GATHERACT LLC

Comprehensive IT Policy

Table Of Contents

Introduction

Information Technology (IT) is an integral and critical component of GATHERACT LLC’s (GATHERACT LLC) daily business. This policy seeks to ensure that GATHERACT LLC's IT resources efficiently serve the primary business functions of GATHERACT LLC, provide security for GATHERACT LLC and members’ electronic data, and comply with federal and other regulations. IT resources include hardware (computers, servers, peripherals), software (licensed applications, operating systems), network equipment (routers, firewalls, wiring), and IT personnel. The integrity of all IT resources is extremely important to the successful operation of GATHERACT LLC's business.

All computer equipment, peripherals, and software are GATHERACT LLC property and are provided for business purposes. Proper use and control of computer resources is the responsibility of all employees. Intentional or reckless violation of established policies or improper use of GATHERACT LLC computers will result in corrective action up to and including termination. Employees should also be aware that any work completed on GATHERACT LLC computers is subject to monitoring and review, and they should not expect their communications to be private.

This Policy supersedes any previous IT policies of GATHERACT LLC. The following Policy Statement, Disciplinary Action, and Review paragraphs apply to all individual policies contained within this document.

Policy Statement

It is the policy of GATHERACT LLC to use IT resources in a cost-effective manner that safeguards member data and promotes accuracy, safety, Information , and efficiency. The overriding goal of this policy is to comply with all federal and other regulations and to protect the integrity of the
private and confidential member and business data that resides within GATHERACT LLC's technology infrastructure.

Disciplinary Action

Violation of any of these policies may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; or dismissal for interns and volunteers. In accordance with Article 5, Section 6 of the Credit Union Bylaws, any Board Member who violates these policies shall be subject to removal. Additionally, individuals are subject to loss of GATHERACT LLC Information Systems access privileges and may be subject to civil and criminal prosecution.

Review and Acceptance

The Board of Directors, Chief Operations Officer/COO, and IT staff shall review this comprehensive policy at least annually, making such revisions and amendments as deemed appropriate and indicating approval and the date thereof in the policy header.

All GATHERACT LLC staff are responsible for review and acceptance of this policy annually. Appropriate communications by way of reminder will be sent by Senior Management or its assignee along with instructions for acceptance.

Policy 1: Acceptable Use of Information Systems

Definitions

Information Systems: All electronic means used to create, store, access, transmit, and use data, information, or communications in the conduct of administrative, instructional, research, or service activities. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Authorized User: An individual or automated application or process that is authorized access to the resource by the system owner, in accordance with the system owner's procedures and rules.

Extranet: An intranet that is partially accessible to authorized persons outside of a company or organization.

Overview

Data, electronic file content, information systems, and computer systems at GATHERACT LLC must be managed as valuable organization resources.

Information Technology's (IT) intentions are not to impose restrictions that are contrary to GATHERACT LLC's established culture of openness, trust, and integrity. IT is committed to protecting GATHERACT LLC's authorized users, partners, and the company from illegal or damaging actions by individuals either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and File Transfer Protocol (FTP) are the property of GATHERACT LLC. These systems are to be used for business purposes in serving the interests of GATHERACT LLC and of its clients and members during normal operations.

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

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at GATHERACT LLC. These rules are in place to protect the authorized user and GATHERACT LLC. Inappropriate use exposes GATHERACT LLC to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct GATHERACT LLC business or interacts with internal networks and business systems, whether owned or leased by GATHERACT LLC, the employee, or a third party.

All employees, volunteer/directors, contractors, consultants, temporaries, and other workers at GATHERACT LLC, including all personnel affiliated with third parties, are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with GATHERACT LLC policies and standards, local laws, and regulations.

Policy Detail

Ownership of Electronic Files

All electronic files created, sent, received, or stored on GATHERACT LLC owned, leased, or administered equipment or otherwise under the custody and control of GATHERACT LLC are the property of GATHERACT LLC.

Privacy

Electronic files created, sent, received, or stored on GATHERACT LLC owned, leased, or administered equipment, or otherwise under the custody and control of GATHERACT LLC are not private and may be accessed by GATHERACT LLC IT employees at any time without knowledge of the user, sender, recipient, or owner. Electronic file content may also be accessed by appropriate personnel in accordance with directives from Human Resources or the President/CEO.

General Use and Ownership

Access requests must be authorized and submitted from departmental supervisors for employees to gain access to computer systems.

Authorized users are accountable for all activity that takes place under their username.

Authorized users should be aware that the data and files they create on the corporate systems immediately become the property of GATHERACT LLC. Because of the need to protect GATHERACT LLC's network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to GATHERACT LLC.

For security and network maintenance purposes, authorized individuals within the GATHERACT LLC IT Department may monitor equipment, systems, and network traffic at any time.

GATHERACT LLC's IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

GATHERACT LLC's IT Department reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

Security and Proprietary Information

All mobile and computing devices that connect to the internal network must comply with this policy and the following policies:

- Policy 2: Account Management
- Policy 3: Anti-Virus
- Policy 4: GATHERACT LLC Owned Mobile Device Acceptable Use and Security
- Policy 7: E-mail
- Policy 12: Internet
- Policy 14: Safeguarding Member Information
- Policy 16: Personal Device Acceptable Use and Security
- Policy 17: Password
- Policy 20: Cloud Computing
- Policy 28: Wireless (Wi-Fi) Connectivity
- Policy 29: Telecommuting

System level and user level passwords must comply with the Password Policy. Authorized users must not share their GATHERACT LLC login ID(s), account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authentication purposes. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

Authorized users may access, use, or share GATHERACT LLC proprietary information only to the extent it is authorized and necessary to fulfill the users assigned job duties.

All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less.

All users must lockdown their PCs, laptops, and workstations by locking (control-alt delete) when the host will be unattended for any amount of time.

Employees must log-off, or restart (but not shut down) their PC after their shift.

GATHERACT LLC proprietary information stored on electronic and computing devices, whether owned or leased by GATHERACT LLC, the employee, or a third party, remains the sole property of GATHERACT LLC. All proprietary information must be protected through legal or technical means.

All users are responsible for promptly reporting the theft, loss, or unauthorized disclosure of GATHERACT LLC proprietary information to their immediate supervisor and/or the IT Department.

All users must report any weaknesses in GATHERACT LLC computer security and any incidents of possible misuse or violation of this agreement to their immediate supervisor and/or the IT Department.

Users must not divulge dial-up or dial-back modem phone numbers to anyone without prior consent of the GATHERACT LLC IT Department.

Authorized users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan Horse codes.

Unacceptable Use

Users must not intentionally access, create, store, or transmit material which GATHERACT LLC may deem to be offensive, indecent, or obscene.

Under no circumstances is an employee, volunteer/director, contractor, consultant, or temporary employee of GATHERACT LLC authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing GATHERACT LLC-owned resources.

System and Network Activities

The following activities are prohibited by users, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by GATHERACT LLC.

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution from copyrighted sources, copyrighted music, and the installation of any copyrighted software for which GATHERACT LLC or the end user does not have an active license is prohibited. Users must report unlicensed copies of installed software to IT.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

- Using a GATHERACT LLC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

- Attempting to access any data, electronic content, or programs contained on GATHERACT LLC systems for which they do not have authorization, explicit consent, or implicit need for their job duties.

- Installing any software, upgrades, updates, or patches on any computer or information system without the prior consent of GATHERACT LLC IT.

- Installing or using non-standard shareware or freeware software without GATHERACT LLC IT approval.

- Installing, disconnecting, or moving any GATHERACT LLC owned computer equipment and peripheral devices without prior consent of GATHERACT LLC's IT Department.

- Purchasing software or hardware, for GATHERACT LLC use, without prior IT compatibility review.

- Purposely engaging in activity that may;
  - degrade the performance of information systems;
  - deprive an authorized GATHERACT LLC user access to a GATHERACT LLC resource;
  - obtain extra resources beyond those allocated; or
  - circumvent GATHERACT LLC computer security measures.

- Downloading, installing, or running security programs or utilities that reveal passwords, private information, or exploit weaknesses in the security of a system. For example, GATHERACT LLC users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non approved programs on GATHERACT LLC information systems. The GATHERACT LLC IT Department is the only department authorized to perform these actions.

- Circumventing user authentication or security of any host, network, or account.

- Interfering with, or denying service to, any user other than the employee’s host (for example, denial of service attack).

- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user’s terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Access to the Internet at home, from a GATHERACT LLC-owned computer, must adhere to all the same policies that apply to use from within GATHERACT LLC facilities. Authorized users must not allow family members or other non-authorized users to access GATHERACT LLC computer systems.

GATHERACT LLC information systems must not be used for personal benefit.

Incidental Use

As a convenience to the GATHERACT LLC user community, incidental use of information systems is permitted. The following restrictions apply:

- Authorized Users are responsible for exercising good judgment regarding the reasonableness of personal use. Immediate supervisors are responsible for supervising their employees regarding excessive use.

- Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, and so on, is restricted to GATHERACT LLC approved users; it does not extend to family members or other acquaintances.

- Incidental use must not result in direct costs to GATHERACT LLC without prior approval of management.

- Incidental use must not interfere with the normal performance of an employee's work duties.

- No files or documents may be sent or received that may cause legal action against, or embarrassment to, GATHERACT LLC.

- Storage of personal email messages, voice messages, files, and documents within GATHERACT LLC's information systems must be nominal.

- All messages, files, and documents — including personal messages, files, and documents — located on GATHERACT LLC information systems are owned by GATHERACT LLC, may be subject to open records requests, and may be accessed in accordance with this policy.

Review and Acceptance

All GATHERACT LLC staff is responsible for review and acceptance of *Policy 1: Acceptable Use* upon starting work at GATHERACT LLC (see Exhibit A). New employee onboarding and training shall include this *Policy 1* at a minimum, and in addition to all other applicable training and orientation material, and instructions for acceptance shall be provided at that time. Signed acceptance will be received and retained by Information Technology management.

EXHIBIT A

[This exhibit is a copy of the current Acceptable Use of Information Systems receipt.Rev2016- 00.pdf]

Receipt of Acceptable Use of Information Systems

Please sign this form and return it to Information Systems

I have received a copy of the GATHERACT LLC Acceptable Use of Information Systems Policy. I understand the information in the Acceptable Use of Information Systems policy is a summary only, and it is my responsibility to review and become familiar with all of the material contained in the . I understand the most updated policies and Bylaws will always be located on the intranet for my reference, and it will be my responsibility to review the policies and Bylaws as they are updated.

I further understand the content of the supersedes all policies previously issued. I also understand that GATHERACT LLC may supersede, change, eliminate, or add to any policies or practices described in the .

My signature below indicates that I have received my personal copy of the Acceptable Use of Information Systems Policy and it will be my responsibility to review the Comprehensive IT policies as they are updated.

User Signature____

User Name (printed) ____

Date____

**Retain one copy of this Receipt for your records and return the other copy to Information Systems.

Policy 2: Account Management

Definitions

Account: *Any combination of a User ID (sometime referred to as a username) and a password that grants an authorized user access to a computer, an application, the network, or any other information or technology resource.*

Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system. Whereas GATHERACT LLC may have one Information Security Officer, technical management may designate a number of security administrators.

System Administrator: The person responsible for the effective operation and maintenance of information systems, including implementation of standard procedures and controls to enforce an organization's security policy.

Overview

Computer accounts are the means used to grant access to GATHERACT LLC's information systems. These accounts provide a means of providing accountability, a key to any computer security program, for GATHERACT LLC usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose

The purpose of this policy is to establish a standard for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at GATHERACT LLC.

Audience

This policy applies to the employees, Directors, volunteers, contractors, consultants, temporaries, and other workers at GATHERACT LLC, including all personnel affiliated with third parties with authorized access to any GATHERACT LLC information system.

Policy Detail

Accounts

- All accounts created must have an associated written request and signed management approval that is appropriate for the GATHERACT LLC system or service.

- All accounts must be uniquely identifiable using the assigned username. •

Shared accounts on GATHERACT LLC information systems are not

permitted.

- Reference the Employee Access During Leave of Absence Policy for removing an employee’s access while on a leave of absence or vacation.

- All default passwords for accounts must be constructed in accordance with the GATHERACT LLC Password Policy.

- All accounts must have a password expiration that complies with the GATHERACT LLC Password Policy.

- Concurrent connections may be limited for technical or security reasons.

- All accounts must be disabled immediately upon notification of any employee’s termination.

Account Management
The following items apply to System Administrators or other designated staff:

- Information system user accounts are to be constructed so that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with an individual’s account. Further, to eliminate conflicts of interest, accounts shall be created so that no one user can authorize, perform, review, and audit a single transaction.

- All information system accounts will be actively managed. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.

- Access controls will be determined by following established procedures for new employees, employee changes, employee terminations, and leave of absence.

- All account modifications must have a documented process to modify a user account to accommodate situations such as name changes and permission changes.

- Information system accounts are to be reviewed monthly to identify inactive accounts. If an employee or third party account is found to be inactive for 30 days, the owners (of the account) and their manager will be notified of pending disablement. If the account continues to remain inactive for 15 days, it will be manually disabled.

- A list of accounts, for the systems they administer, must be provided when requested by authorized GATHERACT LLC management.

- An independent audit review may be performed to ensure the accounts are properly managed.

Policy 3: Anti-Virus

Definitions

Virus: *A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allows users to generate macros.*

Trojan Horse: Destructive programs, usually viruses or worms, which are hidden in an attractive or innocent looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or removable media, often from another unknowing victim, or may be urged to download a file from a web site or download site.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. Some worms are security threats using networks to spread themselves against the wishes of the system owners and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.

Spyware: Programs that install and gather information from a computer without permission and reports the information to the creator of the software or to one or more third parties.

Malware: Short for malicious software, a program or file that is designed to specifically damage or disrupt a system, such as a virus, worm, or a Trojan horse.

Adware: Programs that are downloaded and installed without user’s consent or bound with other software to conduct commercial advertisement propaganda through pop-ups or other ways, which often lead to system slowness or exception after installing.

Keyloggers: A computer program that captures the keystrokes of a computer user and stores them. Modern keyloggers can store additional information, such as images of the user’s screen. Most malicious keyloggers send this data to a third party remotely (such as via email).

Ransomware: A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files, unless a ransom is paid.

Server: A computer program that provides services to other computer programs in the same or other computers. A computer running a server program is frequently referred to as a server, although it may also be running other client (and server) programs.

Security Incident: In information operations, a security incident is an assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing; disruption or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to information system hardware, firmware, or software characteristics with or without the user's knowledge, instruction, or intent.

E-mail: Abbreviation for electronic mail, which consists of messages sent over any electronic media by a communications application.

Overview

Malware threats must be managed to minimize the amount of downtime realized by GATHERACT LLC's systems and prevent risk to critical systems and member data. This policy is established to:

• Create prudent and acceptable practices regarding anti-virus management •

Define key terms regarding malware and anti-virus protection

• Educate individuals, who utilize GATHERACT LLC system resources, on the responsibilities associated with anti-virus protection

Note: The terms virus and malware, as well as anti-virus and anti-malware, may be used interchangeably.

Purpose

This policy was established to help prevent infection of GATHERACT LLC computers, networks, and technology systems from malware and other malicious code. This policy is intended to help prevent damage to user applications, data, files, and hardware.

Audience

This policy applies to all computers connecting to the GATHERACT LLC network for communications, file sharing, etc. This includes, but is not limited to, desktop computers, laptop computers, servers, and any PC based equipment connecting to the GATHERACT LLC network.

Policy Detail

All computer devices connected to the GATHERACT LLC network and networked resources shall have anti-virus software installed and configured so that the virus definition files are current and are routinely and automatically updated. The anti-virus software must be actively running on these devices.

The virus protection software must not be disabled or bypassed without IT approval.

The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.

The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

Each file server, attached to the GATHERACT LLC network, must utilize GATHERACT LLC IT approved virus protection software and setup to detect and clean viruses that may infect GATHERACT LLC resources.

Each e-mail gateway must utilize GATHERACT LLC IT approved e-mail virus protection software.

All files on computer devices will be scanned periodically for malware.

Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Service Desk.

If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the GATHERACT LLC network until the infection has been removed.

Users should:

- Avoid viruses by NEVER opening any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately then remove them from the Trash or Recycle Bin.

- Delete spam, chain, or other junk mail without opening or forwarding the item. •

Never download files from unknown or suspicious sources.

- Always scan removable media from an unknown or non-GATHERACT LLC source (such as a CD or USB from a vendor) for viruses before using it.

- Back up critical data on a regular basis and store the data in a safe place. Critical GATHERACT LLC data can be saved to network drives and are backed up on a periodic basis. Contact the GATHERACT LLC IT Department for details.

Because new viruses are discovered every day, users should periodically check the Anti-Virus Policy for updates. The GATHERACT LLC IT Department should be contacted for updated recommendations.

Policy 4: GATHERACT LLC Owned Mobile Device Acceptable Use and Security

Definitions

Clear text: *Unencrypted data*

Full disk encryption: Technique that encrypts an entire hard drive, including operating system and data.

Key: Phrase used to encrypt or decrypt data

Overview

Acceptable use of GATHERACT LLC owned mobile devices must be managed to ensure that employees, Board of Directors, and related constituents who use mobile devices to access GATHERACT LLC's resources for business do so in a safe and secure manner.

This policy is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

Purpose

This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data from a mobile device connected to an unmanaged network outside of GATHERACT LLC's direct control. This mobile device policy applies to, but is not limed to, any mobile device issued by GATHERACT LLC that contains stored data owned by GATHERACT LLC and all devices and accompanying media that fit the following device classifications:

- Laptops. Notebooks, and hybrid devices
- Tablets
- Mobile/cellular phones including smartphones
- Any GATHERACT LLC owned mobile device capable of storing corporate data and connecting to an unmanaged network

This policy addresses a range of threats to, or related to, the use of GATHERACT LLC data:

Threat	Description
Loss	Devices used to transfer, or transport work files could be lost or stolen
Theft	Sensitive corporate data is deliberately stolen and sold by an employee
Copyright	Software copied onto a mobile device could violate licensing
Malware	Virus, Trojans, Worms, Spyware and other threats could be introduced via a mobile device
Compliance	Loss or theft of financial and/or personal and confidential data could expose GATHERACT LLC to the risk of non-compliance with various identity theft and privacy laws

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the GATHERACT LLC network.

Audience

This policy applies to all GATHERACT LLC employees, including full and part-time staff, and the Board of Directors who utilize company-owned mobile devices to access, store, back up, relocate, or access any organization or member-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust GATHERACT LLC has built with its members, suppliers, and other constituents. Consequently, employment at GATHERACT LLC does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Policy Detail

This policy applies to any corporate owned hardware and related software that could be used to access corporate resources.

The overriding goal of this policy is to protect the integrity of the private and confidential member and business data that resides within GATHERACT LLC's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to GATHERACT LLC's public image. Therefore, all users employing a GATHERACT LLC owned mobile device, connected to an unmanaged network outside of GATHERACT LLC's direct control, to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

Affected Technology

Connectivity of all mobile devices will be centrally managed by GATHERACT LLC's IT Department and will utilize authentication and strong encryption measures. To protect GATHERACT LLC's infrastructure, failure to adhere to these security protocols will result in immediate suspension of all network access privileges.

Responsibilities

It is the responsibility of any employee or Board Member of GATHERACT LLC, who uses a GATHERACT LLC owned mobile device to access corporate resources, to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any GATHERACT LLC owned mobile device that is used to conduct GATHERACT LLC business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

o **Access control**

IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to GATHERACT LLC and GATHERACT LLC-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts GATHERACT LLC's systems, data, users, and members at risk.

Prior to initial use on the GATHERACT LLC network or related infrastructure, **all mobile devices must be registered with IT.** GATHERACT LLC will maintain a list of approved mobile devices and related software applications and utilities, and it will be stored in the IT Document Storage location. Devices that are not on this list may not be connected to the GATHERACT LLC infrastructure. To find out if a preferred device is on this list, an individual should contact the GATHERACT LLC IT Department Service Desk. Although IT currently allows only listed devices to be connected to the GATHERACT LLC infrastructure, it reserves the right to update this list in the future.

End users who wish to connect such devices to non-corporate network infrastructure to gain access to GATHERACT LLC data **must employ,** for their devices and related infrastructure, **a company-approved personal firewall** and any other security measure deemed necessary by the IT Department. GATHERACT LLC data is not to be accessed on any hardware that fails to meet GATHERACT LLC's established enterprise IT security standards.

All mobile devices attempting to connect to the GATHERACT LLC network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by GATHERACT LLC's IT Department. Devices that are not corporate issued are not in compliance with IT’s security policies and will not be allowed to connect except by provision of the Personal Device Acceptable Use and Security Policy. GATHERACT LLC owned laptop computers may only access the corporate network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) or Internet Protocol Security (IPSec) VPN connection. The SSL or IPSec VPN portal Web address will be provided to users as required. Smart mobile devices such as Smartphones, PDAs, and UMPCs will access the GATHERACT LLC network and data using Mobile VPN software installed on the device by IT.

o **Security**

Employees using mobile devices and related software for network and data access **will**, without exception, **use secure data management procedures.** All mobile devices containing stored data owned by GATHERACT LLC **must use an approved method of encryption** to protect data. Laptops must employ full drive encryption with an approved software encryption package. No GATHERACT LLC data may exist on a laptop in clear text. All mobile devices must be protected by a **strong password.** Refer to the GATHERACT LLC password policy for additional information. **Employees agree to never disclose their passwords to anyone,** particularly to family members, if business work is conducted from home.

All keys used for encryption and decryption must meet complexity requirements described in GATHERACT LLC's Password Policy.

All users of corporate owned mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain GATHERACT LLC data. Users with devices that are not issued by GATHERACT LLC must adhere to the Personal Device Acceptable Use and Security Policy.

To ensure the security of GATHERACT LLC equipment, mobile devices will be transported and stored as specified in the “Mobile Device Transport and Storage” procedure.

Passwords and confidential data should not be stored on unapproved or unauthorized non-GATHERACT LLC devices.

Any corporate owned mobile device that is being used to store GATHERACT LLC data must adhere to the authentication requirements of GATHERACT LLC's IT Department. In addition, all hardware security configurations must be preapproved by GATHERACT LLC's IT Department before any enterprise data-carrying device can be connected to it.

IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with GATHERACT LLC's overarching security policy.

Employees, Board of Directors, and temporary staff will **follow all enterprise sanctioned data removal procedures to permanently erase company specific data from such devices once their use is no longer required.** For assistance with detailed data wipe procedures for mobile devices, an individual should contact the GATHERACT LLC IT Department Service Desk. This information is found in the IT Document Storage location.

In the event of a lost or stolen mobile device, it is incumbent on the user to report this to IT immediately. GATHERACT LLC shall employ remote wipe technology to remotely disable and delete any data stored on a GATHERACT LLC PDA or cell phone that is reported lost or stolen. If the device is recovered, it can be submitted to IT for re-provisioning.

Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to both GATHERACT LLC-owned and personal mobile devices being used within GATHERACT LLC's premises.

IT maintains the process for patching and updating mobile devices. A device’s firmware/operating system **must** be up-to-date in order to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of IT for computing platforms (i.e. laptops).

IT maintains the process for security audits on mobile devices. Since handheld devices are not completely under the control of GATHERACT LLC, a periodic audit will be performed to ensure the devices are not a potential threat to

GATHERACT LLC.

o **Help and Support**

GATHERACT LLC's IT Department will support its sanctioned hardware and software but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department.

Employees, Board of Directors, and temporary staff will not make modifications of any kind to GATHERACT LLC owned and installed hardware or software without the express approval of GATHERACT LLC's IT Department. This includes, but is not limited to, any reconfiguration of the mobile device.

IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the GATHERACT LLC network.

o **Organizational Protocol**

IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. To identify unusual usage patterns or other suspicious activity, the end user agrees to and accepts that his or her access and/or connection to GATHERACT LLC's networks may be monitored to record dates, times, duration of access, etc. This is done to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains GATHERACT LLC's highest priority.

The **end user agrees to immediately report,** to his/her manager and GATHERACT LLC's IT Department, **any incident or suspected incidents of unauthorized data access,** data loss, and/or disclosure of GATHERACT LLC resources, databases, networks, etc.

GATHERACT LLC will not reimburse employees if they choose to purchase their own mobile devices except in accordance with the Personal Device Acceptable Use and Security Policy. Users will not be allowed to expense mobile network usage costs.

GATHERACT LLC prohibits the unsafe and unlawful use of mobile devices, including but not limited to, texting, emailing, or any distracting activity while driving, and requires this audience to comply with all state laws in which one is currently operating, regarding same, hands-free requirements, etc.

Before being granted a device and access to GATHERACT LLC resources, a mobile device user must understand and accept the terms and conditions of this policy.

EXHIBIT A

GATHERACT LLC Owned Mobile Device Agreement

This GATHERACT LLC Owned Mobile Device Agreement is entered into between the User and GATHERACT LLC, effective the date this agreement is executed by GATHERACT LLC's Information Technology Department (IT). The parties agree as follows:

ELIGIBILITY

The use of a GATHERACT LLC supported mobile device by the User for GATHERACT LLC business is a privilege granted to the User, by management approval, per the GATHERACT LLC Owned Mobile Device Acceptable Use and Security Policy. If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to GATHERACT LLC and to ensure the data remains secure.

In the event of a security breach or threat, GATHERACT LLC reserves the right, without prior notice to the User, to disable or disconnect some or all GATHERACT LLC services related to connection of a GATHERACT LLC owned mobile device to the GATHERACT LLC network.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following GATHERACT LLC policies, published elsewhere and made available, is mandatory: Acceptable Use of Information Systems, GATHERACT LLC Owned Mobile Device Acceptable Use and Security, and other related policies including, but not limited to, Anti Virus, E-Mail, Network Security, Password, Safeguarding Member Information, Telecommuting.

The User of the GATHERACT LLC owned mobile device shall not remove sensitive information from the GATHERACT LLC network, attack GATHERACT LLC assets, or violate any of the security policies related to the subject matter of this Agreement.

SUPPORT

GATHERACT LLC will offer the following support for the GATHERACT LLC owned mobile device: connectivity to GATHERACT LLC servers, including email and calendar, and security services, including policy management, password management, and decommissioning and/or remote wiping in case of loss, theft, device failure, device degradation, upgrade (trade-in), and carrier network or system outages that result in a failure of connectivity to the GATHERACT LLC network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the GATHERACT LLC network, programming and other errors, bugs, viruses, and other software or hardware failures resulting in the partial or complete loss of data or which render the mobile device inoperable.

____
Device Make/Model

____ _______________
User **Date**

____ ________________

IT Department Management **Date**

Policy 5: Clean Desk

Overview

GATHERACT LLC is committed to protecting the privacy of its employees and members and shall protect the confidentiality of nonpublic information consistent with state and federal laws. GATHERACT LLC has an obligation to ensure the security and confidentiality of its member records and to protect these records against unauthorized access that could result in any type of loss or inconvenience for its members.

Purpose

The purpose and principle of a "clean desk" policy is to ensure that confidential data is not exposed to individuals who may pass through the area such as members, service personnel, and thieves. It encourages methodical management of one's workspace. Because of the risk of being compromised, confidential information should always be treated with care.

Policy Detail

To maintain the security and privacy of employees' and members' personal information, GATHERACT LLC employees should observe the "clean desk" rule. All employees should take appropriate actions to prevent unauthorized persons from having access to member information, applications, or data. Employees are also required to make a conscientious check of their surrounding work environment to ensure that there will be no loss of confidentiality to data media or documents.

The clean desk policy applies to:

- Day Planners and Rolodexes that may contain non-public information •
File cabinets, storage cabinets, and briefcases containing sensitive or confidential information
- Any confidential or sensitive data, including reports, lists, or statements.
  Sensitive data refers to personal information and restricted data. Personal information includes, but is not limited to:
  - o An individual's name
  - o Social security number
  - o Driver's license number or identification card number
  - o Account number, credit or debit card number, security code, access code, or password that could permit access to an individual's financial account

  Restricted data is divided into two categories:
  - o Personal data, that refers to any combination of information that identifies and describes an individual.
  - o Limited data, that refers to electronic information whose unauthorized access, modification, or loss could seriously or adversely affect GATHERACT LLC, its members, and non-members.
- Electronic devices, including cell phones and PDAs
- Keys used to access sensitive information
- Printouts containing sensitive information

- Data on printers, copy machines, and/or fax machines
- Computer workstations and passwords
- Portable media, such as CD’s, disks, or flash drives
- Desks or work areas, including white boards and bookshelves

Policy 6: E-Commerce

Definitions

Electronic commerce: *Electronic financial services delivered via electronic means including, but not limited to, the Internet or other electronic delivery vehicles.*

Specific examples of e-commerce activities include:

1. *Internet/world wide web services*
   - *Email inquiries and responses*
   - *Publishing of general information on any GATHERACT LLC owned website*
   - *Data entry or verification by staff on a vendor's data processing system*
   - *File transfers of member information for direct mail projects or statement generation*

2. *Web account access*
   - *Viewing share or loan transaction history and balances*
   - *Transferring funds between shares and loans, transfers to other*
   - *financials, or Person to Person Transfers (PTP)*
   - *Requesting a check withdrawal from a share or loan*
   - *Applying for GATHERACT LLC services through applications or forms*
   - *E-mail statements*
   - *Electronic retrieval of check copies*
   - *E-alerts*

3. *Online bill paying services*

4. *Audio response/phone based*

5. *Wireless services*

6. *Mobile banking*

Encryption: *Is the conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people.*

Authentication: *Is the process of determining whether someone or something is, in fact, who or what it is declared to be. Depending on the transactions, a more stringent authentication process may be required.*

Firewall: *Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.*

Overview

GATHERACT LLC recognizes the importance of electronic commerce (e-commerce) activities to its present day operations. GATHERACT LLC is committed to using *e-commerce activities in a cost effective manner that promotes accuracy, safety, security, and efficiency. These activities bring automation and efficiencies to traditional manual tasks and allow quicker access to information resulting in improved member service.*

Purpose

This e-commerce policy is to be used as both a guideline and an overview in the management of GATHERACT LLC's electronic services.

Policy Detail

GATHERACT LLC is committed to enhancing member service through the use of many forms of e-commerce activities.

Electronic commerce activities include GATHERACT LLC's web site, email, telephone access system, ACH transactions, ATM system, online bill payment, and home banking services. They also include business-to-business transactions where interaction is conducted electronically between GATHERACT LLC and its business partners using the Internet as the communications network.

It is the practice of GATHERACT LLC to safeguard member data at all times, including the processing of e-commerce transactions. Information must be protected at both the sending and receiving ends of each transaction. To accomplish this, there are several levels of protection applied to e-commerce activities.

- **Encryption**

  Encrypting transactions provides security by ensuring that no portion of a transaction is readable except by the parties at each end of the transmission. This ensures that data can be transmitted securely without concern that another party could intercept all or part of the transaction. Encryption also makes certain that the transaction is not tampered with as it routes from point to point and data is received exactly as it was sent. GATHERACT LLC will use a minimum of 128b encryption. This also applies to vendors that host GATHERACT LLC member data.

- **Authentication**

  After a secure connection is established, the initiating party must prove his/her identity prior to conducting the transaction. This is typically handled with user IDs or account numbers, along with password or PIN combinations. Additionally, encryption certificates are also employed to validate the authenticity of both servers and users. System administrators control system access by assigning users different levels of access for applications and data. These access levels are determined by senior management and are specific to each job function. This ensures that access to applications and specific types of transactions are only granted as job functions require.

- **Multi-factor Authentication (MFA)**

  For online banking, MFA offers more than one form of authentication to verify the *legitimacy of a transaction. The layered defense makes it more difficult for an unauthorized person to gain access.*

- **Firewalls**
  GATHERACT LLC will deploy and utilize firewalls as necessary to protect internal systems from threats originating from the Internet, as well as those that might be present when connecting to vendors' networks. Firewall operating systems and configurations will be reviewed periodically to ensure maximum protection. An audit log will be maintained tracking all attempts to access un-configured (blocked) services. Firewalls and other access devices will be used, as needed, to limit access to sites or services that are deemed inappropriate or non corporate in nature. Vendor hosted solution firewalls will be reviewed prior to implementation.

- **Network Traffic Rules and Restrictions**
  Intra-network traffic is subject to distinct operating rules and restrictions. Through the use of firewall technology, outside parties are directed only to approved, internal resources. An example of this is web page services that allow certain types of traffic from the Internet (web page browsing) but have other types of traffic blocked (i.e. administrative tasks). This strategy dramatically reduces the risk of any party gaining unauthorized access to a protected server.

  The internal network is also protected from virus attacks through the use of network-level anti-virus software that is updated automatically on a regular basis. These regular updates are loaded automatically to each PC, as they are available. This provides the most up to date virus protection and security available. E-mail is also scanned prior to delivery, reducing the potential of a virus entering the network in this manner.

- **Physical Site Security**
  The entire IT Department is protected by a card access entry system allowing only authorized personnel into the Department. Sensitive data, hardware, and software are secured in the GATHERACT LLC data center, which is secured with a
  card access entry point and is monitored throughout the day by IT staff. Access to the data center is further limited to a small number of authorized personnel. It is GATHERACT LLC's practice to change administrative passwords and immediately remove card access privileges after any change in IT staff.

  In addition to on-site storage of data, GATHERACT LLC stores overnight backups of critical systems data and replicated Storage Area Network (SAN) storage to a secure, off-site location. This ensures that data is available in the event of a disaster or other critical situation.

- **Staff Training and Review**
  IT staff receives training and reviews all procedures at least annually or as major system additions or changes are implemented.

- **User Password Maintenance**

  GATHERACT LLC has a strict policy prohibiting users from sharing or disclosing their passwords, is intended to prohibit unauthorized access to systems and data. After receiving a change in status from the Human Resources Department or other management team members, IT staff immediately removes user access codes from appropriate systems.

- **Expert Assistance**

  GATHERACT LLC recognizes that e-commerce security issues change daily. New threats to security, safety, and accuracy appear daily and system vendors publish updates and patches regularly to eliminate the threat. To assist in the ongoing maintenance of key components of system security, GATHERACT LLC will engage, at a regularly scheduled interval, consulting and audit oversight with a nationally recognized leader in the area of e-commerce security. This vendor may also provide technical assistance as new e-commerce related features are added to the system to ensure the continued safety and security of existing systems.

- **Communications Network**

  GATHERACT LLC employs the use of several types of data communication lines including dial-up phone lines, direct point-to-point circuits, and other private and public network connections. Data transmissions are secured, encrypted, and/or password protected, as needed.

Response Program

In the event GATHERACT LLC suspects or detects unauthorized individuals have gained access to member information systems, GATHERACT LLC will report such actions to appropriate regulatory and law enforcement agencies according to GATHERACT LLC's information security response procedures.

Policy 7: E-Mail

Definitions

Anti-Spoofing: *A technique for identifying and dropping units of data, called packets, that have a false source address.*

Antivirus: *Software used to prevent, detect, and remove malicious software.*

Electronic mail system: *Any computer software application that allows electronic mail to be communicated from one computing system to another.*

Electronic mail (e-mail): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Email spoofing: The forgery of an email header so the message appears to have originated from someone other than the actual source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation to provide sensitive data or perform an action such as processing a wire transfer.

Inbound filters: A type of software based traffic filter allowing only designated traffic to flow towards a network.

Quarantine: Suspicious email message may be identified by an antivirus filter and isolated from the normal mail inbox.

SPAM: Unsolicited e-mail, usually from Internet sources. It is often referred to as junk e mail.

Overview

E-mail at GATHERACT LLC must be managed as valuable and mission critical resources. Thus, this policy is established to:

- *Create prudent and acceptable practices regarding the use of information resources*
- *Educate individuals who may use information resources with respect to their responsibilities associated with such use*
- *Establish a schedule for retaining and archiving e-mail*

Purpose

The purpose of this policy is to establish rules for the use of GATHERACT LLC email for sending, receiving, or storing of electronic mail.

Audience

This policy applies equally to all individuals granted access privileges to any GATHERACT LLC information resource with the capacity to send, receive, or store electronic mail.

Legal

Individuals involved may be held liable for:

- Sending or forwarding e-mails with any libelous, defamatory, offensive, racist, or obscene remarks
- Sending or forwarding confidential information without permission
- Sending or forwarding copyrighted material without permission
- Knowingly sending or forwarding an attachment that contains a virus

Policy Detail

Corporate e-mail is not private. Users expressly waive any right of privacy in anything they create, store, send, or receive on GATHERACT LLC's computer systems. GATHERACT LLC can, but is not obliged to, monitor emails without prior notification. All e-mails, files, and documents – including personal e-mails, files, and documents – are owned by GATHERACT LLC, may be subject to open records requests, and may be accessed in accordance with this policy.

Incoming email must be treated with the utmost care due to the inherent information security risks. An anti-virus application is used to identify malicious code(s) or files. All email is subjected to inbound filtering of e-mail attachments to scan for viruses, malicious code, or spam. Spam will be quarantined for the user to review for relevancy. Introducing a virus or malicious code to GATHERACT LLC systems could wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, IT must be immediately notified.

Anti-spoofing practices have been initiated for detecting spoofed emails. Employees should be diligent in identifying a spoofed email. If email spoofing has occurred, IT must be immediately notified.

Incoming emails are scanned for malicious file attachments. If an attachment is identified as having an extension known to be associated with malware, or prone to abuse by malware or bad actors or otherwise poses heightened risk, the attachment will be removed from the email prior to delivery.

Email rejection is achieved through listing domains and IP addresses associated with malicious actors. Any incoming email originating from a known malicious actor will not be delivered.

Any email account misbehaving by sending out spam will be shut down. A review of the account will be performed to determine the cause of the actions.

E-mail is to be used for business purposes and in a manner that is consistent with other forms of professional business communication. All outgoing attachments are automatically scanned for virus and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm GATHERACT LLC's reputation.

The following activities are prohibited by policy:

- Sending e-mail that may be deemed intimidating, harassing, or offensive. This includes, but is not limited to: abusive language, sexually explicit remarks or pictures, profanities, defamatory or discriminatory remarks regarding race, creed, color, sex, age, religion, sexual orientation, national origin, or disability.
- Using e-mail for conducting personal business.
- Using e-mail for the purposes of sending SPAM or other unauthorized solicitations.
- Violating copyright laws by illegally distributing protected works.
- Sending e-mail using another person's e-mail account, except when authorized to send messages for another while serving in an administrative support role.
- Creating a false identity to bypass policy.
- Forging or attempting to forge e-mail messages.
- Using unauthorized e-mail software.
- Knowingly disabling the automatic scanning of attachments on any GATHERACT LLC personal computer.
- Knowingly circumventing e-mail security measures.
- Sending or forwarding joke e-mails, chain letters, or hoax letters.
- Sending unsolicited messages to large groups, except as required to conduct GATHERACT LLC business.
- Sending excessively large messages or attachments.
- Knowingly sending or forwarding email with computer viruses.

- Setting up or responding on behalf of GATHERACT LLC without management approval.

All confidential or sensitive GATHERACT LLC material transmitted via e-mail, outside GATHERACT LLC's network, must be encrypted. Passwords to decrypt the data should not be sent via email.

E-mail is not secure. Users must not e-mail passwords, social security numbers, account numbers, pin numbers, dates of birth, mother's maiden name, etc. to parties outside the GATHERACT LLC network without encrypting the data.

All user activity on GATHERACT LLC information system assets is subject to logging and review. GATHERACT LLC has software and systems in place to monitor email usage.

E-mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of GATHERACT LLC, unless appropriately authorized (explicitly or implicitly) to do so.

Users must not send, forward, or receive confidential or sensitive GATHERACT LLC information through non-GATHERACT LLC email accounts. Examples of non-GATHERACT LLC e-mail accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and e mail provided by other Internet Service Providers (ISP).

Users with non-GATHERACT LLC issued mobile devices must adhere to the Personal Device Acceptable Use and Security Policy for sending, forwarding, receiving, or storing confidential or sensitive GATHERACT LLC information.

Incidental Use

Incidental personal use of sending e-mail is restricted to GATHERACT LLC approved users; it does not extend to family members or other acquaintances.

Without prior management approval, incidental use must not result in direct costs to GATHERACT LLC.

Incidental use must not interfere with the normal performance of an employee's work duties.

No files or documents may be sent or received that may cause legal liability for or embarrassment to GATHERACT LLC.

Storage of personal files and documents within GATHERACT LLC's IT systems should be nominal.

E-mail Retention

- Messages are retained for 36 months. Emails older than 36 months are subject to automatic purging.

- Deleted and archived emails are subject to automatic purging.
- Appointments, Tasks, and Notes older than the retention period are subject to automatic purging.

Policy 8: Firewall

Definitions

Firewall: *Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.*

Firewall configuration: The system setting affecting the operation of a firewall appliance.

Firewall ruleset: A set of policy statements or instructions used by a firewall to filter network traffic.

Host firewall: A firewall application that addresses a separate and distinct host, such as a personal computer.

Internet Protocol (IP): Primary network protocol used on the Internet.

Network firewall: A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).

Network topology: The layout of connections (links, nodes, etc.) of a computer network.

Simple Mail Transfer Protocol (SMTP): An Internet standard for electronic mail (e mail) transmission across Internet Protocol (IP) networks.

Virtual private network (VPN): A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with private, secure access to their organization's network.

Overview

GATHERACT LLC operates network firewalls between the Internet and its private internal network to create a secure operating environment for GATHERACT LLC's computer and network resources. A firewall is just one element of a layered approach to network security.

Purpose

This policy governs how the firewalls will filter Internet traffic to mitigate the risks and losses associated with security threats to GATHERACT LLC's network and information systems.

The firewall will (at minimum) perform the following security services:

- Access control between the trusted internal network and untrusted external networks
- Block unwanted traffic as determined by the firewall ruleset

- Hide vulnerable internal systems from the Internet
- Hide information, such as system names, network topologies, and internal user IDs, from the Internet
- Log traffic to and from the internal network
- Provide robust authentication
- Provide virtual private network (VPN) connectivity

Policy Detail

All network firewalls, installed and implemented, must conform to the current standards as determined by GATHERACT LLC's IT Department. Unauthorized or non-standard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

The approach adopted to define firewall rulesets is that all services will be denied by the firewall unless expressly permitted in this policy.

- Outbound – allows all Internet traffic to authorized groups
- All traffic is authorized by Internet Protocol (IP) address and port

The firewalls will provide:

- Packet filtering – selective passing or blocking of data packets as they pass through a network interface. The most often used criteria are source and destination address, source and destination port, and protocol.

- Application proxy – every packet is stopped at the proxy firewall and examined and compared to the rules configured into the firewall.

- Stateful Inspection – a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.

The firewalls will protect against:

- IP spoofing attacks – the creation of IP packets with a forged source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.

- Denial-of-Service (DoS) attacks - the goal is to flood the victim with overwhelming amounts of traffic and the attacker does not care about receiving responses to the attack packets.

- Any network information utility that would reveal information about the GATHERACT LLC domain.

A change control process is required before any firewall rules are modified. Prior to implementation, the Third Party Vendor and GATHERACT LLC network administrators are required to have the modifications approved by the Director of IT or the VP of IT. All related documentation is to be retained for three (3) years.

All firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default. The ruleset should be opened incrementally to only allow permissible traffic.

Firewall rulesets and configurations require periodic review to ensure they afford the required levels of protection:

- GATHERACT LLC must review all network firewall rulesets and configurations during the initial implementation process and periodically thereafter.

Firewall rulesets and configurations must be backed up frequently to alternate storage (not on the same device). Multiple generations must be captured and retained, to preserve the integrity of the data, should restoration be required. Access to rulesets and configurations and backup media must be restricted to those responsible for administration and review.

Responsibilities

The IT Department is responsible for implementing and maintaining GATHERACT LLC firewalls, as well as for enforcing and updating this policy. Logon access to the firewall will be restricted to a primary firewall administrator and designees as assigned. Password construction for the firewall will be consistent with the strong password creation practices outlined in the GATHERACT LLC Password Policy.

The specific guidance and direction for information systems security is the responsibility of IT. Accordingly, IT will manage the configuration of the GATHERACT LLC firewalls.

GATHERACT LLC has contracted with a Third Party Vendor to manage the external firewalls. This vendor will be responsible for:

- Retention of the firewall rules
- Patch Management
- Review the firewall logs for:
    - o System errors
    - o Blocked web sites
    - o Attacks
- Sending alerts to the GATHERACT LLC network administrators in the event of attacks or system errors
- Backing up the firewalls

Policy 9: Hardware and Electronic Media Disposal

Definitions

Beyond reasonable repair: Refers to any and all equipment whose condition requires fixing or refurbishing that is likely to cost as much or more than total replacement.

Chain of Custody (CoC): *Refers to the chronological documentation of the custody, transportation, or storage of evidence to show it has not been tampered with prior to destruction.*

Disposition: *Refers to the reselling, reassignment, recycling, donating, or disposal of IT equipment through responsible, ethical, and environmentally sound means.*

Non-leased: *Refers to any and all IT assets that are the sole property of GATHERACT LLC, that is, equipment not rented, leased, or borrowed from a third-party supplier or partner company.*

Obsolete: Refers to any and all equipment that no longer meets requisite functionality.

Surplus: Refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

Overview

Hardware and electronic media disposition is necessary at GATHERACT LLC to ensure the proper disposition of all non-leased GATHERACT LLC IT hardware and media capable of storing member information. Improper disposition can lead to potentially devastating fines and lawsuits, as well as possible irreparable brand damage.

Purpose

GATHERACT LLC owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse, including media, are covered by this policy. Where assets have not reached end of life, it is desirable to take advantage of residual value through reselling, auctioning, donating, or reassignment to a less critical function. This policy will establish and define standards, procedures, and restrictions for the disposition of non-leased IT equipment and media in a legal, cost-effective manner. GATHERACT LLC's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and GATHERACT LLC's upgrade guidelines. All disposition procedures for retired IT assets must adhere to company approved methods.

Policy Detail

Disposition procedures for all IT assets and equipment will be centrally managed and coordinated by GATHERACT LLC's IT Department. The IT Department is responsible for backing up data from IT assets slated for disposition (if applicable) and removing company tags and/or identifying labels. IT is responsible for selecting and approving external agents for hardware sanitization, reselling, recycling, or destruction of the equipment. IT is also responsible for the chain of custody in acquiring credible documentation from contracted third parties that verify adequate disposition and disposal that adhere to legal requirements and environmental regulations

It is the responsibility of any employee of GATHERACT LLC's IT Department, with the appropriate authority, to ensure that IT assets are disposed of according to the methods in the Hardware and Electronic Media Disposal Procedure. It is imperative that all dispositions are done appropriately, responsibly, and according to IT lifecycle standards, as well as with GATHERACT LLC's resource planning in mind.

Hardware asset types and electronic media that require secure disposal include, but are not limited to, the following:

- Computers (desktops and laptops)
- Printers
- Handheld devices
- Servers
- Networking devices (hubs, switches, bridges, and routers)
- Floppy disks
- Backup tapes
- CDs and DVDs
- Zip drives
- Hard drives
- Flash memory
- Other portable storage devices

Policy 10: Security Incident Management

Definitions

Security incident: *Refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Incidents can include, but are not limited to, unauthorized access, malicious code, network probes, and denial of service attacks.*

Overview

Security Incident Management at GATHERACT LLC is necessary to detect security incidents, determine the magnitude of the threat presented by these incidents, respond to these incidents, and if required, notify GATHERACT LLC members of the breach.

Purpose

This policy defines the requirement for reporting and responding to incidents related to GATHERACT LLC information systems and operations. Incident response provides GATHERACT LLC with the capability to identify when a security incident occurs. If monitoring were not in place, the magnitude of harm associated with the incident would be significantly greater than if the incident were noted and corrected.

This policy applies to all information systems and information system components of GATHERACT LLC. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities.
- Devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities. • Firewalls, Intrusion Detection/Prevention (IDP) sensors, and other devices that provide dedicated security capabilities.

In the event a breach of member's information occurs, GATHERACT LLC is required by Wisconsin state law to notify the individual(s) as described in Wisconsin Statute Section 895.507(2).

Policy Detail

Program Organization

- **Computer Emergency Response Plans**

  GATHERACT LLC management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or
  degradation of service. For example, Charter connectivity is interrupted or an isolated malware discovery.

- **Incident Response Plan Contents**

  The GATHERACT LLC incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of relevant external partners. Specific areas covered in the plan include:

  o Specific incident response procedures
  o Business recovery and continuity procedures
  o Data backup processes
  o Analysis of legal requirements for reporting compromises
  o Identification and coverage for all critical system components o Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers

- **Incident Response Testing**
  - o At least once every year, the IT Department must utilize simulated incidents to mobilize and test the adequacy of response.
  - o Where appropriate, tests will be integrated with testing of related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.

- **Incident Response and Recovery**

  A security incident response capability will be developed and implemented for all information systems that house or access GATHERACT LLC controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:

  - o Preparation
  - o Detection
  - o Analysis
  - o Containment
  - o Eradication
  - o Recovery
  - o Post-Incident Activity

  To facilitate incident response operations, responsibility for incident handling operations will be assigned to an incident response team. If an incident occurs, the members of this team will be charged with executing the incident response plan. To ensure that the team is fully prepared for its responsibilities, all team members will be trained in incident response operations on an annual basis.

  Incident response plans will be reviewed and, where applicable, revised on an annual basis. The reviews will be based upon the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of plan revision, updated plans will be distributed to key stakeholders.

- **Intrusion Response Procedures**

  The IT Department must document and periodically revise the Incident Response Plan with intrusion response procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.

- **Malicious Code Remediation**

  Steps followed will vary based on scope and severity of a malicious code incident as determined by Information Security Management. They may include but are not limited to: malware removal with one or more tools, data quarantine, permanent data deletion, hard drive wiping, or hard drive/media destruction.

• **Data Breach Management**
GATHERACT LLC management should prepare, test, and annually update the Incident Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.

• **Incident Response Plan Evolution**
The Incident Response Plan must be updated to reflect the lessons learned from actual incidents.

The Incident Response Plan must be updated to reflect developments in the industry.

Program Communication

• **Reporting to Third Parties**
Unless required by law or regulation to report information security violations to external authorities, senior management, in conjunction with legal representatives, the Security Officer, and the VP of IT must weigh the pros and cons of external disclosure before reporting these violations.

If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.

If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Security Officer must be notified immediately.

• **Display of Incident Reporting Contact Information**
GATHERACT LLC contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters, and the intranet.

• **Member Notification**
The notification will be conducted and overseen by GATHERACT LLC's Director of Risk Management. The notification should contain, at a minimum, the following elements:

- Recommendations for the member to protect him/herself
- Contact information for the Federal Trade Commission
- Contact information for the credit bureaus

Sample notification letter:

[enter date here]

Dear *[enter member's name here],*

We, at GATHERACT LLC, believe in acting quickly in our member's best interest. We recently became aware of an incident involving unauthorized access to certain member's confidential information. *[describe here the incident in general terms]*

We have taken steps to mitigate the incident and protect our member's information from further risk. *[describe here the steps taken by GATHERACT LLC in general terms]*

This incident may have increased the probability of your information being used for fraudulent purposes. It is impossible to know with certainty whether you will experience trouble, but there are steps you can take to protect yourself. Here are some recommendations:

- Carefully review your account statements. If anything looks suspicious, promptly report the suspicious activity to GATHERACT LLC.

- Visit the Federal Trade Commission's (FTC) web site or call their toll-free number to obtain identity theft guidance and to report suspected incidents of identity theft.

  - http://www.ftc.gov/bcp/edu/microsites/idtheft//
  - Phone: 1-877-438-4338
  - TTY: 1-866-653-4261

- The Fair Credit Reporting Act allows you, under certain circumstances, to place a fraud alert in your consumer credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. Placing a fraud alert in your file entitles you to order one free copy of your credit report from each agency. Review your credit reports carefully for unauthorized inquiries or accounts you did not open.

  - TransUnion:
    Fraud Victim Assistance Division

PO Box 6790
Fullerton, CA 92834-6790

1-800-680-7289
www.transunion.com

o Equifax:

PO Box 740241
Atlanta, GA 30374-0241

1-800-525-6285
www.equifax.com

o Experian:

PO Box 9554
Allen, TX 75013

1-888-397-3742
www.experian.com

- You will need to remain observant for the next 12 to 24 months in checking your accounts for suspicious activity. Promptly report incidents of suspected identity theft to GATHERACT LLC.
- It is recommended that you obtain credit reports periodically from each of the nationwide credit reporting agencies and have information relating to fraudulent transactions deleted. Subscription services are available that can provide notification to you anytime there are changes or inquiries in your credit record.

Please do not hesitate to contact GATHERACT LLC at 608-755-6065 or 800-779-5555 for assistance and information related to this incident.

Sincerely,

GATHERACT LLC

Policy 11: Information Technology Purchasing

Overview

Information Technology purchasing at GATHERACT LLC must be managed to ensure compatibility and to control costs of the technology and services requested.

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for the purchase of all IT hardware, software, computer-related components, and technical services purchased with GATHERACT LLC funds.

Purchases of technology and technical services for GATHERACT LLC must be approved and coordinated through the IT Department.

Scope

The scope of this policy includes, but is not limited to, the following GATHERACT LLC technology resources:

- Desktops, laptops, smartphones/PDAs, cell phones, tablets, TCDs, TCRs, and servers
- Software running on the devices mentioned above
- Peripheral equipment, such as printers and scanners
- Cables or connectivity-related devices

- Audio-visual equipment, such as projectors and cameras

This policy extends to technical services, such as off-site disaster recovery solutions and Internet Service Providers (ISPs), as well as professional services, such as consultants and legal professionals hired through the IT Department. These include, but are not limited to, the following:

- Professionals or firms contracted for application development and maintenance
- Web services provided by a third party
- Consulting professionals
- Recruiting services
- Training services
- Disaster recovery services
- Hosted telephone services
- Telephone network services
- Data network services

Policy Detail

All hardware, software, or components purchased with GATHERACT LLC funds are the property of GATHERACT LLC. This also includes all items purchased using a personal credit card, for which the employee is later reimbursed.

All purchase requests for hardware, software, computer-related components, internet services, or third-party electronic services must be submitted to the IT Department, via the Service Desk, for final purchase approval. If the requested item is already in inventory, then it will be made available to the requestor, assuming that it meets organizational unit goals.

For purchases within IT

A procurement procedure is maintained by the CEO. Purchasing within the IT Department falls under four general categories.

- **Standard Items**

  Purchase of items, which have been pre-approved by IT management, that require only a Service Desk request.

  The standard items list, located in the IT procedure documentation, contains preapproved vendors and products which GATHERACT LLC has standardized. Standard items have been proven to be both supportable by the IT Department, as well as cost effective.

- **Non-Standard Items**

  Purchase of non-standard items/services, which are not classified as capital expenses, such as non-standard hardware/software that is expensed or contracted services.

Non-standard purchases should be minimized as much as reasonably possible. Requests for non-standard items will go through a formal selection process that will involve thorough vendor sourcing. IT will review non-standard purchases for viability of support and compatibility.

The selection process may vary depending on the type, cost, and other purchase significance factors. Before approval will be granted, employees or departments requesting non-emergency specialized software, or components, must submit a plan detailing how this item will be supported. Support options include assigning a staff member to maintain and/or support the component, arranging for external vendor support, or arranging for a service-level agreement with the IT Department.

Individuals requesting non-standard items for purchase can suggest a potential vendor, if a pre-existing relationship exists between that vendor and GATHERACT LLC.

- **Capital Expenses**

  Purchase of non-standard capitalized hardware, software, or equipment.

  Capitalized expenditures, defined as hardware, software, or equipment above $2,500.00 or as specified in the GATHERACT LLC Fixed Asset Policy, which are capitalized by GATHERACT LLC, must go through the CFO and CEO for approval. These purchases may only be requisitioned by department managers. The purchase selection process for these expenditures will be evaluated by Senior Management.

- **Employee Purchasing**

  Items that do not require any purchase approval.

System replacement

Major technology purchases are approved through the budgetary process. Equipment replaced during the course of any period shall be based on a minimum annual review of the asset management program and hardware replenishment schedule, hardware inventory, and fixed asset budget schedules.

Asset Management Program

Certain classes of GATHERACT LLC assets, as defined below (“Qualified Assets” or “Asset”), procured or curated by the GATHERACT LLC Information Technology department shall be duly managed with the objective of protecting them from misappropriation and unplanned obsolescence. Methods shall be devised and followed to allow for asset identification, assignment, tracking, lifecycle management, reporting, and disposition.

Included asset classes are as follows: Technology equipment, computer hardware, peripherals, and other items purchased by GATHERACT LLC IT or managed by same that are

- semi-permanent in their end-user assignment (example: specific person, department) or purpose (example: loaner laptop, projector) AND
- are valued at greater than $300 AND
- are not high-turnover or frequently moved devices (example: small peripherals such as mice and ID scanners)

Reimbursable Expenses

Paying for and/or reimbursing employees will be handled with a completed Expense Report submitted to the VP of IT.

GATHERACT LLC will also include expenses incurred by employees and will reimburse the following, in addition to standard travel expenses, as indicated in the Employee Reimbursement Policy:

- Standard item peripheral hardware
- Business related shipping/courier expenses

Policy 12: Internet

Definitions

Internet: *A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges.*

Intranet: A private network for communications and sharing of information that, like the Internet, is based on Transmission Control Protocol/Internet Protocol (TCP/IP), but is accessible only to authorized employees within an organization. An organization's intranet is usually protected from external access by a firewall.

User: An individual or automated application or process that is authorized access to the resource by the system owner, in accordance with the system owner's procedures and rules.

World Wide Web (www): A system of Internet hosts that supports documents formatted in Hypertext Markup Language (HTML) that contains links to other documents (hyperlinks) and to audio, video, and graphic images. Individuals can access the Web with special applications called browsers, such as Microsoft Internet Explorer.

Overview

Internet access and usage at GATHERACT LLC must be managed as valuable and mission critical resources. This policy is established to:

• Create prudent and acceptable practices regarding the use of the Internet. • Educate individuals who may use information resources with respect to their responsibilities associated with such use.

Purpose

The purpose of this policy is to establish the rules for the use of GATHERACT LLC Internet for access to the Internet or the Intranet.

Audience

This policy applies equally to all individuals granted access privileges to any GATHERACT LLC information system or resource with the capacity to access the Internet, the Intranet, or both.

Policy Detail

Accessing the Internet

Users are provided access to the Internet to assist them in the performance of their jobs. At any time, at the request of management, Internet access may be revoked. IT may restrict access to certain Internet sites that reduce network performance or are known or found to be compromised with and by malware. GATHERACT LLC will use internet filters *to block high-risk content and deny access to any unwanted material or malware in support of the Acceptable Use Policy.*

All software used to access the Internet must be part of the GATHERACT LLC standard software suite or approved by IT. Such software must incorporate all vendor provided security patches.

Users accessing the Internet through a computer connected to GATHERACT LLC's network must do so through an approved Internet firewall or other security device. All software used to access the Internet shall be configured to use a proxy or other means of managing or controlling. Bypassing GATHERACT LLC's network security, by accessing the Internet directly, is strictly prohibited.

Users are prohibited from using GATHERACT LLC Internet access for: unauthorized access to local and remote computer systems, software piracy, illegal activities, the transmission of threatening, obscene, or harassing materials, or personal solicitations.

Expectation of privacy

Users should have no expectation of privacy in anything they create, store, send, or receive using GATHERACT LLC's Internet access.

Users expressly waive any right of privacy in anything they create, store, send, or receive using GATHERACT LLC's Internet access.

File downloads and virus protection

Users are prohibited from downloading and installing software on their PC without proper authorization from IT. Technical controls may be utilized to limit the download and installation of software.

Downloaded software may be used only in ways that conform to its license and copyrights.

All files, downloaded from the Internet, must be scanned for viruses using GATHERACT LLC approved virus detection software. If a user suspects a file may be infected, he/she must notify IT immediately.

Users are prohibited from using the Internet to deliberately propagate any virus, worm, Trojan Horse, trap-door, or other malicious program.

Monitoring of computer and Internet usage

All user activity on GATHERACT LLC IT assets is subject to logging and review. GATHERACT LLC has the right to monitor and log all aspects of its systems including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.

Frivolous use

Computer resources are not unlimited. Network bandwidth and storage capacity have *finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.*

Personal use, beyond incidental use of the Internet, may be done only on break room PCs and only in compliance with this policy.

Content

GATHERACT LLC utilizes software that makes it possible to identify and block access to Internet sites containing sexually explicit material or other material deemed inappropriate in the workplace. The display, storing, archiving, or editing of such content on any GATHERACT LLC PC is prohibited.

Users are prohibited from attempting to access or accessing inappropriate sites from any GATHERACT LLC PC. If a user accidentally connects to a site containing such material, the user must disconnect at once and report the incident immediately to IT.

GATHERACT LLC Departments may not host their own websites or contract for the hosting of websites by a vendor without the permission of IT.

Content on all GATHERACT LLC hosted websites must comply with the GATHERACT LLC Acceptable Use of Information Systems and Privacy Policies. No internal data will be made available to hosted Internet websites without approval of IT.

No personal or non-GATHERACT LLC commercial advertising may be made available via hosted GATHERACT LLC websites.

Transmissions

All sensitive GATHERACT LLC material transmitted over the Internet or external network must be encrypted.

Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

Incidental use

Incidental personal use of Internet access is restricted to GATHERACT LLC approved Users; it does not extend to family members or other acquaintances.

Incidental use must not result in direct costs to GATHERACT LLC.

Incidental use must not interfere with the normal performance of an employee's work *duties.*

No files or documents may be sent or received that may cause legal liability for, or embarrassment to, GATHERACT LLC. Storage of personal files and documents within GATHERACT LLC's IT should be nominal.

All files and documents, including personal files and documents, are owned by GATHERACT LLC, may be subject to open records requests, and may be accessed in accordance with this policy.

Reimbursement

An employee, whose position requires him/her to have remote access, will be reimbursed for his/her Internet expenses up to a reasonable amount if agreed upon as part of his/her contract. An Expense Report will need to be completed and submitted to his/her manager for approval.

Policy 13: Log Management

Definitions

End points: *Any user device connected to a network. End points can include personal computers, personal digital assistants, scanners, etc.*

Flow: *The traffic that corresponds to a logical connection between two processes in the network.*

IP: *Internet Protocol is the method or protocol by which data is sent from one computer to another on the Internet.*

Packet: *The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.*

Overview

Most components of the IT infrastructure at GATHERACT LLC are capable of producing logs chronicling their activity over time. These logs often contain very detailed information about the activities of applications and the layers of software and hardware that support those applications.

Logging from critical systems, applications, and services can provide key information and potential indicators of compromise and is critical to have for forensics analysis.

Purpose

Log management can be of great benefit in a variety of scenarios, with proper management, to enhance security, system performance, resource management, and regulatory compliance. GATHERACT LLC will perform a periodic risk assessment to determine what information may be captured from the following:

- Access – who is using services
- Change Monitoring – how and when services were modified
- Malfunction – when services fail
- Resource Utilization – how much capacity is used by services
- Security Events – what activity occurred during an incident, and when
- User Activity – what people are doing with services

Policy Detail

Log generation

Depending on the volume of activity and the amount of information in each log entry, logs have the potential of being very large. Information in logs often cannot be controlled by application, system, or network administrators, so while the listed items are highly desirable, they should not be viewed as absolute requirements.

Application logs

Application logs identify what transactions have been performed, at what time, and for whom. Those logs may also describe the hardware and operating system resources that were used to execute that transaction.

System logs

System logs for operating systems and services, such as web, database, authentication, print, etc., provide detailed information about their activity and are an integral part of system administration. When related to application logs, they provide an additional layer of detail that is not observable from the application itself. Service logs can also aid in intrusion analysis, when an intrusion bypasses the application itself.

Change management logs, that document changes in the IT or business environment, provide context for the automatically generated logs.

Other sources, such as physical access or surveillance logs, can provide context when investigating security incidents.

Client workstations also generate system logs that are of interest, particularly for local authentication, malware detection, and host-based firewalls.

Network logs

Network devices, such as firewalls, intrusion detection/prevention systems, routers, and switches are generally capable of logging information. These logs have value of their own to network administrators, but they also may be used to enhance the information in application and other logs.

Many components of the IT infrastructure, such as routers and network-based firewalls, generate logs. All of the logs have potential value and should be maintained. These logs typically describe flows of information through the network, but not the individual packets contained in that flow.

Other components for the network infrastructure, such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) servers, provide valuable information about network configuration elements, such as IP addresses, that change over time.

Time synchronization

One of the important functions of a log management infrastructure is to relate records from various sources by time. Therefore, it is important that all components of the IT infrastructure have synchronized clocks. GATHERACT LLC uses Network Time Protocol (NTP) for time synchronization.

Use of log information

Logs often contain information that, if misused, could represent an invasion of the privacy of members of GATHERACT LLC. While it is necessary for GATHERACT LLC to perform regular collection and monitoring of these logs, this activity should be done in the least invasive manner.

Baseline behavior

It is essential that a baseline of activity, within the IT infrastructure, be established and tracked as it changes over time. Understanding baseline behavior allows for the detection of anomalous behavior, which could indicate a security incident or a change in normal usage patterns. Procedures will be in place to ensure that this information is reviewed on a regular and timely basis.

Investigation

When an incident occurs, various ad hoc questions will need to be answered. These incidents may be security related, or they may be due to a malfunction, a change in the IT infrastructure, or a change in usage patterns. Whatever the cause of the incident, it will be necessary to retrieve and report log records.

Thresholds shall be established that dictate what level of staff or management response is required for any given log entry or group of entries and detailed in a procedure.

Log record life-cycle management

When logs document or contain valuable information related to activities of GATHERACT LLC's information resources or the people who manage those resources, they are GATHERACT LLC Administrative Records, subject to the requirements of GATHERACT LLC to ensure that they are appropriately managed and preserved and can be retrieved as needed.

Retention

To facilitate investigations, as well as to protect privacy, the retention of log records should be well-defined to provide an appropriate balance among the following:

- Confidentiality of specific individuals' activities
- The need to support investigations
- The cost of retaining the records

Care should be taken not to retain log records that are not needed. The cost of long term retention can be significant and could expose GATHERACT LLC to high costs of retrieving and reviewing the otherwise unneeded records in the event of litigation. Most logs should not be retained for more than 7 days.

Log management infrastructure

A log management infrastructure will be established to provide common management of log records. To facilitate the creation of log management infrastructures, system-wide groups will be established to address the following issues:

- Technology solutions that can be used to build log management infrastructures

- Typical retention periods for common examples of logged information

Policy 14: Safeguarding Member Information

Definitions

These terms are defined by the NCUA Part 748.

Member: *An individual who has an established, ongoing relationship with GATHERACT LLC. This includes both members and non-members who have co-signed on loans. Examples of non-members include, but are not limited to, the following:*

- *Non-member joint account holders*
- *Non-members holding an account in a state-chartered credit union under state law*

Service provider: *A third party that maintains, processes, or otherwise is permitted access to member information while performing services for GATHERACT LLC.*

Member information: *Any record maintained by, or on behalf of, GATHERACT LLC that contains information regarding an individual who has an established, ongoing relationship with GATHERACT LLC. This includes records, data, files, or other information in paper, electronic, or other form that are maintained by, or on behalf of, any service provider on behalf of GATHERACT LLC.*

Member information system: *Any electronic or physical method used to access, collect, store, use, transmit, protect, or dispose of member information.*

Overview

This policy addresses the following topics:

- Board Involvement
- Risk Assessment
- Management and Control of Risk
- Member Information Security Controls
    - o Vendor Management Review Program
    - o Software Inventory
    - o Hardware Inventory
    - o Critical Systems List
    - o Records Management
    - o Clean Desk Policy
    - o Hardware and Electronic Media Disposal Policy
    - o IT Acquisition Policy
    - o Incident Response Plan
    - o Information Sharing
- Training
- Testing

Purpose

The purpose of this policy is to ensure that GATHERACT LLC complies with existing federal and state laws, and to ensure that information regarding members is kept secure and confidential.

Policy Detail

It is the policy of GATHERACT LLC to protect the confidentiality, security, and integrity of each member's non-public personal information in accordance with existing state and federal laws. GATHERACT LLC will establish and maintain appropriate standards relating to administrative, technical, and physical safeguards for member records and information.

GATHERACT LLC will maintain physical, electronic, and procedural safeguards, which comply with federal standards, to guard members' non-public personal information.

GATHERACT LLC will not gather, collect, or maintain any information about its members that is not necessary to offer its products and services, to complete member transactions, or for other relevant business purposes.

GATHERACT LLC does not sell or provide any member information to third parties, including list services, telemarketing firms, or outside companies for independent use.

The Board of Directors must approve the Safeguarding Member Information Policy, required by NCUA Part 748 Appendix A.

GATHERACT LLC's Information Security Officer is responsible for annually reviewing the program, making any needed adjustments, and coordinating staff training. GATHERACT LLC Management is responsible for ensuring that its departments comply with the requirements of the program.

Information Security Program

Management is responsible for developing, implementing, and maintaining an effective information security program to:

- Ensure the security and confidentiality of member records and information
- Protect against any anticipated threats or hazards to the security or integrity of such records
- Protect against unauthorized access to, or use of, such records or information that would result in substantial harm or inconvenience to any member

Management shall report to the Board of Directors, at least annually, on the current status of GATHERACT LLC's Information Security Program. The Board of Directors will also be notified of any security breaches or violations and the management team's response and recommendations for changes in the Information Security Program.

Board Involvement

On an annual basis, the Board of Directors is required to provide the NCUA and DFI Regional Director with a certification of GATHERACT LLC's compliance with NCUA Part 748. The certification is contained in the Report of Officials submitted after the annual election of officials. Prior to the certification, GATHERACT LLC's Information Security Officer will provide the Board with a status report of GATHERACT LLC's Safeguarding Member Information Program.

Risk Assessment

GATHERACT LLC maintains a risk assessment that identifies potential threats to member information and evaluates the potential impact of the threats.

On an annual basis, the risk assessment is reviewed and updated by the Information Security Officer and GATHERACT LLC's Management. GATHERACT LLC's controls are then updated accordingly.

Management and Control of Risk

In order to manage and control the risks that have been identified, GATHERACT LLC will:

- Establish written procedures designed to implement, maintain, and enforce GATHERACT LLC's information security program

- Limit access to GATHERACT LLC's member information systems to authorized employees only

- Establish controls to prevent employees from providing member information to unauthorized individuals

- Limit access at GATHERACT LLC's physical locations containing member information, such as building, computer facilities, and records storage facilities, to authorized individuals only

- Provide encryption of electronic member information including, but not limited to, information in transit or in storage on networks or systems to which unauthorized individuals may have access.

- Ensure that member information system modifications are consistent with GATHERACT LLC's information security program

- Implement dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, member information

- Monitor GATHERACT LLC's systems and procedures to detect actual and attempted attacks on, or intrusions into, the member information systems

- Establish response programs that specify actions to be taken when GATHERACT LLC suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies

- Implement measures to protect against destruction, loss, or damage of member information due to environmental hazards, such as fire and water damage or technical failures

- Regularly test, monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of member information, business arrangements, outsourcing arrangements, and internal or external threats to GATHERACT LLC's information security systems

Member information security controls

GATHERACT LLC has established a series of member information security controls to manage the threats identified in the risk assessment. The controls fall into ten categories.

- **Vendor management review program**

  GATHERACT LLC will exercise appropriate due diligence when selecting service providers. When conducting due diligence, management will conduct a documented vendor review process as outlined in the Vendor Due Diligence Procedure. GATHERACT LLC will also consider obtaining SSAE 16 reports from prospective service providers.

  All service providers, who may access member information, must complete a Vendor Confidentiality Agreement requiring the provider to maintain the safekeeping and confidentiality of member information in compliance with applicable state and federal laws. Such agreements must be obtained prior to any sharing of member information. Once the agreement has been completed, management will, according to risk, monitor service providers by reviewing audits, summaries of test results, or other evaluations.

- **Software inventory**

  GATHERACT LLC will maintain an inventory of its desktop, server, and infrastructure software. The information from this collection will provide critical information in identifying the software required for rebuilding systems. A template incorporated into the software inventory ensures that the security configuration and configuration standards are enforced. The template will also provide personnel with a quick resource in the event of a disaster. The software inventory list will be reviewed and updated on a continual basis.

- **Hardware inventory**

  GATHERACT LLC will maintain an inventory of its desktop, server, and infrastructure hardware. The information from this collection will provide critical information in identifying the hardware requirements for rebuilding systems. A template incorporated into the hardware inventory ensures that GATHERACT LLC standards are enforced. The template will also provide personnel with a quick resource in the event of a disaster. The hardware inventory list will be reviewed and updated on a continual basis.

- **Critical systems list**

  GATHERACT LLC will maintain a listing of its critical systems. This listing will support critical reliability functions, communications, services, and data. The identification of these systems is crucial for securing member information from vulnerabilities, performing impact analysis, and in preparing for unscheduled events that affect the operations of GATHERACT LLC.

- **Records management**

  The industry wide general principles of records management apply to records in any format. GATHERACT LLC will adhere to policies and procedures for protecting critical records from all outside and unauthorized access. Access to sensitive data will be defined as to who can access which data and under what circumstances. The access will be logged to provide accountability.

  GATHERACT LLC will adhere to the required state statues, NCUA, Data Classification Procedures, and federal guidelines designated for record retention. GATHERACT LLC will adhere to the Records Retention Policy for the proper process to dispose of records. Record disposal will be well documented. An inventory will be maintained of the types of records that are disposed of, including certification that the records have been destroyed.

- **Clean desk policy**

  GATHERACT LLC employees will comply with the Clean Desk Policy. This policy was developed to protect sensitive data from being readily available to unauthorized individuals.

- **Hardware and electronic media disposal procedure**

  GATHERACT LLC will take precautions, as outlined in the Hardware and Electronic Media Disposal Policy, to ensure sensitive data cannot be retrieved from retired hardware or electronic media.

- **IT acquisition policy**

  GATHERACT LLC will adhere to policies and procedures for acquisition of computer related items. Computer related purchases will be reviewed by designated IT personnel for compliance with security plans and alignment with operational and strategic plans. An annual review of acquisition policies and procedures will occur with input from the Information Security Officer.

  A review of technology needs will occur during the annual budgeting and work planning processes. Needs will be classified into either current year plans or long range needs. The acquisition of technology solutions will be assessed to ensure that both current and future needs are met.

- **Incident response plan**

Incident response is defined as an organized approach to addressing and managing the aftermath of a security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

As required in the Incident Response Plan, GATHERACT LLC will assemble a team to handle any incidents that occur. Necessary actions to prepare GATHERACT LLC and the Incident Response Team will be conducted prior to an incident as required in the Incident Response Plan.

Below is a summary of the steps the IT Department, as well as GATHERACT LLC management, would take:

- The IT Department will immediately investigate the intrusion to:
    - Prevent any further intrusion to the system
    - Determine the extent of the intrusion and any damage caused
    - Take any steps possible to prevent any future such intrusions
- The IT Department will notify Administrative Management and Risk Management of the intrusion. Administrative Management will be responsible for notifying the Board of Directors.
- The IT Department will follow escalation processes and notification procedures as outlined in the Incident Response Plan. Examples include, but are not limited to, notifications to staff, regulatory agencies, law enforcement agencies, FBI, NCUA, or the public.
- If applicable, the Director of Compliance Bank Secrecy Act Officer (BSA) will be notified and will file a Suspicious Activity Report with FinCEN.
- If applicable, notices will be sent to affected members in compliance with the requirements of Wisconsin State Civil Codes.

- **Information Sharing**

GATHERACT LLC recognizes the value in the concept of information and intelligence sharing. This may be done through free or paid subscriptions to periodicals, especially electronically disseminated content such as email and RSS feeds, websites, and threat intelligence feeds that are accurate to the day and even up to-the-minute. Management will ensure that they and appropriate staff have access to information sharing forums or platforms and the means to use them and use them in our information security practice. Also, certain channels may be conducive to out-sharing pertinent information to peers, law enforcement, regulatory bodies or other authorities. The information shared and the receiving party must be considered in reporting candidly, anonymously, or otherwise to ensure there is no breach of confidence.

Training

GATHERACT LLC recognizes that adequate training is of primary importance in preventing IT security breaches, virus outbreaks, and other related problems. GATHERACT LLC will conduct regular IT training through methods such as staff meetings and computer based tutorial programs. In addition, employees will be trained to recognize, respond to, and where appropriate, report any unauthorized or fraudulent attempts to obtain member information.

All new employees will receive IT Security Training, as part of their orientation training, emphasizing security and IT responsibility. The Training Specialist, or designee, is responsible for training new employees on Information Security.

Testing

The Information Security Officer annually audits GATHERACT LLC's Safeguarding Member Information Program. The Information Security Officer provides a formal report of its findings to Senior Management, the Security Officer, and the Board of Directors.

GATHERACT LLC will require periodic tests of the key controls, systems, and procedures of the information security program. In accordance with current industry standards, the frequency and nature of such tests shall be determined by the IT Department. The Information Security Officer will be responsible for reviewing the results of these tests and for making recommendations for improvements where needed.

Policy 15: Network Security and VPN Acceptable Use

Definitions

Virtual Private Network (VPN): A private network that extends across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Some VPNs allow employees to securely access a corporate intranet while located outside the office.

User Authentication: *A method by which the user of a system can be verified as a legitimate user independent of the computer or operating system being used.*

Multi-Factor Authentication: *A method of computer access control in which a user is granted access only after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories:* o *Knowledge (something they know)*

o *Possession (something they have)*
o *Inherence (something they are)*

Dual Homing: *Having concurrent connectivity to more than one network from a computer or network device. Examples include:*

o *Being logged into the corporate network via a local Ethernet connection, and dialing into AOL or another Internet Service Provider (ISP)*
o *Being on a GATHERACT LLC provided remote access home network, and connecting to another network, such as a spouse's remote access*
o *Configuring an Integrated Services Digital Network (ISDN) router to dial into GATHERACT LLC and an ISP, depending on packet destination*

DSL: *Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).*

ISDN: *There are two flavors of ISDN: BRI and PRI. BRI is used for home/office/remote access. BRI has two "Bearer" channels at 64kb (aggregate 128kb) and 1 D channel for signaling information.*

Remote Access: *Any access to GATHERACT LLC's corporate network through a non GATHERACT LLC controlled network, device, or medium.*

Split-tunneling: *Simultaneous direct access to a non-GATHERACT LLC network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into GATHERACT LLC's corporate network via a Virtual Private network (VPN) tunnel. VPN is a method for accessing a remote network via* *“tunneling: through the Internet.*

IPSec Concentrator: *A device in which VPN connections are terminated.*

Cable Modem: *Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.*

CHAP: *Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user’s access channel in a frame relay network and has local significance only to that channel.*

Overview

This policy is to protect GATHERACT LLC's electronic information from being inadvertently compromised by authorized personnel connecting to the GATHERACT LLC network locally and remotely via VPN.

Purpose

The purpose of this policy is to define standards for connecting to GATHERACT LLC's network from any host. These standards are designed to minimize the potential exposure to GATHERACT LLC from damages, which may result from unauthorized use of GATHERACT LLC resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical GATHERACT LLC internal systems, etc.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, ISDN, DSL, VPN, SSH, and cable modems, etc.

Audience

This policy applies to all GATHERACT LLC employees, volunteers/directors, contractors, vendors, and agents with a computer or workstation used to connect to the GATHERACT LLC network. This policy applies to remote access connections used to do work on behalf of GATHERACT LLC, including reading or sending email and viewing intranet resources.

Policy Detail

Network Security

Users are permitted to use only those network addresses assigned to them by GATHERACT LLC's IT Department.

All remote access to GATHERACT LLC will either be through a secure VPN connection on a GATHERACT LLC owned device that has up-to-date anti-virus software, or on approved mobile devices (see the GATHERACT LLC Owned Mobile Device

Acceptable Use and Security Policy and the Personal Device Acceptable Use and Security Policy).

Remote users may connect to GATHERACT LLC Information Systems using only protocols approved by IT.

Users inside the GATHERACT LLC firewall may not be connected to the GATHERACT LLC network at the same time a remote connection is used to an external network.

Users must not extend or re-transmit network services in any way. This means a user must not install a router, switch, hub, or wireless access point to the GATHERACT LLC network without GATHERACT LLC IT approval.

Users must not install network hardware or software that provides network services without GATHERACT LLC IT approval.

Non-GATHERACT LLC computer systems that require network connectivity must be approved by GATHERACT LLC IT.

Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, GATHERACT LLC users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the GATHERACT LLC network infrastructure. Only the IT Department is permitted to perform these actions.

Users are not permitted to alter network hardware in any way.

Remote Access

It is the responsibility of GATHERACT LLC employees, volunteers/directors, contractors, vendors, and agents, with remote access privileges to GATHERACT LLC's corporate network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to GATHERACT LLC.

General access to the Internet, through the GATHERACT LLC network is permitted for employees who have flat-rate services and only for business purposes. GATHERACT LLC employees are responsible to ensure that they:

- Do not violate any GATHERACT LLC policies
- Do not perform illegal activities
- Do not use the access for outside business interests

GATHERACT LLC employees bear responsibility for the consequences should access be misused.

Employees are responsible for reviewing the following topics (listed elsewhere in this policy) for details of protecting information when accessing the corporate network via remote access methods and acceptable use of GATHERACT LLC's network:

- Virtual Private Network (VPN)
- Wireless Communications

Dial-in modem usage is not a supported or acceptable means of connecting to the GATHERACT LLC network.

Requirements

Secure remote access must be strictly controlled. Control will be enforced with Multi Factor Authentication (MFA).

GATHERACT LLC employees, volunteers/directors, and contractors should never provide their login or email password to anyone, including family members.

GATHERACT LLC employees, volunteers/directors, and contractors with remote access privileges:

- Must ensure that their computer, which is remotely connected to GATHERACT LLC's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

- Must not use non-GATHERACT LLC email accounts (i.e. Hotmail, Yahoo, AOL), or other external resources to conduct GATHERACT LLC business, thereby ensuring that official business is never confused with personal business.

Reconfiguration of a home user's equipment for split-tunneling or dual homing is not permitted at any time.

For remote access to GATHERACT LLC hardware, all hardware configurations must be approved by IT.

All hosts that are connected to GATHERACT LLC internal networks, via remote access technologies, must use up-to-date, anti-virus software applicable to that device or platform.

Organizations or individuals who wish to implement non-standard Remote Access solutions to the GATHERACT LLC production network must obtain prior approval from IT.

Virtual Private Network (VPN)

The purpose of this section is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the GATHERACT LLC corporate network. This applies to implementations of VPN that are directed through an IPSec Concentrator.

This applies to all GATHERACT LLC employees, volunteers/directors, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPN's to access the GATHERACT LLC network.

Approved GATHERACT LLC employees, volunteers/directors, and authorized third parties (customers, vendors, etc.) may utilize the benefit of a VPN on a GATHERACT LLC device, which is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and paying associated fees. Further details may be found in the Remote Access section.

The following guidelines will also apply:

- It is the responsibility of employees or volunteer/directors, with VPN privileges, to ensure that unauthorized users are not allowed access to GATHERACT LLC internal networks.
- VPN use is controlled using a multi-factor authentication paradigm.
- When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped.
- VPN gateways will be set up and managed by GATHERACT LLC IT.
- All computers connected to GATHERACT LLC internal networks via VPN or any other technology must use up-to-date, anti-virus software applicable to that device or platform.
- VPN users will be automatically disconnected from GATHERACT LLC's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 hours.
- To ensure protection from viruses, as well as protection of member data, only GATHERACT LLC-owned equipment or non-GATHERACT LLC devices in accordance with the Personal Device Acceptable Use and Security Policy (BYOD) will have VPN and Remote Access.
- Only IT approved VPN clients may be used.
- By using VPN technology, users must understand that their machines are an extension of GATHERACT LLC's network and as such are subject to the same rules and regulations, as well as monitoring for compliance with this policy.

VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a GATHERACT LLC approved VPN configured to drop all unauthenticated and unencrypted traffic and will be provisioned with split-tunneling disabled. As with all GATHERACT LLC computers, Windows or other OS and/or browser Internet proxy settings will be enabled to effectively route Internet access to the device through GATHERACT LLC firewalls and Internet filters. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 128 bits, support a hardware address that can be registered and tracked (i.e. a MAC address), and support and employ strong user authentication, which checks against an external database such as TACACS+, iDiTJS, or something similar.

Any deviation from this practice will be considered on a case-by-case basis.

VPN Approval, Acceptable Use Review and Acceptance

Approval from a staff director or higher authority is required for a user's VPN access account creation. An acceptable use form is attached to the VPN procedure maintained by Information Technology and shall be reviewed and signed by each approved user to acknowledge having read and understood the policy (see Exhibit A). This form shall in turn be approved, collected, and retained by IT management prior to the user's VPN account use.

Wireless Communications

Access to GATHERACT LLC networks is permitted on wireless systems that have been granted an exclusive waiver by IT for connectivity to GATHERACT LLC's networks.

This section covers any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to GATHERACT LLC's networks do not fall under the review of this policy.

Register Access Points and Cards

All wireless Access Points/Base Stations connected to the corporate network must be registered and approved by IT. If they are installed in corporate PCs, all wireless Network Interface Cards (i.e. PC cards) used in corporate laptop or desktop computers must be registered with IT.

Approved Technology

All wireless LAN access must use GATHERACT LLC approved vendor products and security configurations.

Setting the Service Set Identifier (SSID)

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

EXHIBIT A

[This exhibit is a copy of the Addendum A in the VPN Connectivity to Network Procedure.doc]

Virtual Private Network (VPN) Agreement

This Virtual Private Network Agreement is entered into between the User and GATHERACT LLC, effective the date this agreement is executed by GATHERACT LLC's Information Technology Department (IT). The parties agree as follows:

ELIGIBILITY

The use of a mobile device connecting to the GATHERACT LLC network is a privilege granted to the User by management approval per the Network Security and VPN Acceptable Use Policy. If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to GATHERACT LLC and to ensure the data remains secure.

In the event of a security breach or threat, GATHERACT LLC reserves the right, without prior notice to the User, to disable or disconnect the VPN connection of the mobile device.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following GATHERACT LLC policies, published elsewhere and made available, is mandatory: Acceptable Use of Information Systems, Anti-Virus, E-Mail, Password, Safeguarding Member Information, and Telecommuting.

User of the mobile device shall not remove sensitive information from the GATHERACT LLC network, attack GATHERACT LLC assets, or violate any of the security polices related to the subject matter of this agreement.

The User understands and agrees that his/her use of the VPN software is required as part of his/her employment at GATHERACT LLC and is permitted to connect to internal information services in support of GATHERACT LLC activities only. The User will safeguard the VPN access as well as its components (software/password) from any unauthorized use.

The VPN will be used on a company issued mobile device that is protected by a personal firewall. The company issued mobile device may be subject to scanning from the IT Department to check compliance with the contents of this Agreement.

SUPPORT

GATHERACT LLC will offer support for connectivity to the GATHERACT LLC network. GATHERACT LLC is not responsible for ISP outages that result in a failure of connectivity to the GATHERACT LLC network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the GATHERACT LLC network.

The User certifies that this Agreement has been read and has an understanding of the above conditions under which the User may be provided access to GATHERACT LLC computer/information systems and further that the User understands and agrees to abide by them. The User also understands that limitations on disclosure of any information covered under this Agreement shall survive the modification or elimination of the User access to GATHERACT LLC computer/information systems.

____ ______________

User Date

____ ________________

IT Department Management Date

Rev. 0.2 – 12/2016

Policy 16: Personal Device Acceptable Use and Security (BYOD)

Definitions

Bring Your Own Device (BYOD): Privately owned wireless and/or portable electronic handheld equipment.

Overview

Acceptable use of BYOD at GATHERACT LLC must be managed to ensure that access to GATHERACT LLC's resources for business are performed in a safe and secure manner for participants of the GATHERACT LLC BYOD program. A participant of the BYOD program includes, but is not limited to:

- Employees
- Contractors
- Board of Directors
- Volunteers
- Related constituents who participate in the BYOD program

This policy is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

Purpose

This policy defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access corporate data using their personal device. This policy applies to, but is not limited to, any mobile devices owned by any users listed above participating in the GATHERACT LLC BYOD program which contains stored data owned by GATHERACT LLC, and all devices and accompanying media that fit the following device classifications:

- Laptops. Notebooks, and hybrid devices
- Tablets
- Mobile/cellular phones including smartphones
- Any non-GATHERACT LLC owned mobile device capable of storing corporate data and connecting to an unmanaged network

Refer to the Company and Personally Owned Mobile Device Procedure.

This policy addresses a range of threats to, or related to, the use of GATHERACT LLC data:

Threat	Description
Loss	Devices used to transfer, or transport work files could be lost or stolen
Theft	Sensitive corporate data is deliberately stolen and sold by an employee
Copyright	Software copied onto a mobile device could violate licensing
Malware	Virus, Trojans, Worms, Spyware and other threats could be introduced via a mobile device
Compliance	Loss or theft of financial and/or personal and confidential data could expose GATHERACT LLC to the risk of non-compliance with various identity theft and privacy laws

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT. Non-sanctioned use of mobile devices to backup, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the GATHERACT LLC network.

Audience

This policy applies to all GATHERACT LLC employees, including full and part-time staff, Board of Directors, volunteers, contractors, freelancers, and other agents who utilize personally-owned mobile devices to access, store, back up, relocate, or access any organization or member-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust GATHERACT LLC has built with its members, suppliers, and other constituents. Consequently, employment at GATHERACT LLC does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

Policy Detail

This policy applies to:

- Any privately owned wireless and/or portable electronic handheld equipment, hereby referred to as BYOD. GATHERACT LLC grants potential participants of the BYOD program the privilege of purchasing and using a device of their choosing at work for their convenience.

- Related software that could be used to access corporate resources.

This policy is intended to protect the security and integrity of GATHERACT LLC's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

The Audience, as defined above, must agree to the terms and conditions set forth in this policy to be able to connect their devices to the company network. If users do not abide by this policy, GATHERACT LLC reserves the right to revoke this privilege.

The following criteria will be considered initially, and on a continuing basis, to determine if the Audience is eligible to connect a personal smart device to the GATHERACT LLC network.

- Management's written permission and certification of the need and efficacy of BYOD for that Employee
- Sensitivity of data the Audience can access
- Legislation or regulations prohibiting or limiting the use of a personal smart device for GATHERACT LLC business
- Must be listed on the Information Technology Department's list of approved mobile devices
- Audience's adherence to the terms of the Bring Your Own Device Agreement and this policy and other applicable policies
- Technical limitations
- Other eligibility criteria deemed relevant by GATHERACT LLC or IT

Responsibilities of GATHERACT LLC

- IT will centrally manage the BYOD program and devices including, but not limited to, onboarding approved users, monitoring BYOD connections, and terminating BYOD connections to company resources upon the users leave of employment or service to GATHERACT LLC.
- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable.
- IT reserves the right to refuse, by non-physical means, the ability to connect mobile devices to GATHERACT LLC and GATHERACT LLC-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts GATHERACT LLC's systems, data, users, and members at risk.
- IT will maintain a list of approved mobile devices and related software applications and utilities. Devices that are not on this list may not be connected to the GATHERACT LLC infrastructure. To find out if a preferred device is on this list, an individual should contact the GATHERACT LLC IT department Service Desk. Although IT currently allows only listed devices to be connected to the GATHERACT LLC infrastructure, IT reserves the right to update this list in the future.
- IT will maintain enterprise IT security standards.
- IT will inspect all mobile devices attempting to connect to the GATHERACT LLC network through an unmanaged network (i.e. the Internet) using technology centrally managed by the IT Department.
- IT will install the Mobile VPN software required on Smart mobile devices, such as

Smartphones, to access the GATHERACT LLC network and data.

GATHERACT LLC's IT Department reserves the right to:

- Install anti-virus software on any BYOD participating device
- Restrict applications
- Limit use of network resources
- Wipe data on lost/damaged devices or upon termination from the BYOD program or GATHERACT LLC employment
- Properly perform job provisioning and configuration of BYOD participating equipment before connecting to the network
- Through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the GATHERACT LLC network

Responsibilities of BYOD Participants

Security and Damages

- All potential participants will be granted access to the GATHERACT LLC network on the condition that they read, sign, respect, and adhere to the
- GATHERACT LLC policies concerning the use of these devices and services (see Exhibit A).
- Prior to initial use on the GATHERACT LLC network or related infrastructure, **all personally owned mobile devices must be registered with IT.**
- Participants of the BYOD program and related software for network and data access **will**, without exception:
    - Use secure data management procedures. All BYOD equipment, containing stored data owned by GATHERACT LLC, must use an approved method of encryption during transmission to protect data.
    - Be expected to adhere to the same security protocols when connected with approved BYOD equipment to protect GATHERACT LLC's infrastructure.
    - GATHERACT LLC data is not to be accessed on any hardware that fails to meet GATHERACT LLC's established enterprise IT security standards.
    - Ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied to BYOD use.
    - Utilize a device lock with authentication, such as a fingerprint or strong password, on each participating device**.** Refer to the GATHERACT LLC password policy for additional information.
    - Employees agree to never disclose their passwords to anyone, particularly to family members, if business work is conducted from home.
    - Passwords and confidential data should not be stored on unapproved or unauthorized non-GATHERACT LLC devices.
    - Exercise reasonable physical security measures. It is the end

users responsibility to keep their approved BYOD equipment safe and secure.

- A device's firmware/operating system **must** be up-to-date in order to prevent vulnerabilities and make the device more stable. The patching and updating processes are the responsibility of the owner.
- Any non-corporate computers used to synchronize with BYOD equipment will have installed anti-virus and anti-malware software deemed necessary by GATHERACT LLC's IT Department. Anti-virus signature files must be up to date on any additional client machines – such as a home PC – on which this media will be accessed.
- IT can and will establish audit trails and these will be accessed, published, and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse.
- **If A) any BYOD device is lost or stolen, immediately contact GATHERACT LLC IT**; **and, if B) any BYOD device is scheduled to be upgraded or exchanged, the user must contact IT in advance.** IT will disable the BYOD and delete associated company data.
- BYOD equipment that is used to conduct GATHERACT LLC business will be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's access.
- Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with GATHERACT LLC's overarching security policy.
- Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace.
- The user agrees to and accepts that his or her access and/or connection to GATHERACT LLC's networks may be monitored to record dates, times, duration of access, etc. This is done to identify unusual usage patterns or other suspicious activity, and to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains GATHERACT LLC's highest priority.
- Employees, Board of Directors, volunteers, contractors, and temporary staff will not reconfigure mobile devices with any type of GATHERACT LLC owned and installed hardware or software without the express approval of GATHERACT LLC's IT Department.
- The **end user agrees to immediately report,** to his/her manager and GATHERACT LLC's IT Department, **any incident or suspected incidents of unauthorized data access,** data loss, and/or disclosure of GATHERACT LLC resources, databases, networks, etc.

Third Party Vendors

Third party vendors are expected to secure all devices with up-to-date anti-virus signature files and anti-malware software relevant or applicable to a device or platform. All new connection requests between third parties and GATHERACT LLC require that the third party and GATHERACT LLC representatives agree to and sign the Third Party Agreement. This agreement must be signed by the Vice President of the sponsoring department, as well as a representative from the third party who is legally empowered to sign on behalf of the third party. By signing this agreement, the third party agrees to abide by all referenced policies. The document is to be kept on file. All non-publicly accessible information is the sole property of GATHERACT LLC.

The IT Department can supply a non-GATHERACT LLC Internet connection utilizing a US Cellular hot spot if needed.

Help and Support

GATHERACT LLC's IT Department is not accountable for conflicts or problems caused by using unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department.

Organizational Protocol

GATHERACT LLC may offer a reimbursement of expenses to employees if they choose to use their own mobile devices in lieu of accepting a GATHERACT LLC-issued device. This may vary on the employees' function within the company and will be in accordance with a schedule in the associated procedure. Refer to the Company and Personally Owned Mobile Device Procedure.

EXHIBIT A

Bring Your Own Device (BYOD) Agreement

This Bring Your Own Device Agreement is entered into between the User and GATHERACT LLC, effective the date this agreement is executed by GATHERACT LLC's Information Technology Department (IT). The parties agree as follows:

ELIGIBILITY

The use of a supported smart device owned by the User in connection with GATHERACT LLC business is a privilege granted to the User, by management approval, per the Personal Device Acceptable Use and Security Policy. A supported smart device is defined as an Android- or IOS-based cell phone or tablet running a manufacturer's supported version of its operating system. If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to GATHERACT LLC and to ensure the data remains secure.

In the event of a security breach or threat, GATHERACT LLC reserves the right, without prior notice to the User, to disable or disconnect some or all BYOD services related to connection of a personal smart device to the GATHERACT LLC network.

REIMBURSEMENT CONSIDERATIONS

GATHERACT LLC offers a fixed reimbursement to eligible Users starting the month following BYOD enrollment. Reference the Company and Personally Owned Mobile Device Procedure, Appendix B for the reimbursement schedule. The User is personally liable for the device and carrier service. Accordingly, GATHERACT LLC will NOT reimburse the User, over and above the monthly reimbursement, for any loss, cost, or expense associated with the use or connection of a personal smart device to the GATHERACT LLC network. This includes, but is not limited to, expenses for voice minutes used to perform GATHERACT LLC business, data charges related to the use of GATHERACT LLC services, expenses related to text or other messaging, cost of handheld devices, components, parts, or data plans, cost of replacement handheld devices in case of malfunction whether or not the malfunction was caused by using applications or services sponsored or provided by GATHERACT LLC, loss related to unavailability of, disconnection from, or disabling the connection of a smart device to the GATHERACT LLC network, and loss resulting from compliance with this Agreement or applicable GATHERACT LLC policies.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following GATHERACT LLC policies, published elsewhere and made available, is mandatory: Acceptable Use of Information Systems, Personal Device Acceptable Use and Security, and other related policies including, but not limited to, Anti-Virus, E-Mail, Network Security, Password, Safeguarding Member Information, Telecommuting.

The User of the personal smart device shall not remove sensitive information from the GATHERACT LLC network, attack GATHERACT LLC assets, or violate any of the security policies related to the subject matter of this Agreement.

SUPPORT

GATHERACT LLC will offer the following support for the personal smart device: connectivity to GATHERACT LLC servers, including email and calendar, and security services, including policy management, password management, and decommissioning and/or remote wiping in case of loss, theft, device failure, device degradation, upgrade (trade-in), or change of ownership. GATHERACT LLC is not able to provide any additional assistance on any personally owned device and is not responsible for carrier network or system outages that result in a failure of connectivity to the GATHERACT LLC network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the GATHERACT LLC network, programming and other errors, bugs, viruses, and other software or hardware failures resulting in the partial or complete loss of data or which render the smart device inoperable.

DISCLAIMER

GATHERACT LLC expressly disclaims, and the User releases GATHERACT LLC from, all liability for any loss, cost, or expense of any nature whatsoever sustained by the User in connection with the privilege afforded the User under the terms of the Agreement.

____ ________________

User **Date**

____ ________________

IT Department Management **Date**

Rev. 2015-08

Policy 17: Password

Definitions

Application Administration Account: *Any account that is for the administration of an application (i.e. SQL database administrator, etc.).*

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant or deny access to private or shared data.

Strong Password: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically, the longer the password, the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about the password owner such as a birth date, social security number, and so on.

Two Factor Authentication: Two-factor authentication (2FA) is a security system that requires two distinct forms of identification in order to access something. Two-factor authentication can be used to strengthen the security of an online account. 2FA does this by requiring two types of information from the user—a password or personal identification number (PIN), a code sent to the user's smartphone, or a fingerprint—before whatever is being secured can be accessed.

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of GATHERACT LLC's entire corporate network. As such, all GATHERACT LLC employees or volunteers/directors (including contractors and vendors with access to GATHERACT LLC systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

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

Audience

This policy applies to all personnel or volunteers/directors who have, or are responsible for, an account (or any form of access that supports or requires a password) on any system that resides at any GATHERACT LLC facility, has access to the GATHERACT LLC network, or stores any non-public GATHERACT LLC information.

Policy Detail

User Network Passwords

Passwords for GATHERACT LLC network access must be implemented according to the following guidelines:

- Passwords must adhere to a minimum length of 8 characters
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#$%^&*_+=?/~’;’,<>|\).
- Passwords must not be easily tied back to the account owner such as: username, social security number, nickname, relative’s names, birth date, etc. • Passwords must not be dictionary words or acronyms
- Passwords cannot be reused for 1 year
- Passwords must be further protected by two factor authentication when a 2FA service is made available. GATHERACT LLC will provide this service for all company email accounts at a minimum.

System-Level Passwords

All system-level passwords must adhere to the following guidelines:

- All administrator accounts must have 10 character passwords which must contain three of the four items: upper case, lower case, numbers, and special characters.
- Non-expiring passwords must be documented listing the requirements for those accounts. These accounts need to adhere to the same standards as administrator accounts.
- Administrators must not circumvent the Password Policy for the sake of ease of use

Password Protection

- The same password **must not** be used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential GATHERACT LLC information.
- Stored passwords must be encrypted.
- Passwords must not be inserted in e-mail messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Passwords must not be revealed on questionnaires or security forms.
- Users must not hint at the format of a password (for example, “my family name”).
- GATHERACT LLC passwords must not be shared with anyone, including co-workers, managers, or family members, while on vacation.
- Passwords must not be written down and stored anywhere in any office. Passwords must not be stored in a file on a computer system or mobile device (phone, tablet) without encryption.
- If the security of an account is in question, the password must be changed immediately. In the event passwords are found or discovered, the following steps must be taken:
    - Take control of the passwords and protect them
    - Report the discovery to IT
- Users cannot circumvent password entry with an auto logon, application remembering, embedded scripts, or hard coded passwords in client software. Exceptions may be made for specific applications (like automated backup

processes) with the approval of IT. For an exception to be approved, there must be a procedure to change the passwords.

- PCs must not be left unattended without enabling a password-protected screensaver or logging off the device.
- Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with GATHERACT LLC.

Application Development Standards

Application developers must ensure their programs follow security precautions in this policy and industry standards.

Policy 18: Patch Management

Overview

Patch Management at GATHERACT LLC is required to mitigate risk to the confidential data and the integrity of GATHERACT LLC's systems. Patch management is an effective tool used to protect against vulnerabilities, a process that must be done routinely, and should be as all-encompassing as possible to be most effective. GATHERACT LLC must prioritize its assets and protect the most critical ones first; however, it is important to ensure patching takes place on all machines.

Purpose

Security vulnerabilities are inherent in computing systems and applications. These flaws allow the development and propagation of malicious software, which can disrupt normal business operations, in addition to placing GATHERACT LLC at risk. In order to effectively mitigate this risk, software “patches” are made available to remove a given security vulnerability.

Given the number of computer workstations and servers that comprise the GATHERACT LLC network, it is necessary to utilize a comprehensive patch management solution that can effectively distribute security patches when they are made available. Effective security is
a team effort involving the participation and support of every GATHERACT LLC employee and the Board of Directors.

This policy is to assist in providing direction, establishing goals, enforcing governance, and to outline compliance.

Audience

This policy applies to all employees, contractors, consultants, temporaries, and the Board of Directors at GATHERACT LLC. This policy applies to all equipment that is owned or leased by GATHERACT LLC, such as, all electronic devices, servers, application software, computers, peripherals, routers, and switches.

Adherence to this policy is mandatory.

Policy Detail

Many computer operating systems, such as Microsoft Windows, Linux, and others, include software application programs which may contain security flaws.

Occasionally, one of those flaws permits a hacker to compromise a computer. A compromised computer threatens the integrity of the GATHERACT LLC network, and all computers connected to it. Almost all operating systems and many software applications have periodic security patches, released by the vendor, that need to be applied. Patches, which are security related or critical in nature, should be installed as soon as possible.

- In the event that a critical or security related patch cannot be centrally deployed by IT, it must be installed in a timely manner using the best resources available.

- Failure to properly configure new workstations is a violation of this policy. Disabling, circumventing, or tampering with patch management protections and/or software constitutes a violation of policy.

Responsibility

The VP of IT is responsible for providing a secure network environment for GATHERACT LLC. It is GATHERACT LLC's policy to ensure all computer devices (including servers, desktops, printers, etc.) connected to GATHERACT LLC's network, have the most recent operating system, security, and application patches installed.

Every user, both individually and within the organization, is responsible for ensuring prudent and responsible use of computing and network resources.

IT is responsible for ensuring all known and reasonable defenses are in place to reduce network vulnerabilities, while keeping the network operating.

IT Management and Administrators are responsible for monitoring security mailing lists, reviewing vendor notifications and Web sites, and researching specific public Web sites for the release of new patches. Monitoring will include, but not be limited to:

- Scheduled third party scanning of GATHERACT LLC's network to identify known vulnerabilities

- Identifying and communicating identified vulnerabilities and/or security breaches to GATHERACT LLC's VP of IT

- Monitoring Computer Emergency Readiness Team (CERT), notifications, and Web sites of all vendors that have hardware or software operating on GATHERACT LLC's network

The IT Security and System Administrators are responsible for maintaining accuracy of patching procedures which detail the what, where, when, and how to eliminate confusion, establish routine, provide guidance, and enable practices to be auditable.

Documenting the implementation details provides the specifics of the patching process, which includes specific systems or groups of systems and the timeframes associated with patching.

Once alerted to a new patch, IT Administrators will download and review the new patch. The patch will be categorized by criticality to assess the impact and determine the installation schedule.

Policy 19: Physical Access Control

Definitions

Information systems: Is any combination of information technology and individuals' activities using that technology, to support operations management.

Display mechanisms: A monitor on which to view output from an information system.

Overview

Physical access controls define who is allowed physical access to GATHERACT LLC facilities that house information systems, to the information systems within those facilities, and/or the display mechanisms associated with those information systems. Without physical access controls, the potential exists that information systems could be illegitimately, physically accessed and the security of the information they house could be compromised.

Purpose

This policy applies to all facilities of GATHERACT LLC, within which information systems or information system components are housed. Specifically, it includes:

- Data centers or other facilities for which the primary purpose is the housing of IT infrastructure
- Data rooms or other facilities, within shared purpose facilities, for which one of the primary purposes is the housing of IT infrastructure
- Switch and wiring closets or other facilities, for which the primary purpose is not the housing of IT infrastructure

Policy Detail

Access to facilities, information systems, and information system display mechanisms will be limited to authorized personnel only. Authorization will be demonstrated with authorization credentials (badges, identity cards, etc.) that have been issued by GATHERACT LLC.

Access to facilities will be controlled at defined access points with the use of card readers and locked doors. Before physical access to facilities, information systems, or information system display mechanisms is allowed, authorized personnel are required to authenticate themselves at these access points. The delivery and removal of information systems will also be controlled at these access points. No equipment will be allowed to enter or leave the facility, without prior authorization, and all deliveries and removals will be logged.

A list of authorized personnel will be established and maintained so that newly authorized personnel are immediately appended to the list and those personnel who have lost authorization are immediately removed from the list. This list shall be reviewed and, where necessary, updated on at least an annual basis.

If visitors need access to the facilities that house information systems or to the information systems themselves, those visitors must have prior authorization, must be positively identified, and must have their authorization verified before physical access is granted. Once access has been granted, visitors must be escorted, and their activities monitored at all times.

Policy 20: Cloud Computing Adoption

Definitions

Cloud computing: *Is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction.*

Public cloud: Is based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

Private Cloud: Is based on the standard cloud computing model but uses a proprietary architecture at an organization's in-house facilities or uses an infrastructure dedicated to a single organization.

Financial information: Is any data for GATHERACT LLC, its employees, members, or other third
parties.

Intellectual property: Is any data that is owned by GATHERACT LLC or provided by a third party that would not be distributed to the public.

Other non-public data or information: Are assets deemed the property of GATHERACT LLC.

Other public data or information: Are assets deemed the property of GATHERACT LLC.

Personally Identifiable Information (PII): Is any data that contains personally identifiable information concerning any members, employees, or other third parties.

Overview

Cloud computing would allow GATHERACT LLC to take advantage of technologies for storing and/or sharing documents and other files, and virtual on-demand computing resources. Cloud computing can be beneficial in reducing cost and providing flexibility and scalability.

Purpose

The purpose of this policy is to ensure that GATHERACT LLC can potentially make appropriate cloud adoption decisions and at the same time does not use, or allow the use of, inappropriate cloud service practices. Acceptable and unacceptable cloud adoption examples are listed in this policy. All other cloud use cases are approved on a case-by-case basis.

Policy Detail

It is the policy of GATHERACT LLC to protect the confidentiality, security, and integrity of each member's non-public personal information. GATHERACT LLC will take responsibility for its use of cloud computing services to maintain situational awareness, weigh alternatives, set priorities, and effect changes in security and privacy that are in the best

Policy 22: Encryption Key Management Procedures

Definitions

Cryptographic Key: *Is defined as a complex string of characters that are used to encrypt and decrypt data.*

Overview

Encryption Key Management encompasses the policies and practices used to protect encryption keys against modification and unauthorized disclosure or export outside the United States. Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys used to secure sensitive data and hence, compromise of the data. While users may understand it's important to encryption certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys.

Purpose

This policy outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

Policy Detail

- State agencies shall control centrally stored keys and system software, even when developed or maintained by a contractor. State agencies shall also control the configuring of the key management hardware and software.
- Key management responsibility may only be delegated to a party who has passed a background check and signed a confidentiality agreement.
- Encryption systems shall be designed such that no single person has full knowledge of any single encryption key. This is achieved by separation of duties (use of more

than one individual to handle a certain important activity) and dual control (two people shall be simultaneously present for an important activity to be accomplished).

- Users shall be trained to keep their encryption keys secure and shall be made aware of their liabilities and responsibilities.

Generation

- Encryption algorithms used to protect production information and information systems shall adhere to industry standards.
- Each individual key record shall be signed to enable tamper detection.
- Encryption keys shall be generated by means which are not practically discernible by an adversary.
- Materials to develop encryption keys as well as the keys themselves shall be kept secured when not in use and throughout the life cycle of the information.

Distribution

- The information protected with encryption shall be transmitted over a different communication channel than the keys used to govern the encryption process.
- Private and secret encryption keys transmitted over communication lines shall be sent in encrypted form with one of the following key exchange algorithms:
    - RSA
    - Elliptic Curve
    - Diffie-Hellman

Storage

- Access to encryption keys shall be strictly limited to those who have a need-to-know.
- Encryption keys shall be prevented from unauthorized disclosure via technical controls such as encryption under a separate key and use of tamper-resistant hardware.
- Encryption or split knowledge and dual control shall be used to protect centrally stored user secret keys, private keys, master keys, to secure the distribution of user tokens, and to initialize all crypto-modules.
- If a key is stored on a token and a PIN is used to access the token, then only that token's owner shall have possession of both the token and its corresponding PIN. The token and its PIN shall be distributed via separate secure mailings.
- Software at the central key management site shall be electronically signed and periodically verified to check the integrity of the code.
- All centrally stored data that is related to user keys shall be signed for integrity, and encrypted or use dual control and split knowledge for confidentiality.
- Automated resources that generate keys and initialization vectors require layered physical protection to prevent disclosure, modification or

replacement by those without a need to know.

- Backup copies shall be made of central/root keys and stored offsite.
- Encryption keys and the data they protect shall be stored on separate physical media.
- Automatic backup systems shall not copy the readable version of private keys used for digital signatures and digital certificates. Readable backups are prevented by keeping private keys in smart cards or in encrypted form.
- Encryption keys used to conceal backup data shall themselves be backed-up. These keys shall also be stored with security measures comparable to or more stringent than measures applied to the backed-up data.
- All encryption processes running on production information systems shall include key recovery functions. Key escrow allows management to recover encrypted information should there be system errors, human errors, or other problems.
- Keys used for digital signatures, digital certificates, and user authentication shall not be included in a key escrow arrangement with a third party.

Life Cycle

- The crypto-period (the time a key can be used for signature verification or decryption) shall be determined based on the sensitivity of the information and the risk of key compromise.
- All encryption keys shall have a stated life and shall be changed on or before the stated expiration date.
- Key lifetime (the time during which a key can be used to generate a signature or perform encryption) is dependent upon the user's roles, responsibilities, the applications used, and the security services provided by the key.
- Reissuing keys shall be performed often enough to minimize the loss caused by compromise, but not so often that it becomes a burden.
- The secrecy of any encryption key used for confidentiality purposes shall be maintained until all the protected information is no longer considered confidential.
- Private digital signature keys shall be kept confidential and accessible for at least the number of years that they might be used in a legal challenge.
- All supplies used for the generation, distribution, and storage of keys shall be protected from disclosure to unauthorized persons. When they are no longer needed, they shall be destroyed by pulping, shredding, burning, or other approved methods.

Key Change or Compromise

- State agencies shall have a plan for handling the compromise or suspected compromise of central/root keys or key components at a central site before the system goes live. This includes key recovery capabilities for terminated users.
- Encryption keys that have been compromised shall immediately be revoked retroactively to the last known time when the keys were safe.

- Key management systems shall be capable of designating a key as “lost” or “compromised”, so that signatures generated prior to a specified date can still be verified.
- If a public encryption key has been posted on a publicly accessible location, all regular correspondents shall be notified whenever there is a change in the public key.

Export

- The U.S Government controls the export of cryptographic implementations. For the current rules, refer to Title 15 of the Code of Federal Regulations.
- "Mass market" encryption commodities and software with symmetric key lengths exceeding 64-bits may be exported following a 30-day review by the U.S. Department of Commerce.

Policy 23: Security Awareness Training

Overview

Security and privacy awareness and training is an important aspect in protecting the Confidentiality, Integrity, and Availability (CIA) of sensitive information. Employees are the first line of defense and must be made aware of the security risks associated with the work performed at GATHERACT LLC.

Purpose

GATHERACT LLC understands that people are often the biggest threat (intentionally or inadvertently) to the security of sensitive information. As such, all users of information systems must be made aware of the security risks associated with their activities and of the applicable federal and agency requirements related to the security of Strategic information systems performing work on behalf of the Centers for Medicare and Medicaid Services (CMS). Those with significant security responsibilities must be adequately trained to carry out their assigned information security-related duties and responsibilities.

Scope

This policy applies to all GATHERACT LLC employees and contractors and anyone else needing access to GATHERACT LLC information and its systems.

Policy Detail

All employees, contractors, and anyone accessing GATHERACT LLC information systems must understand how to protect the CIA of information and information systems.

GATHERACT LLC will ensure that all employees and contractors are given security and privacy awareness training during the new hire process and before accessing any GATHERACT LLC systems. This training reflects common security and privacy awareness specific to GATHERACT LLC's environment including, but not limited to, physical access, restricted areas, potential incidents, how to report incidents, laptop best practices, and how to spot a phishing scam.

In addition to the initial security training provided in the new hire orientation, all employees must take a security and privacy awareness course and pass the post-test within 30 days of hire. This course and test is provided and tracked by the Learning Management System (LMS). In some cases, it may be necessary to administer an in-person training, not through an LMS. In these instances, https://www.cdse.edu/catalog/cybersecurity.html will be used to deliver a live training by an instructor along with a live verbal examination. The instructor will keep records of student success.

GATHERACT LLC will provide ongoing training through the Security and Privacy Awareness and Training (SPAT) Team activities. The SPAT provides information on a monthly basis on selected topics. An initial SPAT Chat presentation is conducted at the beginning of the month to give information, demonstrations, and general Q&A for all attendees. The SPAT also provides information via posters in designated areas throughout the facility and weekly articles posted on the internal intranet page.

GATHERACT LLC will also conduct annual refresher training for all employees and anytime there are significant changes to the environment. This will be administered via the LMS and tracked for completeness and passing grade to show adequate understanding of the material.

This policy will be reviewed on an annual basis or whenever there are significant changes to the environment.

Management Commitment

GATHERACT LLC Senior Management will commit to the development of a security and privacy awareness program allocating staff and resources. The Information Security Manager will have access to both the compliance and training departments for completion and update of training materials and tracking results.

Roles and Responsibilities

All employees and contractors are responsible for understanding and following all security related policies and procedures, and asking their manager or Security Officer for clarification if needed.

Managers are responsible for ensuring all employees complete required security training.

The LMS Administrator is responsible for enrolling all employees in first-time and annual security training and tracking results.

The Security Manager is responsible for:

- Maintaining ongoing SPAT team activities
- Updating annual security training materials
- Conducting new hire training
- Ensuring all employees understand and following security related policies and procedures

Coordination Among Organizational Entities

Security is everybody’s business. As security tends to cross departmental and organizational boundaries, GATHERACT LLC employees and contractors will work together to ensure that required security controls are in place, are maintained, and comply with the policy described in this document. Security concerns, security incidents, or suspected/confirmed vulnerabilities will be shared with appropriate personnel in the organization so that the vulnerability can be remediated (or mitigated with compensating security controls) and we can ensure that similar vulnerabilities in other systems or processes can be addressed.

Compliance

Compliance with the policy defined in this document is mandatory. Failure to comply with GATHERACT LLC Information Security Policies may result in disciplinary actions up to and including termination of employment. Employees may also be held personally liable for any violations of this policy. Failure to comply with GATHERACT LLC Information Security Policies may result in termination of contracts for contractors, partners, consultants, and other entities. Legal actions may also be taken for violations of applicable regulations and laws. Systems that do not satisfy GATHERACT LLC Information Security Policy requirements may be prevented from being allowed to operate as a production system.

Security Awareness (AT-2)

GATHERACT LLC requires that all users complete a security awareness and training course (or courses as applicable) prior to being granted access to GATHERACT LLC corporate or client systems. Users are provided basic security awareness training as part of initial training for new users, as well as when required by system changes. All users must take refresher training at least annually. Employees or contractors shall acknowledge having received the security awareness training either in writing or electronically as part of the training course completion (the current process involves sending copies of course completion certificates to the GATHERACT LLC CISO). The GATHERACT LLC CISO maintains and stores completed security awareness and training evidence artifacts (certificates) for users. Security awareness and training course completion artifacts (certificates) will be provided to the Agency ISSO or Security Steward upon request.

Security Training (AT-3)

GATHERACT LLC must provide role-based, security-related training before authorizing access to the system or performing assigned duties, as well as when required by a system change or changes in personnel roles.

GATHERACT LLC must provide security training materials that address the procedures and activities necessary to fulfill the defined roles and responsibilities for information system security. GATHERACT LLC must provide role-based security-related training to all appropriate personnel at least once every three years. Appropriate personnel includes but is not limited to System

Administrators, Database Administrators, Network Engineers, Security Analysts, and the CISO. The employee or consultant shall acknowledge having received the role-based training either in writing or electronically as part of the training course completion.

Security Training Records (AT-4)

GATHERACT LLC must create and disseminate to users the security training documents. The GATHERACT LLC CISO must ensure activities for monitoring and documenting basic security awareness training, as well as role-based training, are conducted. Employees and contractors must provide evidence of successful course completion (certificates) to the GATHERACT LLC CISO. All security training records must be stored for at least 5 years.

Policy 24: Change Management/Control

Overview

Being organized and disciplined about changes to GATHERACT LLC systems and software is an important part of the quality of our products and services. Have a clear policy for change management and control is a valuable tool for this.

Purpose

The purpose of the GATHERACT LLC Change Management/Control Policy is to establish the rules for the creation, evaluation, implementation, and tracking of changes made to GATHERACT LLC Information Resources.

Scope

This policy applies to any individual, entity, or process that creates, evaluates, and/or implements changes to GATHERACT LLC Information Resources.

Policy Detail

- Changes to production GATHERACT LLC Information Resources must be documented and classified according to their:
  - Importance,
  - Urgency,
  - Impact, and
  - Complexity
- Change documentation must include, at a minimum:
  - Date of submission and date of change,
  - Owner and custodian contact information,
  - Nature of the change,
  - Change requestor,
  - Change classification(s),
  - Roll-back plan,
  - Change approver,
  - Change implementer, and
  - An indication of success or failure.
- Changes with a significant potential impact to GATHERACT LLC Information Resources must be scheduled.
- GATHERACT LLC Information Resource owners must be notified of changes that affect the systems they are responsible for.
- Authorized change windows must be established for changes with a high potential impact.
- Changes with a significant potential impact and/or significant complexity must have usability, security, and impact testing and back out plans included in the change documentation.

- Change control documentation must be maintained in accordance with the GATHERACT LLC Data Retention Policy.
- Changes made to GATHERACT LLC customer environments and/or applications must be communicated to customers, in accordance with governing agreements and/or contracts.
- All changes must be approved by the Information Resource Owner, Director of Information Technology, or Change Control Board (if one is established).
- Emergency changes (i.e. break/fix, incident response, etc.) may be implemented immediately and complete the change control process retroactively.

Waivers

Waivers from certain policy provisions may be sought following the (Company) Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Policy 25: Data Retention Policy

Overview

GATHERACT LLC seeks to ensure that it retains only data necessary to effectively conduct its program activities and work in fulfillment of its mission. The need to retain data varies widely with the type of data and the purpose for which it was collected. GATHERACT LLC strives to ensure that data is only retained for the period necessary to fulfil the purpose for which it was collected, and is fully deleted when no longer required.

Purpose

This policy sets forth guidelines on data retention and is to be consistently applied throughout the organization.

Scope

This policy covers all data collected by GATHERACT LLC and stored on GATHERACT LLC owned or leased systems and media, regardless of location. It applies to both data collected and held electronically (including photographs, video and audio recordings) and data that is collected and held as hard copy or paper files. The need to retain certain information may be mandated by federal or local law, federal regulations and legitimate business purposes, as well as the EU General Data Protection Regulation (GDPR) when applicable.

Policy Detail

Reasons for Data Retention

GATHERACT LLC retains only that data that is necessary to effectively conduct its program activities, fulfill its mission and comply with applicable laws and regulations.

Reasons for data retention include:

- Providing an ongoing service to the data subject (e.g. sending a newsletter, publication or ongoing program updates to an individual, ongoing training or participation in GATHERACT LLC's programs, processing of employee payroll and other benefits)
- Compliance with applicable laws and regulations associated with financial and programmatic reporting by GATHERACT LLC to its funding agencies and other donors
- Compliance with applicable labor, tax and immigration laws
- Other regulatory requirements
- Security incident or other investigation
- Intellectual property preservation
- Litigation

Data Duplication

GATHERACT LLC seeks to avoid duplication in data storage whenever possible, though there may be instances in which for programmatic or other business reasons it is necessary for data to be held in more than one place. This policy applies to all data in GATHERACT LLC's possession, including duplicate copies of data.

Retention Requirements

GATHERACT LLC has set the following guidelines for retaining all personal data as defined in the company's data privacy policy.

- Website visitor data, when collected, will be retained as long as necessary to provide the service requested/initiated through the GATHERACT LLC owned websites.
- Contributor data will be retained for the year in which the individual has contributed, and then for 5 years after the date of the last contribution.
- Financial information will not be retained longer than is necessary to process a single transaction.
- Event participant data will be retained for the period of the event, including any follow-up activities, such as the distribution of reports, plus a period of 1 month;
- Program participant data (including sign in sheets) will be retained for the duration of the grant agreement that financed the program plus any additional time required under the terms of the grant agreement.
- Personal data of subgrantees, subcontractors and vendors will be kept for the duration of the contract or agreement.
- Employee data will be held for the duration of employment and then 1 year after the last day of employment.
- Data associated with employee wages, leave and pension shall be held for the period of employment plus 1 year, with the exception of pension eligibility and retirement beneficiary data which shall be kept for 10 years.
- Recruitment data, including interview notes of unsuccessful applicants, will be held for 1 year after the closing of the position recruitment process.
- Consultant (both paid and pro bono) data will be held for the duration of the consulting contract plus 1 year after the end of the consultancy.
- Board member data will be held for the duration of service on the Board plus for 1 year after the end of the member's term.
- Data associated with tax payments (including payroll, corporate and VAT) will be held for 5 years.
- Operational data related to program proposals, reporting and program management will be held for the period required by the GATHERACT LLC donor, but not more than 2 years.

Data Destruction

Data destruction ensures that GATHERACT LLC manages the data it controls and processes it in an efficient and responsible manner. When the retention period for the data as outlined above expires, GATHERACT LLC will actively destroy the data covered by this policy. If an individual believes that there exists a legitimate business reason why certain data should not be destroyed at the end of a retention period, he or she should identify this data to his/her supervisor and provide information as to why the data should not be destroyed. Any exceptions to this data retention policy must be approved by GATHERACT LLC's data protection offer in consultation with legal counsel. In rare circumstances, a litigation hold may be issued by legal counsel prohibiting the destruction of certain documents. A litigation hold remains in effect until released by legal counsel and prohibits the destruction of data subject to the hold.