the right to monitor any and all use of the computer network. To ensure compliance with RETA policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.13 **Bandwidth Usage**
Excessive use of RETA bandwidth or other RETA resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low RETA usage.

4.14 **Personal Usage**
Personal usage of RETA computer systems is permitted if such usage follows pertinent guidelines elsewhere in this document and does not have a detrimental effect on RETA or on the user's job performance.
4.15 Remote Desktop Access
Use of non-RETA-supplied remote desktop software and/or services (such as Citrix, VNC, GoToMyPC, etc.) is prohibited.

4.16 Circumvention of Security
Using RETA-owned or RETA-provided computer systems to circumvent any security systems, authentication systems, user-based systems, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited.

4.17 Use for Illegal Activities
No RETA-owned or RETA-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:

- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing
- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of Terrorism
- Identity Theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes
- Downloading, storing, or distributing copyrighted material

RETA will take all necessary steps to report and prosecute any violations of this policy.

4.18 Non-RETA-Owned Equipment
RETA allows the use of outside or non-RETA-provided computer systems on the RETA network as long as the network systems and/or resources are not negatively affected. The user must take reasonable precautions to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the RETA network.

4.19 Personal Storage Media
RETA does not restrict the use personal storage media, which includes but is not limited to: USB or flash drives, external hard drives, personal music/media players, and CD/DVD writers, on the RETA network provided that guidelines for data confidentiality are followed. The user must take reasonable precautions to ensure viruses, Trojans, worms, malware, spyware, and other undesirable security risks are not introduced onto the company network. Use of personal storage media must conform to RETA’s Mobile Device Policy.
4.20 Software Installation
Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance. RETA expects users to use discretion when installing software on RETA-owned computers. When in doubt, the best course of action is not to install the software in question.

4.21 Reporting of Security Incident
If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and/or follow any applicable guidelines as detailed in the RETA Incident Response Policy. Examples of incidents that require notification include:

- Suspected compromise of login credentials (username, password, etc.).
- Suspected virus/malware/Trojan infection.
- Loss or theft of any device that contains company information.
- Loss or theft of ID badge or keycard.
- Any attempt by any person to obtain a user's password over the telephone or by email.
- Any other suspicious event that may impact RETA's information security.

Users must treat a suspected security incident as confidential information and report the incident only to his or her supervisor. Users must not withhold information relating to a security incident or interfere with an investigation.

4.22 Applicability of Other Policies
This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions
- **Blogging** The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").
- **Instant Messaging** A text-based computer application that allows two or more Internet-connected users to "chat" in real time.
- **Peer-to-Peer (P2P) File Sharing** A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.
- **Remote Desktop Access** Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.
- **Streaming Media** Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.
1.0 Overview
A backup policy is similar to an insurance policy - it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document. RETA's backup policy is among its most important policies.

2.0 Purpose
The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

3.0 Scope
This policy applies to all data stored on RETA systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

4.0 Policy

4.1 Identification of Critical Data
RETA must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.

4.2 Data to be Backed Up
A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

- All data determined to be critical to RETA operation and/or employee job function.
- All information stored on the RETA file server(s) and email server(s), as well as these servers operating systems and logs. It is the user's responsibility to ensure any data of importance is moved to the file server.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.
- Logs and configuration of network devices such as switches, routers, etc.
- Information stored on employee desktops if the backup administrator deems such information necessary and backup facilities exist for such an endeavor. The backup administrator may instead choose to backup a standard desktop configuration and restore data from the file server at his or her discretion.
- Off-site backup should be encrypted with 256 bit or higher to protect the security and privacy of all RETA records.

4.3 Backup Frequency
Backup frequency is critical to successful data recovery. RETA has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden
on the users, network, and backup administrator.

- Incremental: Daily backup to onsite servers is recommended with minimum protection of backup every 3 days to an onsite external drive at RETA. Backup to offsite servers should occur at least once every two weeks.
- Full: Full backup to onsite servers is recommended at least once per week. Full backup to offsite services should occur at least once each month.

### 4.4 Off-Site Rotation

Geographic separation from the backups must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet RETA's uptime requirements. RETA has determined that backup media must be rotated off-site at least once per week.

### 4.5 Backup Storage

Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, RETA data, precautions must be taken that are commensurate to the type of data being stored. RETA has set the following guidelines for backup storage.

There are no restrictions to how and where backups can be stored when on-site. When shipped off-site, backups should be reasonably secured from theft or fire. A hardened facility (i.e., commercial backup service or safe deposit box) can be used but is not required. Online backups are allowable if the service meets the criteria specified herein.

### 4.6 Backup Retention

When determining the time required for backup retention, RETA must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. RETA has determined that the following will meet all requirements (note that the backup retention policy must confirm to the company's data retention policy and any industry regulations, if applicable):

- Incremental Backups must be saved for two weeks.
- Full Backups must be saved for three months.

### 4.7 Restoration Procedures & Documentation

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis.

### 4.8 Restoration Testing

Since a backup policy does no good if the restoration process fails it is important to periodically test the restore procedures to eliminate potential problems.

Backup restores must be tested when any change is made that may affect the backup system, as well as twice per year.
4.9  **Expiration of Backup Media**
Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

4.10  **Applicability of Other Policies**
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0  **Enforcement**
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0  **Definitions**
- **Backup**  To copy data to a second location, solely for the purpose of safe keeping of that data.
- **Backup Media**  Any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.
- **Full Backup**  A backup that makes a complete copy of the target data.
- **Incremental Backup**  A backup that only backs up files that have changed in a designated time period, typically since the last backup was run.
- **Restoration Also**  called "recovery."  The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

**CONFIDENTIAL DATA POLICY**

1.0  **Overview**
Confidential data is typically the data that holds the most value to RETA. Often, confidential data is valuable to others as well, and thus can carry greater risk than general RETA data. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

2.0  **Purpose**
The purpose of this policy is to detail how confidential data, as identified by the Data Classification Policy, should be handled. This policy lays out standards for the use of confidential data and outlines specific security controls to protect this data.

3.0  **Scope**
The scope of this policy covers all RETA-confidential data, regardless of location. Also covered by the policy are hardcopies of RETA data, such as printouts, faxes, notes, etc.
4.0 Policy

4.1 Treatment of Confidential Data
For clarity, the following sections on storage, transmission, and destruction of confidential data are restated from the Data Classification Policy.

4.1.1 Storage
Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

4.1.2 Transmission
Confidential data must not be 1) transmitted outside the RETA network without the use of strong encryption, or 2) left on voicemail systems, either inside or outside RETA's network.

4.1.3 Destruction
Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

• Paper/documents: cross cut shredding is required.
• Storage media (CD's, DVD's): physical destruction is required.
• Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformating a drive does not make the data unrecoverable. If wiping is used, RETA must use the most secure commercially-available methods for data wiping. Alternatively, RETA has the option of physically destroying the storage media.

4.2 Use of Confidential Data
A successful confidential data policy is dependent on the users knowing and adhering to RETA's standards involving the treatment of confidential data. The following applies to how users must interact with confidential data:

• Users must be advised of any confidential data they have been granted access. Such data must be marked or otherwise designated "confidential."
• Users must only access confidential data to perform his/her job function.
• Users must not seek personal benefit, or assist others in seeking personal benefit, from the use of confidential information.
• Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or the action is approved by his or her supervisor.
• Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.
• If confidential information is shared with third parties, such as contractors or vendors, a confidential information or non-disclosure agreement must govern the third parties' use of confidential information. Refer to RETA's outsourcing policy for additional guidance.

4.3 Security Controls for Confidential Data
Confidential data requires additional security controls in order to ensure its integrity. The company requires
that the following guidelines are followed:

- **Strong Encryption.** Strong encryption must be used for confidential data transmitted external to RETA. If confidential data is stored on laptops or other mobile devices, it must be stored in encrypted form.
- **Network Segmentation.** Separating confidential data by network segmentation is strongly encouraged.
- **Authentication.** Strong passwords must be used for access to confidential data.
- **Physical Security.** Systems that contain confidential data should be reasonably secured.
- **Printing.** When printing confidential data, the user should use best efforts to ensure that the information is not viewed by others. Printers that are used for confidential data must be located in secured areas.
- **Faxing.** When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.
- **Emailing.** Confidential data must not be emailed outside RETA without the use of strong encryption.
- **Mailing.** If confidential information is sent outside RETA, the user must use a service that requires a signature for receipt of that information.
- **Discussion.** When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.
- **Confidential data must be removed from documents unless its inclusion is absolutely necessary.**
- **Confidential data must never be stored on non-RETA-provided machines (i.e., home computers).**
- **If confidential data is written on a whiteboard or other physical presentation tool, the data must be erased after the meeting is concluded.**

### 4.4 Examples of Confidential Data

The following list is not intended to be exhaustive but should provide RETA with guidelines on what type of information is typically considered confidential. Confidential data can include:

- Employee, member or candidate social security numbers or personal information
- Medical and healthcare information
- Electronic Protected Health Information (EPHI)
- Member or candidate data
- Sales forecasts
- Product and/or service plans, details, and schematics
- Network diagrams and security configurations
- Communications about corporate legal matters
- Passwords
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

### 4.5 Applicability of Other Policies

This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics
covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Authentication** A security method used to verify the identity of a user and authorize access to a system or network.
- **Critical Personal Information** Confidential information required to manage RETA business and operations such as employee salaries, medical records and similar personal data.
- **Encryption** The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
- **Mobile Data Device** A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.
- **Operational Data** Confidential information required to manage RETA business and operations such as member credit card numbers, personal information, billing records and other data related to delivering and/or managing RETA services.
- **Two-Factor Authentication** A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

EMAIL POLICY

1.0 Overview
Email is an essential component of business communication; however, it presents a particular set of challenges due to its potential to introduce a security threat to the network. Email can also have an effect on RETA's liability by providing a written record of communications, so having a well thought out policy is essential. This policy outlines expectations for appropriate, safe, and effective email use.

2.0 Purpose
The purpose of this policy is to detail RETA's usage guidelines for the email system. This policy will help RETA reduce risk of an email-related security incident, foster good business communications both internal and external to RETA, and provide for consistent and professional application of RETA's email principles.

3.0 Scope
The scope of this policy includes RETA's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the RETA network.
4.0 Policy

4.1 Proper Use of Company Email Systems
Users are asked to exercise common sense when sending or receiving email from RETA accounts. Additionally, the following applies to the proper use of the RETA email system.

4.1.1 Sending Email
When using a RETA email account, email must be addressed and sent carefully. Users should keep in mind that RETA loses any control of email once it is sent external to the RETA network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help RETA avoid the unintentional disclosure of sensitive or non-public information.

4.1.2 Personal Use and General Guidelines
Personal usage of RETA email systems is permitted as long as A) such usage does not negatively impact the RETA computer network, and B) such usage does not negatively impact the user's job performance.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive but is included to provide a frame of reference for types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to RETA may not be sent via email, regardless of the recipient, without proper encryption.
- It is RETA policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

Please note that the topics above may be covered in more detail in other sections of this policy.

4.1.3 Business Communications and Email
RETA uses email as an important communication medium for business operations. Users of the RETA email system are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, users are asked to recognize that email sent from a RETA account reflects on RETA, and, as such, email must be used with professionalism and courtesy.

4.1.4 Email Signature
Email signatures (contact information appended to the bottom of each outgoing email) may or may not be used, at the discretion of the individual user. Users are asked to keep any email signatures professional in nature; however, RETA does not place any restrictions on email signature content.
4.1.5 **Auto-Responders**
An auto-responder can be a useful tool when a user will be out of the office for an extended period. RETA neither requires nor forbids the use of email auto-responders.

4.1.6 **Mass Emailing**
RETA makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for both sales and non-sales purposes (such as when communicating with RETA's employees, members, boards, committees or other interested parties), and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

It is RETA's intention to comply with applicable laws governing the sending of mass emails. For this reason, as well as in order to be consistent with good business practices, RETA requires that email sent to more than twenty (20) recipients external to RETA have the following characteristics:

1. The email must contain instructions on how to unsubscribe from receiving future emails (a simple "reply to this message with UNSUBSCRIBE in the subject line" will do). Unsubscribe requests must be honored immediately.
2. The email must contain a subject line relevant to the content.
3. The email must contain contact information, including the full physical address, of the sender.
4. The email must contain no intentionally misleading information (including the email header), blind redirects, or deceptive links.

Note that emails sent to RETA employees, members, board members, committees, existing members, or persons who have already inquired about RETA's services are exempt from the above requirements.

4.1.7 **Opening Attachments**
Users must use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users should:

- Never open unexpected email attachments.
- Never open email attachments from unknown sources.
- Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially-formatted emails can hide a malicious URL.

RETA may use methods to block what it considers to be dangerous or emails or strip potentially harmful email attachments as it deems necessary.

4.1.8 **Monitoring and Privacy**
Users should expect no privacy when using the RETA network or RETA resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. RETA reserves the right to monitor any and all use of the computer network. To ensure compliance with RETA policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

4.1.9 **Company Ownership of Email**
Users should be advised that RETA owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by RETA and it may be subject
to use for purposes not be anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.

4.1.10 Contents of Received Emails
Users must understand that RETA has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, RETA may attempt to reduce the amount of this email that the users receive, however no solution will be 100 percent effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she should notify his or her supervisor.

4.1.11 Access to Email from Mobile Phones
Many mobile phones or other devices, often called smartphones, provide the capability to send and receive email. RETA permits users to access the company email system from a mobile phone. Refer to the Mobile Device Policy for more information.

4.1.12 Email Regulations
Any specific regulations (industry, governmental, legal, etc.) relating to RETA's use or retention of email communications must be listed here or appended to this policy.

4.2 External and/or Personal Email Accounts
RETA recognizes that users may have personal email accounts in addition to their RETA-provided account. The following sections apply to non-RETA provided email accounts:

4.2.1 Use for Company Business
Users of RETA's email systems are given the flexibility to use either the RETA email system, or personal email accounts, whichever is more convenient to the user. Users should ensure that, when using non-RETA-provided email accounts for RETA business, the applicable email policies are followed.

4.2.2 Access from the Company Network
Users are permitted to access external or personal email accounts from the RETA network, as long as such access uses no more than a trivial amount of the users' time and company resources.

4.2.3 Use for Personal Reasons
Users are strongly encouraged to use a non-RETA-provided (personal) email account for any non-business communications. Users must follow applicable policies regarding the access of non-RETA-provided accounts from the RETA network.

4.3 Confidential Data and Email
The following sections relate to confidential data and email:

4.3.1 Passwords
As with any RETA passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. At the discretion of the IT Manager, RETA may further secure email with certificates, two factor authentication, or another security mechanism.
4.3.2 Emailing Confidential Data
Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient.

RETA requires that any email containing confidential information, regardless of whether the recipient is internal or external to the RETA network, be encrypted using commercial-grade, strong encryption.

Further guidance on the treatment of confidential information exists in RETA's Confidential Data Policy. If information contained in the Confidential Data Policy conflicts with this policy, the Confidential Data Policy will apply.

4.4 Company Administration of Email
RETA will use its best effort to administer RETA's email system in a manner that allows the user to both be productive while working as well as reduce the risk of an email-related security incident.

4.4.1 Filtering of Email
A good way to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, RETA will filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed A) contrary to this policy, or B) a potential risk to RETA's IT security. No method of email filtering is 100 percent effective, so the user is asked additionally to be cognizant of this policy and use common sense when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. This functionality may or may not be used at the discretion of the IT Manager.

4.4.2 Email Disclaimers
The use of an email disclaimer, usually text appended to the end of every outgoing email message, is an important component in RETA's risk reduction efforts. RETA requires the use of email disclaimers on all outgoing email sent during regular communications from RETA HQ. Such disclaimers must contain the following notices:

- The email is for the intended recipient only
- The email may contain private information
- If the email is received in error, the sender should be notified, and any copies of the email destroyed
- Any unauthorized review, use, or disclosure of the contents is prohibited

RETA acknowledges that staff often may respond to email inquiries from a cell phone or other remotely connected device in which a disclaimer statement may not be available. Under such circumstances, staff should include the appropriate disclaimer at the next opportunity to do so in their communications with the involved person.

An example of such a disclaimer is:

NOTE: This email message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by replying...
to this email, and destroy all copies of the original message.

RETA should review any applicable regulations relating to its electronic communication to ensure that its email disclaimer includes all required information.

4.4.3 Email Deletion
Users are encouraged to delete email periodically when the email is no longer needed for business purposes. The goal of this policy is to keep the size of the user's email account manageable and reduce the burden on the company to store and backup unnecessary email messages.

However, users are strictly forbidden from deleting email in an attempt to hide a violation of this or another RETA policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

RETA must note and document here any applicable regulations or statutes that apply to email deletion.

4.4.4 Retention and Backup
Email should be retained and backed up in accordance with the applicable policies, which may include but are not limited to the: Data Classification Policy, Confidential Data Policy, Backup Policy, and Retention Policy.

Unless otherwise indicated, for the purposes of backup and retention, email should be considered operational data.

4.4.5 Address Format
Email addresses must be constructed in a standard format in order to maintain consistency across RETA. Some recommended formats are:

- Firstname.lastname@RETA.com
- Firstinitial.lastname@RETA.com
- Firstname-lastname@RETA.com
- FirstnameLastname@RETA.com

RETA can choose virtually any format, as long as it can be applied consistently throughout the organization. The intent of this policy is to simplify email communication as well as provide a professional appearance.

4.4.6 Email Aliases
Often the use of an email alias, which is a generic address that forwards email to a user account, is a good idea when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for RETA email, as well as (often) the names of RETA employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

A few examples of commonly used email aliases are:

- sales@RETA.com
- techsupport@RETA.com
• pr@RETA.com
• info@RETA.com

RETA may or may not use email aliases, as deemed appropriate by the IT Manager and/or executive team. Aliases may be used inconsistently, meaning: RETA may decide that aliases are appropriate in some situations but not others depending on the perceived level of risk.

4.4.7 Account Activation
Email accounts will be set up for each user determined to have a business need to send and receive RETA email. Accounts will be set up at the time a new hire starts with RETA, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive email.

4.4.8 Account Termination
When a user leaves RETA, or his or her email access is officially terminated for another reason, RETA will disable the user's access to the account by password change, disabling the account, or another method. RETA is under no obligation to block the account from receiving email and may continue to forward inbound email sent to that account to another user or set up an auto-response to notify the sender that the user is no longer employed by RETA.

4.4.9 Storage Limits
As part of the email service, email storage may be provided on RETA servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the IT Manager. Storage limits may vary by employee or position within RETA.

4.5 Prohibited Actions
The following actions shall constitute unacceptable use of the RETA email system. This list is not exhaustive but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the RETA email system to:

• Send any information that is illegal under applicable laws.
• Access another user’s email account without A) the knowledge or permission of that user - which should only occur in extreme circumstances, or B) the approval of RETA executives in the case of an investigation, or C) when such access constitutes a function of the employee’s normal job responsibilities.
• Send any emails that may cause embarrassment, damage to reputation, or other harm to RETA.
• Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
• Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.
• Make fraudulent offers for products or services.
• Attempt to impersonate another person or forge an email header.
• Send spam, solicitations, chain letters, or pyramid schemes.
• Knowingly misrepresent RETA’s capabilities, business practices, warranties, pricing, or policies.
• Conduct non-RETA-related business.

RETA may take steps to report and prosecute violations of this policy, in accordance with RETA standards and applicable laws.
4.5.1 Data Leakage
Data can leave the network in a number of ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to RETA's control of its data.

Unauthorized emailing of RETA data, confidential or otherwise, to external email accounts for the purpose of saving this data external to RETA systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user should notify his or her supervisor rather than emailing the data to a personal account or otherwise removing it from RETA systems.

RETA may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the IT Manager.

4.5.2 Sending Large Emails
Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. RETA does not wish to impose a hard limit on email attachment size but asks the user to exercise discretion so that the system isn't unnecessarily strained. RETA employees should consult senior management regarding identification of a preferred way of sending large email attachments.

The user is further asked to recognize the additive effect of large email attachments when sent to multiple recipients and use restraint when sending large files to more than one person.

4.6 Applicability of Other Policies
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, RETA may report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

6.0 Definitions

- **Auto Responder** An email function that sends a predetermined response to anyone who sends an email to a certain address. Often used by employees who will not have access to email for an extended period of time, to notify senders of their absence.

- **Certificate** Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.

- **Data Leakage** Also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is
sometimes malicious and sometimes inadvertent by users with good intentions.

- **Email** Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a company or between companies.

- **Encryption** The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

- **Mobile Device** A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

- **Password** A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

- **Spam** Unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.

- **Smartphone** A mobile telephone that offers additional applications, such as PDA functions and email.

- **Two Factor Authentication** A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

**ENCRYPTION POLICY**

1.0 **Overview**

Encryption, also known as cryptography, can be used to secure data while it is stored or being transmitted. It is a powerful tool when applied and managed correctly. As the amount of data RETA must store digitally increases, the use of encryption must be defined and consistently implemented in order to ensure that the security potential of this technology is realized.

2.0 **Purpose**

The purpose of this policy is to outline RETA’s standards for use of encryption technology so that it is used securely and managed appropriately. Many policies touch on encryption of data so this policy does not cover what data is to be encrypted, but rather how encryption is to be implemented and controlled.

3.0 **Scope**

This policy covers all data stored on or transmitted across RETA systems.

4.0 **Policy**

4.1 **Applicability of Encryption**

1. Data while stored. This includes any data located on RETA-owned or RETA-provided systems, devices, media, etc. Examples of encryption options for stored data include:
   - Whole disk encryption
   - Encryption of partitions/files
   - Encryption of disk drives
   - Encryption of personal storage media/USB drives
   - Encryption of backups
   - Encryption of data generated by applications
2. Data while transmitted. This includes any data sent across the company network, or any data sent to
or from a RETA-owned or RETA-provided system. Types of transmitted data that can be encrypted
include:
   - VPN tunnels
   - Remote access sessions
   - Web applications
   - Email and email attachments
   - Remote desktop access
   - Communications with applications/databases

4.2 Encryption Key Management
Key management is critical to the success of an implementation of encryption technology. The following
guidelines apply to RETA's encryption keys and key management:
   - Management of keys must ensure that data is available for decryption when needed
   - Keys must be backed up
   - Keys must be kept secure
   - Keys must never be transmitted in clear text
   - Keys are confidential data
   - Keys must not be shared
   - Physical key generation materials must be destroyed within 5 business days.
   - Keys must be used and changed in accordance with the password policy.
   - When user encryption is employed, minimum key length is 10 characters.

4.3 Acceptable Encryption Algorithms
Only the strongest types of generally-accepted, non-proprietary encryption algorithms are allowed, such as
AES or 3DES. Acceptable algorithms should be reevaluated as encryption technology changes.

Use of proprietary encryption is specifically forbidden since it has not been subjected to public inspection and
its security cannot be assured.

4.4 Legal Use
Some governments have regulations applying to the use and import/export of encryption technology. The
company must conform with encryption regulations of the local or applicable government.

RETA specifically forbids the use of encryption to hide illegal, immoral, or unethical acts. Anyone doing so is
in violation of this policy and will face immediate consequences per the Enforcement section of this
document.

4.5 Applicability of Other Policies
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics
covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and Executive Team. Violations may result in disciplinary action,
which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Encryption** The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
- **Encryption Key** An alphanumeric series of characters that enables data to be encrypted and decrypted.
- **Mobile Storage Media** A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.
- **Password** A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.
- **Remote Access** The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.
- **Remote Desktop Access** Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.
- **Virtual Private Network (VPN)** A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.
- **Whole Disk Encryption** A method of encryption that encrypts all data on a particular drive or volume, including swap space and temporary files.

GUEST ACCESS POLICY

1.0 Overview

Guest access to RETA's network is often necessary for board members, committees, customers, consultants, or vendors who are visiting RETA's offices. This can be simply in the form of outbound Internet access, or the guest may require access to specific resources on RETA's network. Guest access to RETA's network must be tightly controlled.

2.0 Purpose

RETA may wish to provide network access as a courtesy to guests wishing to access the Internet, or by necessity to visitors with a business need to access RETA's resources. This policy outlines RETA's procedures for securing guest access.

3.0 Scope

The scope of this policy includes any visitor to RETA wishing to access the network or Internet through RETA's infrastructure and covers both wired and wireless connections. This scope excludes guests accessing wireless broadband accounts directly through a cellular carrier or third party where the traffic does not traverse RETA's network.
4.0 Policy

4.1 Granting Guest Access
Guest access will be provided on a case-by-case basis to any person who can demonstrate a reasonable business need to access the network or access the Internet from the RETA network.

4.1.1 AUP Acceptance
Guests must agree to and sign RETA's Acceptable Use Policy (AUP) before being granted access.

4.1.2 Approval
Guest need for access will be evaluated and provided on a case-by-case basis. This should involve management approval if the request is non-standard.

4.1.3 Account Use
RETA may provide a generic guest account that can be re-used by different guests. If these accounts are offered, they are only to be used by guests. Users with network accounts must use their accounts for network access.

4.1.4 Security of Guest Machines
Guests are expected to be responsible for maintaining the security of his or her machine, and to ensure that it is free of viruses, Trojans, malware, etc. RETA reserves the right to inspect the machine if a security problem is suspected but will not inspect each guest's system prior to accessing the network.

4.2 Guest Access Infrastructure Requirements
Best practices dictate that guest access be kept separate, either logically or physically, from the corporate network, since guests have typically not undergone the same amount of scrutiny as the company's employees. Guest access will be a segregated network with access only to WiFi and the Internet unless the guest has a specific need to access RETA's corporate records. Guest access should be provided prudently and monitored for appropriateness of use.

4.3 Restrictions on Guest Access
Guest access will be restricted to the minimum amount necessary. Depending on the guest needing access, this can often be limited to outbound Internet access only. RETA will evaluate the need of each guest and provide further access if there is a business need to do so.

4.4 Monitoring of Guest Access
RETA's policy is that if it is granting access to a guest, that guest is a trusted user. As such, RETA does not wish to monitor guest access.

4.5 Applicability of Other Policies
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are
suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Account** A combination of username and password that allows access to computer or network resources.
- **Guest** A visitor to RETA premises who is not an employee.

INCIDENT RESPONSE POLICY

1.0 Overview

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Policy is critical to successful recovery from an incident. This policy covers all incidents that may affect the security and integrity of RETA's information assets, and outlines steps to take in the event of such an incident.

2.0 Purpose

This policy is intended to ensure that RETA is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents. Note that this policy is not intended to provide a substitute for legal advice and approaches the topic from a security practices perspective.

3.0 Scope

The scope of this policy covers all information assets owned or provided by RETA, whether they reside on the RETA network or elsewhere.

4.0 Policy

4.1 Types of Incidents

A security incident, as it relates to RETA's information assets, can take one of two forms. For the purposes of this policy a security incident is defined as one of the following:

- **Electronic**: This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection.
- **Physical**: A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain RETA information.

4.2 Preparation

Work done prior to a security incident is more important than work done after an incident is discovered. The most important preparation work, obviously, is maintaining good security controls that will prevent or limit damage in the event of an incident. This includes technical tools such as firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as good physical security for laptops and mobile devices.
Additionally, prior to an incident, RETA must ensure that the following is clear to IT personnel:

- What actions to take when an incident is suspected.
- Who is responsible for responding to an incident.

RETA must have discussions with an IT Security company that offers incident response services before such an incident occurs in order to prepare an emergency service contract. This will ensure that high-end resources are quickly available during an incident.

Finally, RETA should review any industry or governmental regulations that dictate how it must respond to a security incident (specifically, loss of member or certification candidate data), and ensure that its incident response plans adhere to these regulations.

### 4.3 Confidentiality

All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained. This will serve both to protect employees’ reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or members and candidates.

#### 4.4 Electronic Incidents

When an electronic incident is suspected, RETA’s goal is to recover as quickly as possible, limit the damage done, and secure the network. The following steps should be taken in order:

1. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.
2. Disable the compromised account(s) as appropriate.
3. Report the incident to the IT Manager.
4. Backup all data and logs on the machine, or copy/image the machine to another system.
5. Determine exactly what happened and the scope of the incident. Was it an accident? An attack? A Virus? Was confidential data involved? Was it limited to only the system in question or was it more widespread?
6. Notify RETA management/executives as appropriate.
7. Contact an IT Security consultant as needed.
8. Determine how the attacker gained access and disable this access.
9. Rebuild the system, including a complete operating system reinstall.
10. Restore any needed data from the last known good backup and put the system back online.
11. Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.
12. Reflect on the incident.
   - What can be learned?
   - How did the Incident Response team perform?
   - Was the policy adequate?
   - What could be done differently?
13. Consider a vulnerability assessment as a way to spot any other vulnerabilities before they can be exploited.

### 4.5 Physical Incidents
Physical security incidents are challenging, since often the only actions that can be taken to mitigate the incident must be done in advance. This makes preparation critical. One of the best ways to prepare is to mandate the use of strong encryption to secure data on mobile devices. Applicable policies, such as those covering encryption and confidential data, should be reviewed.

Physical security incidents are most likely the result of a random theft or inadvertent loss by a user, but they must be treated as if they were targeted at RETA.

RETA must assume that such a loss will occur at some point, and periodically survey a random sampling of laptops and mobile devices to determine the risk if one were to be lost or stolen.

**4.5.1 Response**

Establish the severity of the incident by determining the data stored on the missing device. This can often be done by referring to a recent backup of the device. Two important questions must be answered:

1. Was confidential data involved?
   a. If not, refer to "Loss Contained" below.
   b. If confidential data was involved, refer to "Data Loss Suspected" below.

2. Was strong encryption used?
   a. If strong encryption was used, refer to "Loss Contained" below.
   b. If not, refer to "Data Loss Suspected" below.

**4.5.2 Loss Contained**

First, change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Notify the IT Manager. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities if a theft has occurred.

**4.5.3 Data Loss Suspected**

First, notify the executive team, legal counsel, and/or public relations group so that each team can evaluate and prepare a response in their area.

Change any usernames, passwords, account information, WEP/WPA keys, passphrases, etc., that were stored on the system. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities as needed if a theft has occurred and follow disclosure guidelines specified in the notification section.

Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls.

**4.6 Notification**

If an electronic or physical security incident is suspected to have resulted in the loss of third-party/member/candidate data, notification of the public or affected entities should occur. First this must be discussed with executive team and legal counsel to determine an appropriate course of action. If notification is deemed an appropriate, it should occur in an organized and consistent manner.
4.7 Managing Risk
Managing risk of a security incident or data loss is the primary reason to create and maintain a comprehensive security policy. Risks can come in many forms: electronic risks like data corruption, computer viruses, hackers, or malicious users; or physical risks such as loss/theft of a device, hardware failure, fire, or a natural disaster. Protecting critical data and systems from these risks is of paramount importance to RETA.

4.7.1 Risk Assessment
As part of the risk management process, RETA must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the company's critical or confidential information. The process must include the following steps:

a) Scope the assessment. Determine both the physical and logical boundaries of the assessment.
b) Gather information. Determine what confidential or critical information is maintained by RETA. Determine how this information is secured.
c) Identify threats. Determine what man-made and natural events could affect RETA's electronic information.
d) Identify Vulnerabilities. After threats have been identified, determine RETA's exposure to each threat. External assessments may be useful here, as covered in the Network Security Policy.
e) Assess Security Controls. After vulnerabilities have been cataloged, determine the efficiency of RETA's security controls in mitigating that vulnerability.
f) Determine the potential impact of each vulnerability being exploited. Would the event result in loss of confidentiality, loss of integrity, or loss of availability of the information?
g) Determine RETA's level of risk. Based on the information gathered in the previous steps, make a determination to RETA's level of risk of each event.
h) Recommend security controls. Security controls that will mitigate the identified risks are evaluated during this step. Consider cost, operational impact, and effectiveness of each control.
i) Document the risk assessment results. The final step is to document the risk assessment, including the results of each step.

4.7.2 Risk Management Program
A formal risk management program must be implemented to cover any risks known to RETA (which should be identified through a risk assessment) and insure that reasonable security measures are in place to mitigate any identified risks to a level that will ensure the continued security of RETA's confidential and critical data.

4.8 Applicability of Other Policies
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions
Mobile Device Policy

1.0 Overview
Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.

2.0 Purpose
The purpose of this policy is to specify RETA standards for the use and security of mobile devices.

3.0 Scope
This policy applies to RETA data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with RETA data.

4.0 Policy

4.1 Physical Security
By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. RETA should
carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

- Laptop locks and cables can be used to secure laptops when in the office or other fixed locations.
- Mobile devices should be kept out of sight when not in use.
- Care should be given when using or transporting mobile devices in busy areas.
- As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.
- RETA should evaluate the data that will be stored on mobile devices and require remote wipe/remote delete technology. This technology allows a user or administrator to make the data on the mobile device unrecoverable.
- RETA should continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.

4.2 Data Security
If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting RETA data. The following sections specify the company’s requirements for data security as it relates to mobile devices.

4.2.1 Laptops
Use of encryption is not required but it is encouraged if data stored on the device is especially sensitive. Laptops should require a username and password or biometrics for login.

4.2.2 PDAs/Smart Phones
Use of a security passcode is required on all PDA/Smart phones if sensitive data will be accessible on the phone. Encryption is not required on PDAs/smart phones, but it is encouraged if data stored on the device is especially sensitive.

4.2.3 Mobile Storage Media
This section covers any USB drive, flash drive, memory stick or other personal data storage media. Any such device that contains sensitive RETA information must be encrypted. Storage of RETA data on such devices is such as meeting agendas and materials is permitted without passcodes or encryption.

4.2.4 Portable Media Players
No RETA data can be stored on personal media players.

4.2.5 Other Mobile Devices
Unless specifically addressed by this policy, storing RETA data on other mobile devices, or connecting such devices to RETA systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the IT Manager.

4.3 Connecting to Unsecured Networks
Users are permitted to connect RETA-provided computers to public or unsecured networks. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of RETA.
4.4 General Guidelines
The following guidelines apply to the use of mobile devices:

- Loss, Theft, or other security incident related to a company-provided mobile device must be reported promptly.
- Confidential data should not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device, it must be appropriately secured and comply with the Confidential Data policy.
- Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.
- Users should take precautions when storing company data on non-company-provided mobile devices. Storing confidential data on non-company-provided mobile devices is expressly prohibited.

4.5 Audits
RETA must conduct periodic reviews to ensure policy compliance. A sampling of mobile devices should be taken and audited against this policy on during the RETA annual audit.

4.6 Applicability of Other Policies
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Encryption** The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
- **Mobile Devices** A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.
- **Mobile Storage Media** A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.
- **Password** A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.
- **PDA** Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.
- **Portable Media Player** A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.
- **Sensitive Information** Any information that RETA staff recognize should be kept confidential is defined for purposes of this policy as “sensitive information” and should be treated accordingly.
are required to use good judgement in handling such information.

- **Smartphone** A mobile telephone that offers additional applications, such as PDA functions and email.

**NETWORK ACCESS AND AUTHENTICATION POLICY**

1.0 Overview
Consistent standards for network access and authentication are critical to RETA's information security and are often required by regulations or third-party agreements. Any user accessing the company's computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.

2.0 Purpose
The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the RETA network are authenticated in an appropriate manner, in compliance with RETA standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

3.0 Scope
The scope of this policy includes all users who have access to RETA-owned or RETA-provided computers or require access to the RETA network and/or systems. This policy applies to employees, guests, contractors, and anyone requiring access to the RETA network. Public access to RETA's externally-reachable systems, such as its RETA website or public web applications, are specifically excluded from this policy.

4.0 Policy

4.1 Account Setup
During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources is required.
- Users will be granted the least amount of network access required to perform his or her job function.
- Users will be granted access only if he or she accepts the Acceptable Use Policy.
- Access to the network will be granted in accordance with the Acceptable Use Policy.

4.2 Account Use
Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format (i.e., firstname-lastname, or firstinitial-lastname, etc.)
- Accounts must be password protected (refer to the Password Policy for more detailed information).
- Accounts must be for individuals only. Account sharing and group accounts are not permitted.
- User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.
• Occasionally guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed.
• Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the IT Manager or executive team, or as required by applicable regulations or third-party agreements.

4.3 Account Termination
Any person who leaves RETA as an employee, consultant or volunteer who had access to RETA databases or networks must immediately surrender all sensitive and confidential information. Network access and user accounts must end immediately by changing access codes or taking other precautions to protect sensitive RETA information. When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the company, that employee's account can be disabled. Human Resources must notify the IT Manager immediately in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.).

4.4 Authentication
User machines must be configured to request authentication against the domain at startup. If the domain is not available or authentication for some reason cannot occur, then authentication should occur on the local machine.

4.5 Use of Passwords
When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to RETA's Password Policy.

4.6 Remote Network Access
Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, RETA encourages additional scrutiny of users remotely accessing the network. RETA's standards dictate that username and password is an acceptable means of authentication as long as appropriate policies are followed. Remote access must adhere to the Remote Access Policy.

4.7 Screensaver Passwords
Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason, screensaver passwords are required. Employees must disable access to their computer screens whenever they are unattended.

4.8 Minimum Configuration for Access
Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users should update their antivirus software, as well as other critical software, to the latest versions before accessing the network.

4.9 Encryption
Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication
credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the RETA network or across a public network such as the Internet.

4.10 Failed Logons
Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, RETA must lock a user's account after five unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Manager.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

4.11 Non-Business Hours
While some security can be gained by removing account access capabilities during non-business hours, RETA does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because RETA's business requires all-hours access.

4.12 Applicability of Other Policies
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Antivirus Software** An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

- **Authentication** A security method used to verify the identity of a user and authorize access to a system or network.

- **Biometrics** The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

- **Encryption** The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

- **Password** A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

- **Smart Card** A plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.

- **Token** A small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.
NETWORK SECURITY POLICY

1.0 Overview
RETA wishes to provide a secure network infrastructure in order to protect the integrity of RETA data and mitigate risk of a security incident. While security policies typically avoid providing overly technical guidelines, this policy is necessarily a more technical document than most.

2.0 Purpose
The purpose of this policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support RETA's comprehensive set of security policies. However, this policy purposely avoids being overly-specific in order to provide some latitude in implementation and management strategies.

3.0 Scope
This policy covers all IT systems and devices that comprise the corporate network or that are otherwise controlled by RETA.

4.0 Policy

4.1 Network Device Passwords
A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords. All devices and applications must replace default passwords and access codes as soon as they are installed to protect the security of RETA data sources and information.

4.1.1 Password Construction
The following statements apply to the construction of passwords for network devices:

- Passwords should be at least 8 characters
- Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
- Passwords should be comprised of a mix of upper and lower-case characters
- Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.

4.1.2 Failed Logons
Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the company must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Manager.

In order to protect against account guessing, when logon failures occur the error message transmitted
to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

### 4.1.3 Change Requirements
Passwords must be changed according to RETA's Password Policy. Additionally, the following requirements apply to changing network device passwords:

- If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.
- If a RETA network or system administrator leaves RETA, all passwords to which the administrator could have had access must be changed immediately. This statement also applies to any consultant or contractor who has access to administrative passwords.
- Vendor default passwords must be changed when new devices are put into service.

### 4.1.4 Password Policy Enforcement
If possible, where passwords are used an application should be implemented that enforces RETA's password policies on construction, changes, re-use, lockout, etc.

### 4.1.5 Administrative Password Guidelines
As a general rule, administrative (also known as "root") access to systems should be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can have a major effect on the network, and, as such, network security. Additionally, administrative access to network devices should be logged.

### 4.2 Logging
The logging of certain events is an important component of good network management practices. Logging needs vary depending on the type of network system, and the type of data the system holds. The following sections detail RETA's requirements for logging and log review.

#### 4.2.1 Application Servers
Logs from application servers are of interest since these servers often allow connections from a large number of internal and/or external sources. These devices are often integral to smooth business operations.

Examples: Web, email, database servers

Requirement: Logging of at least errors, faults, and login failures is encouraged but not required. No passwords should be contained in logs.

#### 4.2.2 Network Devices
Logs from network devices are of interest since these devices control all network traffic and can have a huge impact on RETA's security.

Examples: Firewalls, network switches, routers

Requirement: Logging of at least errors, faults, and login failures is encouraged but not required. No passwords should be contained in logs.
4.2.3 Critical Devices
Critical devices are any systems that are critically important to business operations. These systems may also fall under other categories above - in any cases where this occurs, this section shall supersede.

Examples: File servers, lab or manufacturing machines, systems storing intellectual property

Requirements: Logging of at least errors, faults, and login failures is encouraged but not required. No passwords should be contained in logs.

4.2.4 Log Management
While logging is important to RETA’s network security, log management can become burdensome if not implemented appropriately. As logs grow, so does the time required to review the logs. For this reason, RETA recommends that a log management application be considered.

4.2.5 Log Review
Device logs do little good if they are not reviewed on a regular basis. Log management applications can assist in highlighting important events, however, a member of RETA’s IT team should still review the logs as frequently as is reasonable.

4.2.6 Log Retention
Logs should be retained in accordance with RETA’s Retention Policy. Unless otherwise determined by the IT manager, logs should be considered operational data.

4.3 Firewalls
Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks must be separated from the RETA network through the use of a firewall.

4.3.1 Configuration
The following statements apply to RETA's implementation of firewall technology:

- Firewalls must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
- No unnecessary services or applications should be enabled on firewalls. The company should use 'hardened' systems for firewall platforms, or appliances.
- Clocks on firewalls should be synchronized with RETA's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
- The firewall ruleset must be documented and audited annually. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.
- For its own protection, the firewall ruleset should include a "stealth rule," which forbids connections to the firewall itself.
- The firewall should log dropped or rejected packets.

4.3.2 Outbound Traffic Filtering
Firewalls are often configured to block only inbound connections from external sources; however, by
filtering outbound connections from the network, security can be greatly improved. This practice is also referred to as "Egress Traffic Filtering."

Blocking outbound traffic prevents users from accessing unnecessary, and many times, dangerous services. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked. This type of filtering would block root kits, viruses, and other malicious tools if a host were to become compromised. This will also prevent remote desktops from accessing the internal network.

RETA encourages outbound filtering if possible, but it is not required. RETA’s IT consultant should specify permitted “good” services if filtering is deemed possible.

4.4 Networking Hardware
Networking hardware, such as routers, switches, hubs, bridges, and access points, should be implemented in a consistent manner. The following statements apply to RETA’s implementation of networking hardware:

- Networking hardware must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
- Clocks on all network hardware should be synchronized using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
- If possible for the application, switches are preferred over hubs. When using switches RETA should use VLANs to separate networks if it is reasonable and possible to do so.
- Access control lists should be implemented on network devices that prohibit direct connections to the devices. Exceptions to this are management connections that can be limited to known sources.
- Unused services and ports should be disabled on networking hardware.
- Access to administrative ports on networking hardware should be restricted to known management hosts and otherwise blocked with a firewall or access control list.

4.5 Network Servers
Servers typically accept connections from a number of sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. The following statements apply to RETA’s use of network servers:

- Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.
- Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.
- If possible, a standard installation process should be developed for RETA’s network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.
- Clocks on network servers should be synchronized with RETA’s other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

4.6 Intrusion Detection/Intrusion Prevention
Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the
activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically take action when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic.

RETA neither requires nor prohibits the use of IDS or IPS systems. The decision to use IDS/IPS systems is left to the discretion of the IT Manager.

4.7 Security Testing

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining RETA’s network security. Security testing can be provided by IT Staff members but is often more effective when performed by a third party with no connection to RETA’s day-to-day Information Technology activities. The following sections detail RETA’s requirements for security testing.

4.7.1 Internal Security Testing

Internal security testing refers to testing of the internal network performed by members of RETA’s IT team. Internal testing should not replace external testing; however, when external testing is not practical for any reason, or as a supplement to external testing, internal testing can be helpful in assessing the security of the network.

Internal security testing is allowable, but only by employees whose job functions are to assess security, and only with permission of the IT Manager. Internal testing should have no measurable negative impact on RETA’s systems or network performance.

4.7.2 External Security Testing

External security testing, which is testing by a third-party entity, is an excellent way to audit RETA’s security controls. The IT Manager must determine to what extent this testing should be performed, and what systems/applications it should cover.

External testing must not negatively affect network performance during business hours or network security at any time.

"Penetration testing" to protect RETA from the active exploitation of RETA vulnerabilities by a trusted third party should be conducted periodically. If penetration testing is performed, it must not negatively impact RETA systems or data.

RETA encourages external security testing but does not provide rigid guidelines regarding at what intervals the testing should occur. Testing should be performed as often as is necessary, as determined by the IT Manager.

4.8 Disposal of Information Technology Assets

IT assets, such as network servers and routers, often contain sensitive data about RETA’s network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify RETA must be removed before disposal.
- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.
- At a minimum, data wiping must be used. Simply reformatting a drive or deleting data does not make
the data unrecoverable. If wiping is used, RETA must use the most secure commercially-available methods for data wiping. Alternatively, RETA has the option of physically destroying the data storage mechanism from the device (such as its hard drive or solid-state memory).

4.9 Network Compartmentalization
Good network design is integral to network security. By implementing network compartmentalization, which is separating the network into different segments, RETA will reduce its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points. RETA requires the following with regard to network compartmentalization:

4.9.1 Higher Risk Networks
Examples: Guest network, wireless network

Requirements: Segmentation of higher risk networks from RETA's internal network is required.

4.9.2 Externally-Accessible Systems
Examples: Email servers, web servers

Requirements: Segmentation of externally-accessible systems from RETA's internal network required.

4.9.3 Internal Networks
Examples: Sales, Finance, Human Resources

Requirements: Segmentation of internal networks from one another can improve security as well as reduce chances that a user will access data that he or she has no right to access. RETA encourages, but does not require, such segmentation.

4.10 Network Documentation
Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that RETA's IT Staff has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable.

Network documentation should include:

- Network diagram(s)
- System configurations
- Firewall ruleset
- IP Addresses
- Access Control Lists

RETA encourages network documentation but does not require it.

4.11 Antivirus/Anti-Malware
Computer viruses and malware are pressing concerns in today's threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and RETA.
The company provides the following guidelines on the use of antivirus/anti-malware software:

- All RETA-provided user workstations must have antivirus/anti-malware software installed.
- Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.
- Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually.

**4.12 Software Use Policy**

Software applications can create risk in a number of ways, and thus certain aspects of software use must be covered by this policy. RETA provides the following requirements for the use of software applications:

- Only legally licensed software may be used. Licenses for RETA's software must be stored in a secure location.
- Open source and/or public domain software can only be used with the permission of the IT Manager.
- Software should be kept reasonably up-to-date by installing new patches and releases from the manufacturer.
- Vulnerability alerts should be monitored for all software products that RETA uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

**4.13 Maintenance Windows and Scheduled Downtime**

Certain tasks require that network devices be taken offline, either for a simple re-boot, an upgrade, or other maintenance. When this occurs, the IT Staff should make every effort to perform the tasks at times when they will have the least impact on network users.

**4.14 Change Management**

Documenting changes to network devices is a good management practice and can help speed resolution in the event of an incident. The IT Staff must document hardware and/or configuration changes to network devices in a "change log." Network devices must bear a sticker or tag indicating essential information, such as the device name, IP address, MAC address, asset information, and any additional data that may be helpful, such as information about cabling.

**4.15 Suspected Security Incidents**

When a security incident is suspected that may impact a network device, the IT Staff should refer to RETA's Incident Response policy for guidance.

**4.16 Redundancy**

Redundancy can be implemented on many levels, from redundancy of individual components to full site-redundancy. As a general rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost. RETA wishes to provide the IT Manager with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed, and should include some or all of the following:

- Hard drive redundancy, such as mirroring or RAID
- Server level redundancy, such as clustering or high availability
- Component level redundancy, such as redundant power supplies or redundant NICs
- Keeping hot or cold spares onsite
4.17 **Manufacturer Support Contracts**
Outdated products can result in a serious security breach. When purchasing critical hardware or software, RETA should consider purchasing a maintenance plan, support agreement, or software subscription that will allow RETA to receive updates to the software and/or firmware for a specified period of time. If such a plan is purchased, it should meet the following standards:

Hardware: The arrangement should allow for repair/replacement of the device within an acceptable time period, as determined by the IT Manager, as well as firmware or embedded software updates.

Software: The arrangement should allow for updates, upgrades, and hotfixes for a specified period of time.

4.18 **Security Policy Compliance**
It is RETA's intention to comply with this policy not just on paper but in its everyday processes as well. With that goal in mind, RETA requires the following:

4.18.1 **Security Program Manager**
An employee must be designated as a manager for RETA's security program. He or she will be responsible for RETA's compliance with this security policy and any applicable security regulations. This employee must be responsible for A) the initial implementation of the security policies, B) ensuring that the policies are disseminated to employees, C) training and retraining of employees on RETA's information security program (as detailed below), D) any ongoing testing or analysis of RETA's security in compliance with this policy, E) updating the policy as needed to adhere with applicable regulations and the changing information security landscape.

4.18.2 **Security Training**
A training program must be implemented that will detail RETA's information security program to all users and/or employees covered by the policy, as well as the importance of data security. Employees must sign off on the receipt of, and in agreement to, the user-oriented policies. Re-training should be performed at least annually.

4.18.3 **Security Policy Review**
RETA's security policies should be reviewed at least annually as part of the RETA Annual Audit Plan. Additionally, the policies should be reviewed when there is an information security incident, or a material change to RETA's security policies. As part of this evaluation, RETA should review:

- Any applicable regulations for changes that would affect RETA's compliance or the effectiveness of any deployed security controls.
- If RETA's deployed security controls are still capable of performing their intended functions.
- If technology or other changes may have an effect on RETA's security strategy.
- If any changes need to be made to accommodate future IT security needs.

4.19 **Applicability of Other Policies**
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.
5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **ACL** A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.
- **Antivirus Software** An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.
- **Firewall** A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.
- **Hub** A network device that is used to connect multiple devices together on a network.
- **IDS** Stands for Intrusion Detection System. A network monitoring system that detects and alerts to suspicious activities.
- **IPS** Stands for Intrusion Prevention System. A networking monitoring system that detects and automatically blocks suspicious activities.
- **NTP** Stands for Network Time Protocol. A protocol used to synchronize the clocks on networked devices.
- **Password** A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.
- **RAID** Stands for Redundant Array of Inexpensive Disks. A storage system that spreads data across multiple hard drives, reducing or eliminating the impact of the failure of any one drive.
- **Switch** A network device that is used to connect devices together on a network. Differs from a hub by segmenting computers and sending data to only the device for which that data was intended.
- **VLAN** Stands for Virtual LAN (Local Area Network). A logical grouping of devices within a network that act as if they are on the same physical LAN segment.
- **Virus** Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

OUTSOURCING POLICY

1.0 Overview

Outsourcing is a logical practice when specialized expertise is required, which happens frequently in the field of Information Technology (IT). Trust is necessary for a successful outsourcing relationship, however, RETA must be protected by a policy that details and enforces the terms of the outsourcing relationship.
2.0 Purpose
The purpose of this policy is to specify actions to take when selecting a provider of outsourced IT services, standards for secure communications with the provider, and what contractual terms should be in place to protect RETA.

3.0 Scope
This policy covers any IT services being considered for outsourcing.

4.0 Policy

4.1 Deciding to Outsource
Outsourcing IT services is often necessary but should be carefully considered, since by nature a certain amount of control will be lost by doing so. The following questions must be affirmatively answered before outsourcing is considered:

- Can the service be performed better or less expensively by a third-party provider?
- Would it be cost-prohibitive or otherwise unreasonable to perform this service in-house?
- Will outsourcing the service positively affect the quality of this service?
- Is the cost of this service worth the benefit?
- Are any risks associated with outsourcing the service worth the benefit?

4.2 Outsourcing Core Functions
RETA permits the outsourcing of critical and/or core functions of RETA's Information Technology infrastructure as long as this policy is followed. Examples of these types of functions are data backups, remote access, security, and network management.

4.3 Evaluating a Provider
Once the decision to outsource an Information Technology function has been made, selecting the appropriate provider is critical to the success of the endeavor. Due diligence must be performed after the potential providers have been pared to a short list of two to three companies. Due diligence must always be performed prior to a provider being selected.

Due diligence should include an evaluation of the provider's ability to perform the requested services. It should involve a review of the provider's reputation, technical ability, and experience providing the same services to similar companies.

If the outsourced service will involve the provider having access to, or storing RETA's confidential information, due diligence should cover the provider's security controls for access to the confidential information.

4.4 Security Controls
The outsourcing contract must provide a mechanism for secure information exchange with the service provider. This will vary with the type of service being outsourced, but may include remote access, VPN, or encrypted file exchange.

RETA and provider must also maintain a mechanism for verifying the identity of the other party and confirming changes to the service. This will prevent an attacker from using social engineering tactics to gain...
access to RETA data.

4.5 Outsourcing Contracts
All outsourced Information Technology services must be governed by a legal contract, with an original of the executed contract maintained by RETA.

Contracts must:

- Cover a specified time period
- Specify exact pricing for the services
- Specify how the provider will treat confidential information
- Include a non-disclosure agreement
- Specify services to be provided, including Service Level Agreements and penalties for missing the levels
- Allow for cancellation if contractual terms are not met
- Specify standards for subcontracting of the services and reassignment of contract
- Cover liability issues
- Describe how and where to handle contractual disputes

4.6 Access to Information
The provider must be given the least amount of network, system, and/or data access required to perform the contracted services. This access must follow applicable policies and be periodically audited.

4.7 Applicability of Other Policies
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Backup** To copy data to a second location, solely for the purpose of safe keeping of that data.
- **Encryption** The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
- **Network Management** A far-reaching term that refers to the process of maintaining and administering a network to ensure its availability, performance, and security.
- **Remote Access** The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.
- **VPN** A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.
PASSWORD POLICY

1.0 Overview
A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

2.0 Purpose
The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

3.0 Scope
This policy applies to any person who is provided an account on the organization's network or systems, including: employees, guests, contractors, partners, vendors, etc.

4.0 Policy

4.1 Construction
The best security against a password incident is simple: following a sound password construction strategy. The organization mandates that users adhere to the following guidelines on password construction:

- Passwords should be at least 8 characters
- Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
- Passwords should be comprised of a mix of upper and lower-case characters
- Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary
- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this way as well, for example an 'i' can be changed to a '!.'

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

4.2 Confidentiality
Passwords should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization
passwords:

- Users must not disclose their passwords to anyone
- Users must not share their passwords with others (co-workers, supervisors, family, etc.)
- Users must not write down their passwords and leave them unsecured
- Users must not check the "save password" box when authenticating to applications that contain secure RETA data or information
- Users must not use the same password for different systems and/or accounts that contain secure RETA data or information
- Users must not send passwords via email
- Users must not re-use passwords

4.3 Change Frequency
In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. RETA does not wish to apply any hard limits to when passwords must be changed but asks that users exercise discretion and change passwords sporadically.

4.4 Incident Reporting
Since compromise of a single password can have a catastrophic impact on network security, it is the user’s responsibility to immediately report any suspicious activity involving his or her passwords to the IT Manager. Any request for passwords over the phone or email, whether the request came from RETA personnel or not, should be expediently reported. When a password is suspected to have been compromised the IT Manager will request that the user, or users, change all his or her passwords. Any program or application that includes provisions or two-factor authentication should be enabled.

4.5 Applicability of Other Policies
This document is part of the organization's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Authentication** A security method used to verify the identity of a user and authorize access to a system or network.
- **Password** A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.
- **Two Factor Authentication** A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.
**PHYSICAL SECURITY POLICY**

**1.0 Overview**
Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations and servers and transmitted on RETA's physical network infrastructure. In order to secure RETA data, thought must be given to the security of RETA's physical Information Technology (IT) resources to ensure that they are protected from standard risks.

**2.0 Purpose**
The purpose of this policy is to protect RETA's physical information systems by setting standards for secure operations.

**3.0 Scope**
This policy applies to the physical security of RETA's information systems, including, but not limited to, all RETA-owned or RETA-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting RETA's office is covered by this policy.

Please note that this policy covers the physical security of RETA's Information Technology infrastructure and does not cover the security of non-IT items or the important topic of employee security. While there will always be overlap, care must be taken to ensure that this policy is consistent with any existing physical security policies.

**4.0 Policy**

**4.1 Choosing a Site**
When possible, thought should be given to selecting a site for IT Operations that is secure and free of unnecessary environmental challenges. This is especially true when selecting a datacenter or a site for centralized IT operations. At a minimum, RETA's site should meet the following criteria:

- A site should not be particularly susceptible to fire, flood, earthquake, or other natural disasters.
- A site should not be located in an area where the crime rate and/or risk of theft is higher than average.
- A site should have the fewest number of entry points possible.

If these criteria cannot be effectively met for any reason, RETA should consider outsourcing its data in whole or in part to a third-party datacenter or hosting provider, provided that such a company can cost effectively meet or exceed RETA's requirements.

**4.2 Security Zones**
At a minimum, RETA will maintain standard security controls, such as locks on exterior doors and/or an alarm system, to secure RETA's assets. In addition to this RETA must provide security in layers by designating different security zones within the building. Security zones should include:

**Public** This includes areas of the building or office that are intended for public access.
• Access Restrictions: None
• Additional Security Controls: None
• Examples: Lobby, common areas of building

**Company** This includes areas of the building or office that are used only by employees and other persons for official RETA business.

• Access Restrictions: Only RETA personnel and approved/escorted guests
• Additional Security Controls: None
• Examples: Hallways, private offices, work areas, conference rooms

**Private** This includes areas that are restricted to use by certain persons within RETA, such as executives, scientists, engineers, and IT personnel, for security or safety reasons.

• Access Restrictions: Only specifically approved personnel
• Additional Security Controls: None
• Examples: Executive offices, lab space, network room, manufacturing area, financial offices, and storage areas.

### 4.3 Access Controls

Access controls are necessary to restrict entry to RETA premises and security zones to only approved persons. There are several standard ways to do this, which are outlined in this section, along with RETA’s guidelines for their use.

#### 4.3.1 Keys & Keypads

The use of keys and keypads is acceptable. These security mechanisms are the most inexpensive and is the most familiar to users. The disadvantage is that RETA has no control, aside from changing the locks or codes, over how and when the access is used. Keys can be copied, and keypad codes can be shared or seen during input. However, used in conjunction with another security strategy, such as an alarm system, good security can be obtained with keys and keypads.

#### 4.3.2 Keycards & Biometrics

While keycards and biometrics are allowable forms of access controls, RETA does not require their use at this time.

Keycards and biometrics have an advantage over keys in that access policies can be tuned to the individual user. Schedules can be set to forbid off-hours access, or forbid users from accessing a security zone where they are not authorized. Perhaps best of all, these methods allow for control over exactly who possesses the credentials. If a keycard is lost or stolen it can be immediately disabled. If an employee is terminated or resigns, that user's access can be disabled. The granular control offered by keycards and biometrics make them appealing access control methods.

#### 4.3.3 Alarm System

A security alarm system is a good way to minimize risk of theft or reduce loss in the event of a theft. RETA mandates the use of professionally monitored alarm system. The system must be monitored 24x7, with RETA personnel being notified if an alarm is tripped at any time.
4.4 Physical Data Security
Certain physical precautions must be taken to ensure the integrity of RETA's data. At a minimum, the following guidelines must be followed:

- Computer screens should be positioned where information on the screens cannot be seen by outsiders.
- Confidential and sensitive information should not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information.
- Users must log off or shut down their workstations when leaving for an extended time period, or at the end of the workday.
- Network cabling should not run through unsecured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).
- RETA recommends disabling network ports that are not in use.

4.5 Physical System Security
In addition to protecting the data on RETA's information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft.

4.5.1 Minimizing Risk of Loss and Theft
In order to minimize the risk of data loss through loss or theft of RETA property, the following guidelines must be followed:

- Unused systems: If a system is not in use for an extended period of time it should be moved to a secure area or otherwise secured.
- Mobile devices: Special precautions must be taken to prevent loss or theft of mobile devices. Refer to RETA's Mobile Device Policy for guidance.
- Systems that store confidential data: Special precautions must be taken to prevent loss or theft of these systems. Refer to RETA's Confidential Data Policy for guidance.

4.5.2 Minimizing Risk of Damage
Systems that store RETA data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimize the risk of damage, the following guidelines must be followed:

- Environmental controls should keep the operating environment of RETA systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.
- Proper grounding procedures must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimized.
- Strong magnets must not be used in proximity to RETA systems or media.
- Except in the case of a fire suppression system, open liquids must not be located above RETA systems. Technicians working on or near RETA systems should never use the systems as tables for beverages. Beverages must never be placed where they can be spilled onto RETA systems.
- Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for important systems and encouraged for all systems. These devices must carry a warranty that covers the value of the systems if the systems were to be damaged by a power surge.
4.6 Fire Prevention
It is RETA's policy to provide a safe workplace that minimizes the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of IT systems, the fire danger in these areas is typically higher than other areas of RETA's office. The guidelines below are intended to be specific to RETA's information technology assets and should conform to RETA's overall fire safety policy.

- Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.
- Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, or surge protectors together.
- Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.
- Only electrical equipment that has been approved by Underwriters Laboratories and bears the UL seal of approval must be used.
- Unused electrical equipment should be turned off when not in use for extended periods of time (i.e., during non-business hours) if possible.
- Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other electrical devices must be checked for excessive wear or cracks. If overly-worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.
- A smoke alarm monitoring service must be used that will alert a designated RETA employee if an alarm is tripped during non-business hours.

4.7 Entry Security
It is RETA's policy to provide a safe workplace for employees. Monitoring those who enter and exit the premises is a good security practice in general but is particularly true for minimizing risk to RETA systems and data. The guidelines below are intended to be specific to RETA's information technology assets and should conform to RETA's overall security policy.

4.7.1 Use of Identification Badges
Identification (ID) badges are useful to identify authorized persons on RETA premises. RETA has established the following guidelines for the use of ID badges.

- Employees: ID badges are not required.
- Non-employees/Visitors: Visitor badges are not required for individual visitors, though generic visitor badges are encouraged when they could help identify visitors to staff and others while they are in RETA offices.

4.7.2 Sign-in Requirements
RETA does not wish to establish any requirements for employee/visitor sign-in. Use of a visitor sign-in register is encouraged.

4.7.3 Visitor Access
Visitors should be given only the level of access to RETA premises that is appropriate to the reason for their visit. After checking in, visitors must be escorted unless they are considered "trusted" by
RETA. Examples of a trusted visitor may be RETA’s legal counsel, financial advisor, RETA Board and Committee members, RETA consultants and contractors, or a courier that frequents the office. Specific requirements for each person will be decided by RETA executive staff on a case-by-case basis.

4.8 Applicability of Other Policies
This document is part of RETA’s cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Biometrics** The process of using a person’s unique physical characteristics to prove that person’s identity. Commonly used are fingerprints, retinal patterns, and hand geometry.
- **Datacenter** A location used to house a company’s servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.
- **Keycard** A plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.
- **Keypad** A small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.
- **Mobile Device** A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.
- **PDA** Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.
- **Smartphone** A mobile telephone that offers additional applications, such as PDA functions and email.
- **Uninterruptible Power Supplies (UPSs)** A battery system that automatically provides power to electrical devices during a power outage for a certain period of time. Typically, also contains power surge protection.

REMOTE ACCESS POLICY

1.0 Overview
It is often necessary to provide access to RETA information resources to employees or others working outside RETA’s network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.
2.0 Purpose
This policy is provided to define standards for accessing RETA information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

3.0 Scope
The scope of this policy covers all employees, contractors, and external parties that access company resources over a third-party network, whether such access is performed with RETA-provided or non-RETA-provided equipment.

4.0 Policy

4.1 Prohibited Actions
Remote access to RETA systems is only to be offered through a RETA-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router, or other remote access device on a RETA system without the approval of the IT Manager.
- Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from the IT Manager.
- Use of non-RETA-provided remote access software.
- Split Tunneling to connect to an insecure network in addition to the RETA network, or in order to bypass security restrictions.

4.2 Use of non-RETA-provided Machines
Accessing the RETA network through home or public machines can present a security risk, as RETA cannot completely control the security of the system accessing the network. Use of non-RETA-provided machines to access the RETA network is permitted as long as this policy is adhered to, and as long as the machine meets the following criteria:

- It has up-to-date antivirus software installed
- Its software patch levels are current
- It is protected by a firewall

When accessing the network remotely, users must not store confidential information on home or public machines.

4.3 Client Software
RETA will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in order to protect the data during transmission. The user is responsible for maintaining a secure system, free of viruses and backdoors.

4.4 Network Access
There are no restrictions on what information or network segments users can access when working remotely, however the level of access should not exceed the access a user receives when working in the office.
4.5 **Idle Connections**
Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to RETA’s network must be timed out after 1 hour of inactivity.

4.6 **Applicability of Other Policies**
This document is part of RETA’s cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 **Enforcement**
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 **Definitions**
- **Modem** A hardware device that allows a computer to send and receive digital information over a telephone line.
- **Remote Access** The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.
- **Split Tunneling** A method of accessing a local network and a public network, such as the Internet, using the same connection.
- **Timeout** A technique that drops or closes a connection after a certain period of inactivity.
- **Two Factor Authentication** A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

**RETENTION POLICY**

1.0 **Overview**
The need to retain data varies widely with the type of data. Some data can be immediately deleted, and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the company's guidelines on retention are consistently applied throughout the organization.

2.0 **Purpose**
The purpose of this policy is to specify RETA's guidelines for retaining different types of data.

3.0 **Scope**
The scope of this policy covers all RETA data stored on RETA-owned, RETA-leased, and otherwise RETA-provided systems and media, regardless of location.
Note that the need to retain certain information can be mandated by local, industry, or federal regulations. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

4.0 Policy

4.1 Reasons for Data Retention
RETA does not wish to simply adopt a "save everything" mentality. That is not practical or cost-effective and would place an excessive burden on the IT Staff to manage the constantly-growing amount of data.

Some data, however, must be retained in order to protect RETA’s interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:

- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation

4.2 Data Duplication
As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying RETA's data, it is important to also understand where that data may be stored, particularly as duplicate copies, so that this policy may be applied to all duplicates of the information.

4.3 Retention Requirements
This section sets guidelines for retaining the different types of RETA data.

- **Personal** There are no retention requirements for personal data. In fact, RETA requires that it be deleted or destroyed when it is no longer needed.
- **Public** Public data must be retained for 3 years.
- **Operational** Most RETA data will fall in this category. Operational data must be retained for 5 years.
- **Critical** Critical data must be retained for 10 years beyond the expiration date of any certified person’s RETA credential.
- **Confidential** Confidential data must be retained for 10 years beyond the expiration date of any certified person’s RETA credential.

4.4 Retention of Encrypted Data
If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

4.5 Data Destruction
Data destruction is a critical component of a data retention policy. Data destruction ensures that RETA will
not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

When the retention timeframe expires, RETA must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of RETA's executive team.

RETA specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself or destroying data in an attempt to cover up a violation of law or RETA policy.

4.6 Applicability of Other Policies
This document is part of RETA’s cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Backup** To copy data to a second location, solely for the purpose of safe keeping of that data.
- **Encryption** The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.
- **Encryption Key** An alphanumeric series of characters that enables data to be encrypted and decrypted.

TEST DEVELOPMENT AND SECURITY POLICY

1.0 Overview
RETA certification examinations are developed under the direction and supervision of RETA’s Consulting Psychometrician. Test development and security for all RETA examinations is based on guidelines for credentialing exams as specified in the 2014 *Standards for Educational and Psychological Testing* developed by the American Educational Research Association, the American Psychological Association, and the National Council on Educational Measurement.

2.0 Purpose
The purpose of this policy is to specify RETA’s guidelines for protecting the fairness, validity and security of all RETA certification examinations.

3.0 Scope
The scope of this policy covers all RETA examinations.
4.0 Policy

4.1 Test Development Procedures
The RETA Certification Committee (CertComm) serves as the “scheme committee” as defined under ANSI Standard 17024. CertComm procedures are documented separately in the RETA Policies and Procedures Manual under Section 500, Certification, and in the CertComm Operations Manual.

4.2 Access to Confidential and Secure Test Content
RETA’s Consulting Psychometrician controls all access to RETA item banks, test forms and other secure test materials. All reviews of content for RETA exam questions occurs under his/her direct supervision. CertComm members and other consultants who may participate in this process are required to sign and adhere to Non-Disclosure and Confidentiality Agreements specifying that they will not share any secure test content or materials at any time with anyone.

4.3 Test Delivery Vendor Security and Support
Kryterion, RETA’s test delivery vendor, keeps all RETA test content, test forms and documents required for secure design, control and administration of RETA examinations confidential. Test questions for RETA certification exams are delivered through encrypted cloud-based delivery channels to each test center. Each question is removed from the test station computer terminal as soon as a candidate records his or her answer to the question.

RETA’s Consulting Psychometrician places required questions and test forms into Kryterion’s system and controls designations of all active test forms. Kryterion’s technical support may include support in delivery of these services at the request of RETA’s Certification Manager when RETA’s Consulting Psychometrician is not available.

4.4 Types of RETA Examinations

Book Tests RETA offers end-of-course examinations for unproctored online delivery through Kryterion’s system. Candidates who earn a passing score on these Book Tests receive credit toward recertification of a RETA credential. Candidates may take Book Tests at home, at work or on any computer that has the necessary Internet connection.

Practice Tests RETA also provides practice certification examinations for unproctored online delivery through Kryterion’s system. Candidates who complete Practice Tests receive diagnostic reports informing them where questions they answer incorrectly are supported in RETA books and study materials. Candidates may take Practice Tests at home, at work or on any computer that has the necessary Internet connection.

Certification Examinations RETA currently provides four certification examinations through secure, proctored online delivery in approved testing centers throughout the U.S.
- Certified Assistant Refrigeration Operator (CARO)
- Certified Industrial Refrigeration Operator (CIRO)
- Certified Refrigeration Energy Specialist (CRES)
- RETA-Authorized Instructor (RAI)

Each of these certification examinations is administered under strict security and controls under the
supervision of proctors who are screened and approved to maintain the security, validity and integrity of each RETA exam.

4.5 Secure Test Centers

Kryterion Testing Network (KTN) Test Centers  Kryterion maintains a network of over 400 U.S. test centers where secure examinations can be administered under the direct supervision of trained and approved proctors. Kryterion also offers examinations in nearly 400 international test centers. RETA examinations may become available in selected international test centers under mutual agreements as these opportunities develop.

RETA Testing Network Centers  RETA approves and manages test centers in both public and private training facilities that may provide training in industrial refrigeration content. RETA delivers these exams through Kryterion’s cloud-based secure system. All exams in RETA Testing Network Centers are supervised by trained and approved proctors under rules specified in the RETA Testing Network Operations Manual and the RETA Proctor Guide. These also document administrative rules and procedures, including that no person who is involved in training candidates for RETA certification is ever permitted in the test center while any RETA certification test is underway.

5.0 Enforcement

This policy will be enforced by RETA’s Certification Manager, the Executive Team and the Consulting Psychometrician. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of testing in a center or facility. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Proctor**  An individual who is trained and qualified to supervise secure administration of RETA examinations in approved test centers.
- **Test Centers**  Locations that are required to meet test security and administrative procedures by Kryterion and/or RETA.

THIRD PARTY CONNECTION POLICY

1.0 Overview

Direct connections to external entities are sometimes required for business operations. These connections are typically to provide access to vendors or customers for service delivery. Since RETA's security policies and controls do not extend to the users of the third parties' networks, these connections can present a significant risk to the network and thus require careful consideration.

2.0 Purpose

The policy is intended to provide guidelines for deploying and securing direct connections to third parties.
3.0 Scope
The scope of this policy covers all direct connections to RETA's network from non-RETA owned networks. This policy excludes remote access and Virtual Private Network (VPN) access, which are covered in separate policies.

4.0 Policy

4.1 Use of Third Party Connections
Third party connections are to be discouraged and used only if no other reasonable option is available. When it is necessary to grant access to a third party, the access must be restricted and carefully controlled. A requester of a third-party connection must demonstrate a compelling business need for the connection. This request must be approved and implemented by the IT Manager.

4.2 Security of Third Party Access
Third party connections require additional scrutiny. The following statements will govern these connections:

- Connections to third parties must use a firewall or Access Control List (ACL) to separate RETA's network from the third party's network.
- Third parties will be provided only the minimum access necessary to perform the function requiring access. If possible, this should include time-of-day restrictions to limit access to only the hours when such access is required.
- Wherever possible, systems requiring third party access should be placed in a public network segment or demilitarized zone (DMZ) in order to protect internal network resources.
- If a third-party connection is deemed to be a serious security risk, the IT Manager will have the authority to prohibit the connection. If the connection is absolutely required for business functions, additional security measures should be taken at the discretion of the IT Manager.
- Third parties must sign and adhere to a Non-Disclosure and Confidentiality Statement for all information about RETA members, candidates, staff and programs as specified by RETA’s Executive Team. For example, the Northwest Energy Efficiency Alliance (NEEA) and all organizations participating in developing RETA’s Certified Refrigeration Energy Specialist (CRES) certification have been required to provide such agreements.

4.3 Restricting Third Party Access
Best practices for a third-party connection require that the link be held to higher security standards than an intra-RETA connection. As such, the third party must agree to:

- Restrict access to RETA's network to only those users that have a legitimate business need for access.
- Provide RETA with the names and any other requested information about individuals that will have access to the connection. RETA reserves the right to approve or deny this access based on its risk assessment of the connection.
- Supply RETA with on-hours and off-hours contact information for the person or persons responsible for the connection.
- (If confidential data is involved) Provide RETA with the names and any other requested information about individuals that will have access to RETA's confidential data. The steward or owner of the confidential data will have the right to approve or deny this access for any reason.
4.4 Auditing of Connections
In order to ensure that third-party connections are in compliance with this policy, they must be audited quarterly.

4.5 Applicability of Other Policies
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Access Control List (ACL)** A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

- **Demilitarized Zone (DMZ)** A perimeter network, typically inside the firewall but external to the private or protected network, where publicly-accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.

- **Firewall** A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

- **Third Party Connection** A direct connection to a party external to the company. Examples of third party connections include connections to customers, vendors, partners, or suppliers.

VPN POLICY

1.0 Overview
A Virtual Private Network, or VPN, provides a method to communicate with remote sites securely over a public medium, such as the Internet. A site-to-site VPN is a dependable and inexpensive substitute for a point-to-point Wide Area Network (WAN). Site-to-site VPNs can be used to connect the LAN to a number of different types of networks: branch or home offices, vendors, partners, customers, etc. As with any external access, these connections need to be carefully controlled through a policy.

2.0 Purpose
This policy details RETA's standards for site-to-site VPNs. The purpose of this policy is to specify the security standards required for such access, ensuring the integrity of data transmitted and received, and securing the VPN pathways into the network.

3.0 Scope
The scope of this policy covers all site-to-site VPNs that are a part of RETA’s infrastructure, including both
sites requiring access to RETA’s network (inbound) and sites where RETA connects to external resources (outbound). Note that remote access VPNs are covered under a separate Remote Access Policy.

4.0 Policy

4.1 Encryption
Site-to-site VPNs must utilize strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards, such as Triple DES or AES.

4.2 Authentication
Site-to-site VPNs must utilize a strong password, pre-shared key, certificate, or other means of authentication to verify the identity the remote entity. The strongest authentication method available must be used, which can vary from product-to-product.

4.3 Implementation
When site-to-site VPNs are implemented, they should adhere to the policy of least access, providing access limited to only what is required for business purposes if possible. This should be done on a best-effort basis and is not a requirement.

4.4 Management
RETA should manage its own VPN gateways, meaning that a third party must not provide and manage both sides of the site-to-site VPN, unless this arrangement is covered under an outsourcing agreement. If an existing VPN is to be changed, the changes must only be performed with the approval of the IT Manager.

4.5 Logging and Monitoring
RETA does not require logging or monitoring traffic related to the site-to-site VPN.

4.6 Encryption Keys
Site-to-site VPNs are created with pre-shared keys. The security of these keys is critical to the security of the VPN, and by extension, the network. Encryption keys should be changed periodically.

If certificates are used instead of pre-shared keys, the certificates should expire and be re-generated after three years.

4.7 Applicability of Other Policies
This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement
This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.
6.0 Definitions

- **Certificate** Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.
- **Demilitarized Zone (DMZ)** A perimeter network, typically inside the firewall but external to the private or protected network, where publicly-accessible machines are located. A DMZ allows higher-risk machines to be segregated from the internal network while still providing security controls.
- **Encryption** The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
- **Remote Access VPN** A VPN implementation at the individual user level. Used to provide remote and traveling users secure network access.
- **Site-to-Site VPN** A VPN implemented between two static sites, often different locations of a business.
- **Virtual Private Network (VPN)** A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

**WIRELESS ACCESS POLICY**

1.0 Overview

Wireless communication is playing an increasingly important role in the workplace. In the past, wireless access was the exception; it has now become the norm in many companies. However, while wireless access can increase mobility and productivity of users, it can also introduce security risks to the network. These risks can be mitigated with a sound Wireless Access Policy.

2.0 Purpose

The purpose of this policy is to state the standards for wireless access to RETA's network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps RETA wishes to take to secure its wireless infrastructure.

3.0 Scope

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

4.0 Policy

4.1 Physical Guidelines

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points should be located central to the office space rather than along exterior walls. If it is possible with the technology in use, signal broadcast strength should be reduced to only what is necessary to cover the office space. Directional antennas should be considered in order to focus the signal to areas where it is needed.
Physical security of access points should be considered - access points should not be placed in public or easily accessed areas if possible.

4.2 Configuration and Installation
The following guidelines apply to the configuration and installation of wireless networks:

4.2.1 Security Configuration

- The Service Set Identifier (SSID) of the access point must be changed from the factory default. The SSID should be changed to something completely nondescript. Specifically, the SSID must not identify RETA, the location of the access point, or anything else that may allow a third party to associate the access point's signal to RETA.
- Administrative access to wireless access points should utilize strong passwords.
- Encryption should be used to secure wireless communications. Stronger algorithms are preferred to weaker ones (i.e., WPA should be implemented rather than WEP). Encryption keys should be changed and redistributed periodically.

4.2.2 Installation

- Software and/or firmware on the wireless access points and wireless network interface cards (NICs) should be updated prior to deployment.
- Wireless networking must not be deployed in a manner that will circumvent RETA's security controls.
- Wireless devices should be installed only by RETA's IT department.
- Channels used by wireless devices should be evaluated to ensure that they do not interfere with RETA equipment.

4.3 Accessing Confidential Data
Wireless access to confidential data is permitted as long as the access is consistent with this and other policies that apply to confidential data.

4.4 Inactivity
Users should disable their wireless capability when not using the wireless network. This will reduce the chances that their machine could be compromised from the wireless NIC.

Inactive wireless access points should be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to RETA.

4.5 Audits
The wireless network should be periodically audited to ensure that this policy is being followed. Specific audit points should be: location of access points, signal strength, SSID, and use of strong encryption.

4.6 Applicability of Other Policies
This document is part of RETA's cohesive set of security policies. Other policies may apply to the topics
covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of RETA property (physical or intellectual) are suspected, RETA may report such activities to the applicable authorities.

6.0 Definitions

- **Mac Address** Short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.
- **SSID** Stands for Service Set Identifier. The name that uniquely identifies a wireless network.
- **WEP** Stands for Wired Equivalency Privacy. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. WEP can be cryptographically broken with relative ease.
- **WiFi** Short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11 family of standards.
- **Wireless Access Point** A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.
- **Wireless NIC** A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.
- **WPA** Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.
POLICY ACKNOWLEDGEMENT FORM

Company: 
User Name: 
Department: 

I understand that being granted access to computer systems and company information carries a great deal of responsibility. I recognize that I am being granted this access with the understanding that I will use the network resources and company information in a responsible manner. I realize that specific guidelines and expectations of me are detailed in the appropriate policies.

Initial below to indicate which policies you have received, read, understand, and to which you agree:

_______   Acceptable Use       _______  Data Classification
_______  Password              _______  Confidential Data
_______  Remote Access         _______  Mobile Device
_______  Retention
_______  Other (list: __________________________)

I UNDERSTAND THAT WHILE THE COMPANY INTENDS TO PROVIDE A SAFE AND POSITIVE EXPERIENCE WHEN USING COMPANY SYSTEMS AND THE INTERNET, THE COMPANY MAKES NO WARRANTIES AS TO THE CONTENT OF THE NETWORK AND THE INTERNET.

I AM RESPONSIBLE FOR MY OWN ACTIONS AND WILL RELEASE THE COMPANY FROM ANY LIABILITY RELATING TO MY NETWORK USAGE. I AGREE TO USE THE NETWORK AND SYSTEMS IN AN APPROPRIATE MANNER AS SPECIFIED IN THE APPLICABLE POLICIES. I UNDERSTAND THAT MY USE OF THE NETWORK AND SYSTEMS MAY BE MONITORED AT ANY TIME AND I SHOULD HAVE NO EXPECTATION OF PRIVACY IN CONNECTION WITH THIS USE.

I UNDERSTAND THAT FAILURE TO USE THE NETWORK IN A RESPONSIBLE MANNER MAY RESULT IN LOSS OF NETWORK PRIVILEGES, SUSPENSION, OR TERMINATION. I UNDERSTAND THAT IF ILLEGAL ACTIVITY IS SUSPECTED, THE COMPANY WILL REPORT THE ACTIVITY TO THE APPLICABLE AUTHORITIES.

User Name (Print): ____________________________________________

User Signature: ______________________________________________

Date: ________________________________________________________
**GUEST NETWORK ACCESS**

<table>
<thead>
<tr>
<th>Guest Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Company:</td>
<td></td>
</tr>
<tr>
<td>Employee Contact:</td>
<td></td>
</tr>
</tbody>
</table>

The company may wish to provide access to guests on a case-by-case basis in accordance with its Guest Access Policy. Please complete the information below in order to be granted access.

- **Dates Needed:** From: ______________ To: ______________

- **Reason for Access:** ______________________________________________________

- **Access Needed:**
  - [ ] Outbound to Internet (check one)
  - [ ] Specific Resources on the network (list: ____________________________)
  - [ ] Specific Ports or Services (list: ____________________________)

- **Access Requested:**
  - [ ] Wired   [ ] Wireless (check one)

The company reserves the right to require Guests to review and accept the corporate Acceptable Use Policy (AUP) before being granted network access. Please initial the statement below that is most accurate:

- [ ] I have read, understand, and agree to the Acceptable Use Policy.
- [ ] I have read and do not agree to the Acceptable Use Policy.
- [ ] I have not been asked to review the Acceptable Use Policy.

Please provide any additional information related to your request for access below:

______________________________

______________________________

______________________________

**Guest Name (Print):** ___________________________  **Date:** ______________

**Guest Signature:** ________________________________

**Employee Contact:** ________________________________

**Employee Signature:** ________________________________
SECURITY INCIDENT REPORT

Company: 
User Name: 
Department: 

Date of Incident: ________________  Time/Date Incident Detected: ________________

Incident Location: ____________________________________________________________

Type of Incident:  Physical: Loss or theft of device containing company information (circle 1)
                   Complete Section 1

                   Electronic: Suspicious password request, hack attempt, virus infection
                   Complete Section 2

Section 1: Physical Security Incident

Media/Device Type: ____________________________________________________________

Encryption Used?: Yes  No  Confidential Data Involved?: Yes  No  Unsure

Section 2: Electronic Security Incident

Type of Incident: 

☐ Hack attempt
☐ Denial of Service
☐ Malicious Code (Trojan/virus)
☐ Unauthorized system access
☐ Suspicious password request
☐ Misuse of systems
☐ Password compromise
☐ Other (explain below)

Confidential Data Involved?: Yes  No  Unsure

Impact of Incident: 

☐ Data Loss/Corruption
☐ System Damage
☐ System/Network Downtime
☐ Web Page Defacement
☐ Other (explain below)

Section 3: All Incidents

Describe Incident: ______________________________________________________________
                  (attach additional pages if needed)
                  ______________________________________________________________
By signing below, I certify that the information I have provided on this form is true to the best of my knowledge:

User Name (Print): ____________________________________________

User Signature: ______________________________________________

Date: ________________________________________________________

*** Please give this form immediately to the IT Manager or your supervisor ***
**NOTICE OF POLICY NONCOMPLIANCE**

<table>
<thead>
<tr>
<th>Company:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name:</td>
<td></td>
</tr>
<tr>
<td>Supervisor:</td>
<td></td>
</tr>
<tr>
<td>Department:</td>
<td></td>
</tr>
</tbody>
</table>

**Policy:**

**Date of Noncompliance:**

Date of Form Completion:

**Describe Incident:**

(attach additional pages if needed)

**Type of Action:**

Verbal Warning (Internal Use Only) (circle one)
Written Warning

Restriction or termination of network/system access (describe below)

Suspension: From:__________ To:__________

Termination: Effective:__________

**Additional Details About Action:**

**Corrective Action Plan (if applicable):**

**Next Step if Problem Continues:**

---
I acknowledge receipt of this notice of noncompliance with company policy and agree that its contents have been discussed with me. I understand that my signature below does not necessarily indicate agreement with this notice. I understand that I have a right to provide mitigating information to my supervisor regarding the event.

User Name (Print):

User Signature:

Date:

Supervisor Name (Print):

Supervisor Signature:

Date:

Copies of this form must be provided to:

User Supervisor/Department Head Human Resources
I understand that being granted access to computer systems and company information carries a great deal of responsibility. I recognize that I am being granted this access with the understanding that I will use the network resources and company information in a responsible and proper manner. I realize that specific guidelines and expectations of me are detailed in the appropriate policies.

Initial below to indicate which policies you have received, read, understand, and to which you agree:

[ ] Acceptable Use  [ ] Data Classification
[ ] Password  [ ] Confidential Data
[ ] Remote Access  [ ] Mobile Device
[ ] Retention  [ ] Email
[ ] Other (list:________________________________________________________)

I UNDERSTAND THAT WHILE THE COMPANY INTENDS TO PROVIDE A SAFE AND POSITIVE EXPERIENCE WHEN USING COMPANY SYSTEMS AND THE INTERNET, THE COMPANY MAKES NO WARRANTIES AS TO THE CONTENT OF THE NETWORK AND THE INTERNET.

I AM RESPONSIBLE FOR MY OWN ACTIONS AND WILL RELEASE THE COMPANY FROM ANY LIABILITY RELATING TO MY NETWORK USAGE. I AGREE TO USE THE NETWORK AND SYSTEMS IN AN APPROPRIATE MANNER AS SPECIFIED IN THE APPLICABLE POLICIES. I UNDERSTAND THAT MY USE OF THE NETWORK AND SYSTEMS MAY BE MONITORED AT ANY TIME AND I SHOULD HAVE NO EXPECTATION OF PRIVACY IN CONNECTION WITH THIS USE.

I UNDERSTAND THAT FAILURE TO USE THE NETWORK IN A RESPONSIBLE MANNER MAY RESULT IN LOSS OF NETWORK PRIVILEGES, SUSPENSION, OR TERMINATION. I UNDERSTAND THAT IF ILLEGAL ACTIVITY IS SUSPECTED, THE COMPANY WILL REPORT THE ACTIVITY TO THE APPLICABLE AUTHORITIES.

User Name (Print): ______________________________________________________

User Signature: _______________________________________________________

Date: ________________________________________________________________