Comprehensive IT Policy

PurpleSec LLC

Introduction

Information Technology (IT) is an integral and critical component of PurpleSec LLC's (PURPLESEC) daily business. This policy seeks to ensure that PURPLESEC's IT resources efficiently serve the primary business functions of PURPLESEC, provide security for PURPLESEC 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 PURPLESEC's business.

All computer equipment, peripherals, and software are PURPLESEC 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 PURPLESEC computers will result in corrective action up to and including termination. Employees should also be aware that any work completed on PURPLESEC 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 PurpleSec LLC. The following Policy Statement, Disciplinary Action, and Review paragraphs apply to all individual policies contained within this Comprehensive IT policy.

Policy Statement

It is the policy of PurpleSec 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 PURPLESEC'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 PURPLESEC 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 PURPLESEC 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 PURPLESEC must be managed as valuable organization resources.

Information Technology's (IT) intentions are not to impose restrictions that are contrary to PURPLESEC's established culture of openness, trust, and integrity. IT is committed to protecting PURPLESEC'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 PURPLESEC. These systems are to be used for business purposes in serving the interests of PURPLESEC and of its clients and members during normal operations.

Effective security is a team effort involving the participation and support of every PURPLESEC 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 PURPLESEC. These rules are in place to protect the authorized user and PURPLESEC. Inappropriate use exposes PURPLESEC 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 PURPLESEC business or interacts with internal networks and business systems, whether owned or leased by PURPLESEC, the employee, or a third party.

All employees, volunteer/directors, contractors, consultants, temporaries, and other workers at PURPLESEC, 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 PURPLESEC policies and standards, local laws, and regulations.

Policy Detail

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

Privacy
Electronic files created, sent, received, or stored on PURPLESEC owned, leased, or administered equipment, or otherwise under the custody and control of PURPLESEC are not private and may be accessed by PURPLESEC 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 PURPLESEC. Because of the need to protect PURPLESEC's network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to PURPLESEC.

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

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

PURPLESEC'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: PURPLESEC 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 PURPLESEC 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 PURPLESEC 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.

PURPLESEC proprietary information stored on electronic and computing devices, whether owned or leased by PURPLESEC, the employee, or a third party, remains the sole property of PURPLESEC. 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 PURPLESEC proprietary information to their immediate supervisor and/or the IT Department.

All users must report any weaknesses in PURPLESEC 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 PURPLESEC 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 PURPLESEC may deem to be offensive, indecent, or obscene.

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

- 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 PURPLESEC 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 PURPLESEC 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 PURPLESEC 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 PURPLESEC IT.

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

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

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

- Purposely engaging in activity that may;
  - degrade the performance of information systems;
  - deprive an authorized PURPLESEC user access to a PURPLESEC resource;

  - obtain extra resources beyond those allocated; or
  - circumvent PURPLESEC 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, PURPLESEC users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non-approved programs on PURPLESEC information systems. The PURPLESEC 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 PURPLESEC-owned computer, must adhere to all the same policies that apply to use from within PURPLESEC facilities. Authorized users must not allow family members or other non-authorized users to access PURPLESEC computer systems.

PURPLESEC information systems must not be used for personal benefit.

Incidental Use

As a convenience to the PURPLESEC 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 PURPLESEC approved users; it does not extend to family members or other acquaintances.

- Incidental use must not result in direct costs to PURPLESEC 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, PURPLESEC.

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

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

Review and Acceptance
All PURPLESEC staff is responsible for review and acceptance of *Policy 1: Acceptable Use* upon starting work at PURPLESEC (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 PurpleSec 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 Comprehensive IT Policy. 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 Comprehensive IT Policy supersedes all policies previously issued. I also understand that PURPLESEC may supersede, change, eliminate, or add to any policies or practices described in the Comprehensive IT Policy.

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.

Acceptable Use Receipt_Rev 2019-01

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 PURPLESEC 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 PURPLESEC's information systems. These accounts provide a means of providing accountability, a key to any computer security program, for PURPLESEC 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 PURPLESEC.

Audience

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

Policy Detail

Accounts

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

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

- Shared accounts on PURPLESEC 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 PURPLESEC Password Policy.

- All accounts must have a password expiration that complies with the PURPLESEC 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 PURPLESEC 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 PURPLESEC’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 PURPLESEC 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 PURPLESEC 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 PURPLESEC 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 PURPLESEC network.

Policy Detail

All computer devices connected to the PURPLESEC 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 PURPLESEC network, must utilize PURPLESEC IT approved virus protection software and setup to detect and clean viruses that may infect PURPLESEC resources.

Each e-mail gateway must utilize PURPLESEC 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 PURPLESEC 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-PURPLESEC 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 PURPLESEC data can be saved to network drives and are backed up on a periodic basis. Contact the PURPLESEC IT Department for details.

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

Policy 4: PURPLESEC Owned Mobile Device Acceptable Use and Security /R

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 PURPLESEC owned mobile devices must be managed to ensure that employees, Board of Directors, and related constituents who use mobile devices to access PURPLESEC'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 PURPLESEC's direct control. This mobile device policy applies to, but is not limed to, any mobile device issued by PURPLESEC that contains stored data owned by PURPLESEC and all devices and accompanying media that fit the following device classifications:

- Laptops. Notebooks, and hybrid devices
- Tablets
- Mobile/cellular phones including smartphones
- Any PURPLESEC 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 PURPLESEC 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 PURPLESEC 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 PURPLESEC network.

Audience

This policy applies to all PURPLESEC 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 PURPLESEC has built with its members, suppliers, and other constituents. Consequently, employment at PURPLESEC 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 PURPLESEC'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 PURPLESEC's public image. Therefore, all users employing a PURPLESEC owned mobile device, connected to an unmanaged network outside of PURPLESEC'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 PURPLESEC's IT Department and will utilize authentication and strong encryption measures. To protect PURPLESEC's infrastructure, failure to adhere to these security protocols will result in immediate suspension of all network access privileges.

Responsibilities /R

It is the responsibility of any employee or Board Member of PURPLESEC, who uses a PURPLESEC 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 PURPLESEC owned mobile device that is used to conduct PURPLESEC 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:

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

at risk.

Prior to initial use on the PURPLESEC network or related infrastructure, **all mobile devices must be registered with IT.** PURPLESEC 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 PURPLESEC infrastructure. To find out if a preferred device is on this list, an individual should contact the PURPLESEC IT Department Service Desk. Although IT currently allows only listed devices to be connected to the PURPLESEC 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 PURPLESEC 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. PURPLESEC data is not to be accessed on any hardware that fails to meet PURPLESEC's established enterprise IT security standards.

All mobile devices attempting to connect to the PURPLESEC network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by PURPLESEC'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. PURPLESEC 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 PURPLESEC network and data using Mobile VPN software installed on the device by IT.

- **Security /R**
  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 PURPLESEC **must use an approved method of encryption** to protect data. Laptops must employ full drive encryption with an approved software encryption package. No PURPLESEC data may exist on a laptop in clear text. All mobile devices must be protected by a **strong password.** Refer to the PURPLESEC 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 PURPLESEC'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 PURPLESEC data. Users with devices that are not issued by PURPLESEC must adhere to the Personal Device Acceptable Use and Security Policy.

To ensure the security of PURPLESEC 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-PURPLESEC devices.

Any corporate owned mobile device that is being used to store PURPLESEC data must adhere to the authentication requirements of PURPLESEC’s IT Department. In addition, all hardware security configurations must be pre-approved by PURPLESEC’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 PURPLESEC’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 PURPLESEC 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. PURPLESEC shall employ remote wipe technology to remotely disable and delete any data stored on a PURPLESEC 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 PURPLESEC-owned and personal mobile devices being used within PURPLESEC’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). /**R**

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

- **Help and Support**

PURPLESEC'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 PURPLESEC owned and installed hardware or software without the express approval of PURPLESEC'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 PURPLESEC network.

- **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 PURPLESEC'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 PURPLESEC's highest priority.

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

  PURPLESEC 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.

  PURPLESEC 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 PURPLESEC resources, a mobile device user must understand and accept the terms and conditions of this policy.

EXHIBIT A

PURPLESEC Owned Mobile Device Agreement

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

ELIGIBILITY

The use of a PURPLESEC supported mobile device by the User for PURPLESEC business is a privilege granted to the User, by management approval, per the PURPLESEC 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 PURPLESEC and to ensure the data remains secure.

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

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following PURPLESEC policies, published elsewhere and made available, is mandatory: Acceptable Use of Information Systems, PURPLESEC 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 PURPLESEC owned mobile device shall not remove sensitive information from the PURPLESEC network, attack PURPLESEC assets, or violate any of the security policies related to the subject matter of this Agreement.

SUPPORT

PURPLESEC will offer the following support for the PURPLESEC owned mobile device: connectivity to PURPLESEC 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 PURPLESEC network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the PURPLESEC 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

PURPLESEC 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. PURPLESEC 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, PURPLESEC 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:
  - An individual's name
  - Social security number
  - Driver's license number or identification card number
  - 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:
  - Personal data, that refers to any combination of information that identifies and describes an individual.
  - Limited data, that refers to electronic information whose unauthorized access, modification, or loss could seriously or adversely affect PURPLESEC, 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 /R

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 PURPLESEC web site*
    - *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 PURPLESEC 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

PURPLESEC recognizes the importance of electronic commerce (e-commerce) activities to its present day operations. PURPLESEC 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 PURPLESEC's electronic services.

Policy Detail /R

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

Electronic commerce activities include PURPLESEC'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 PURPLESEC and its business partners using the Internet as the communications network.

It is the practice of PURPLESEC 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. PURPLESEC will use a minimum of 128b encryption. This also applies to vendors that host PURPLESEC 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**
  PURPLESEC 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 PURPLESEC 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 PURPLESEC'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, PURPLESEC 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 /R**
  Staff passwords, on the host data processing system, expire after 45 ~~or 90 days~~, forcing users to modify their passwords. This control, along with a strict PURPLESEC 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**
  PURPLESEC 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, PURPLESEC 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**
  PURPLESEC 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 PURPLESEC suspects or detects unauthorized individuals have gained access to member information systems, PURPLESEC will report such actions to appropriate regulatory and law enforcement agencies according to PURPLESEC's information security response procedures.

Policy 7: E-Mail /R

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 PURPLESEC 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 PURPLESEC email for sending, receiving, or storing of electronic mail.

Audience

This policy applies equally to all individuals granted access privileges to any PURPLESEC 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 /R

Corporate e-mail is not private. Users expressly waive any right of privacy in anything they create, store, send, or receive on PURPLESEC's computer systems. PURPLESEC 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 PURPLESEC, 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 PURPLESEC 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 PURPLESEC'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 PURPLESEC 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 PURPLESEC business.

- Sending excessively large messages or attachments.

- Knowingly sending or forwarding email with computer viruses.

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

All confidential or sensitive PURPLESEC material transmitted via e-mail, outside PURPLESEC'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 PURPLESEC network without encrypting the data.

All user activity on PURPLESEC information system assets is subject to logging and review. PURPLESEC 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 PURPLESEC, unless appropriately authorized (explicitly or implicitly) to do so.

Users must not send, forward, or receive confidential or sensitive PURPLESEC information through non-PURPLESEC email accounts. Examples of non-PURPLESEC 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-PURPLESEC issued mobile devices must adhere to the Personal Device Acceptable Use and Security Policy for sending, forwarding, receiving, or storing confidential or sensitive PURPLESEC information.

Incidental Use

Incidental personal use of sending e-mail is restricted to PURPLESEC 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 PURPLESEC.

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 PURPLESEC.

Storage of personal files and documents within PURPLESEC’s IT systems should be nominal.

E-mail Retention /R

- 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.

~~*E-mail Archive*~~

- ~~Only the owner of a mailbox and the system administrator has access to the archive.~~
- ~~Messages will be deleted from the online archive 36 months from the original send/receive date.~~

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

PURPLESEC operates network firewalls between the Internet and its private internal network to create a secure operating environment for PURPLESEC'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 PURPLESEC'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 PURPLESEC'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 PURPLESEC domain.

A change control process is required before any firewall rules are modified. Prior to implementation, the Third Party Vendor and PURPLESEC 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:

- PURPLESEC 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 PURPLESEC 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 PURPLESEC Password Policy.

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

PURPLESEC 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:
  - System errors
  - Blocked web sites
  - Attacks
- Sending alerts to the PURPLESEC 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 PURPLESEC, 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 PURPLESEC to ensure the proper disposition of all non-leased PURPLESEC 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

PURPLESEC 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. PURPLESEC'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 PURPLESEC'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 PURPLESEC'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 PURPLESEC'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 PURPLESEC'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 PURPLESEC is necessary to detect security incidents, determine the magnitude of the threat presented by these incidents, respond to these incidents, and if required, notify PURPLESEC members of the breach.

Purpose

This policy defines the requirement for reporting and responding to incidents related to PURPLESEC information systems and operations. Incident response provides PURPLESEC 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 PURPLESEC. 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, PURPLESEC 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**
  PURPLESEC 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 PURPLESEC 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:

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

- **Incident Response Testing**
  - At least once every year, the IT Department must utilize simulated incidents to mobilize and test the adequacy of response.
  - 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 PURPLESEC controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:

  - Preparation
  - Detection
  - Analysis
  - Containment
  - Eradication
  - Recovery
  - 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**
  PURPLESEC 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**
  PURPLESEC 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 PURPLESEC'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 PurpleSec 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 PURPLESEC 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 PURPLESEC.

- 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

  - Equifax:
    PO Box 740241
    Atlanta, GA 30374-0241

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

  - 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 PURPLESEC.
- 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 PurpleSec LLC at 608-755-6065 or 800-779-5555 for assistance and information related to this incident.

Sincerely,

PurpleSec LLC

Policy 11: Information Technology Purchasing

Overview

Information Technology purchasing at PURPLESEC 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 PURPLESEC funds.

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

Scope

The scope of this policy includes, but is not limited to, the following PURPLESEC 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 PURPLESEC funds are the property of PURPLESEC. 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 VP of IT. 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 PURPLESEC 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 PURPLESEC.

- **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 PURPLESEC Fixed Asset Policy, which are capitalized by PURPLESEC, 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 PURPLESEC assets, as defined below ("Qualified Assets" or "Asset"), procured or curated by the PURPLESEC 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 PURPLESEC 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.

PURPLESEC 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 /R

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 PURPLESEC 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 PURPLESEC Internet for access to the Internet or the Intranet.

Audience

This policy applies equally to all individuals granted access privileges to any PURPLESEC 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. PURPLESEC 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 PURPLESEC 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 PURPLESEC'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 PURPLESEC's network security, by accessing the Internet directly, is strictly prohibited.

Users are prohibited from using PURPLESEC 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 PURPLESEC's Internet access.

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

File downloads and virus protection /R

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 PURPLESEC 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 PURPLESEC IT assets is subject to logging and review. PURPLESEC 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

PURPLESEC 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 PURPLESEC PC is prohibited.

Users are prohibited from attempting to access or accessing inappropriate sites from any PURPLESEC 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.

PURPLESEC 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 PURPLESEC hosted web sites must comply with the PURPLESEC 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-PURPLESEC commercial advertising may be made available via hosted PURPLESEC web sites.

Transmissions

All sensitive PURPLESEC 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 PURPLESEC approved Users; it does not extend to family members or other acquaintances.

Incidental use must not result in direct costs to PURPLESEC.

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, PURPLESEC.

Storage of personal files and documents within PURPLESEC's IT should be nominal.

All files and documents, including personal files and documents, are owned by PURPLESEC, 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. 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 PURPLESEC 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. - PURPLESEC 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. PURPLESEC 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 PURPLESEC. While it is necessary for PURPLESEC 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 PURPLESEC’s information resources or the people who manage those resources, they are PURPLESEC Administrative Records, subject to the requirements of PURPLESEC 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 PURPLESEC to high costs of retrieving and reviewing the otherwise unneeded records in the event of litigation.

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 /R

Definitions

These terms are defined by the NCUA Part 748.

Member: *An individual who has an established, ongoing relationship with PURPLESEC. 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 PURPLESEC.*

Member information: *Any record maintained by, or on behalf of, PURPLESEC that contains information regarding an individual who has an established, ongoing relationship with PURPLESEC. 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 PURPLESEC.*

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
  - Vendor Management Review Program
  - Software Inventory
  - Hardware Inventory
  - Critical Systems List
  - Records Management
  - Clean Desk Policy
  - Hardware and Electronic Media Disposal Policy
  - IT Acquisition Policy
  - Incident Response Plan
  - Information Sharing
- Training
- Testing

Purpose

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

***Policy Detail* /R**

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

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

PURPLESEC 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.

PURPLESEC 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.

PURPLESEC's Information Security Officer is responsible for annually reviewing the program, making any needed adjustments, and coordinating staff training. PURPLESEC 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 PURPLESEC'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 PURPLESEC'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, PURPLESEC's Information Security Officer will provide the Board with a status report of PURPLESEC's Safeguarding Member Information Program.

Risk Assessment

PURPLESEC 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 PURPLESEC's Management. PURPLESEC's controls are then updated accordingly.

Management and Control of Risk
In order to manage and control the risks that have been identified, PURPLESEC will:

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

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

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

- Limit access at PURPLESEC'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 PURPLESEC'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 PURPLESEC'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 PURPLESEC 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 PURPLESEC's information security systems

Member information security controls /R
PURPLESEC 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**
  PURPLESEC 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. PURPLESEC 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**
  PURPLESEC 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**
  PURPLESEC 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 PURPLESEC 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**
  PURPLESEC 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 PURPLESEC.

- **Records management**
  The industry wide general principles of records management apply to records in any format. PURPLESEC 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.

PURPLESEC will adhere to the required state statues, NCUA, Data Classification Procedures, and federal guidelines designated for record retention. PURPLESEC 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**
  PURPLESEC 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**
  PURPLESEC 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**
  PURPLESEC 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 /R**
  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, PURPLESEC will assemble a team to handle any incidents that occur. Necessary actions to prepare PURPLESEC 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 PURPLESEC 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**
  PURPLESEC 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

PURPLESEC recognizes that adequate training is of primary importance in preventing IT security breaches, virus outbreaks, and other related problems. PURPLESEC 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 PURPLESEC'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.

PURPLESEC 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:*

- *Knowledge (something they know)*
- *Possession (something they have)*
- *Inherence (something they are)*

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

- *Being logged into the corporate network via a local Ethernet connection, and dialing into AOL or another Internet Service Provider (ISP)*
- *Being on a PURPLESEC provided remote access home network, and connecting to another network, such as a spouse's remote access*
- *Configuring an Integrated Services Digital Network (ISDN) router to dial into PURPLESEC 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 PURPLESEC's corporate network through a non-PURPLESEC controlled network, device, or medium.*

Split-tunneling: *Simultaneous direct access to a non-PURPLESEC network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into PURPLESEC'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 PURPLESEC's electronic information from being inadvertently compromised by authorized personnel connecting to the PURPLESEC network locally and remotely via VPN.

Purpose

The purpose of this policy is to define standards for connecting to PURPLESEC's network from any host. These standards are designed to minimize the potential exposure to PURPLESEC from damages, which may result from unauthorized use of PURPLESEC resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical PURPLESEC 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 PURPLESEC employees, volunteers/directors, contractors, vendors, and agents with a computer or workstation used to connect to the PURPLESEC network. This policy applies to remote access connections used to do work on behalf of PURPLESEC, 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 PURPLESEC's IT Department.

All remote access to PURPLESEC will either be through a secure VPN connection on a PURPLESEC owned device that has up-to-date anti-virus software, or on approved mobile devices (see the PURPLESEC Owned Mobile Device Acceptable Use and Security Policy and the Personal Device Acceptable Use and Security Policy).

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

Users inside the PURPLESEC firewall may not be connected to the PURPLESEC 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 PURPLESEC network without PURPLESEC IT approval.

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

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

Users must not download, install, or run security programs or utilities that reveal weaknesses in the security of a system. For example, PURPLESEC users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the PURPLESEC 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 PURPLESEC employees, volunteers/directors, contractors, vendors, and agents, with remote access privileges to PURPLESEC's corporate network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to PURPLESEC.

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

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

PURPLESEC 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 PURPLESEC's network:

- Virtual Private Network (VPN)
- Wireless Communications

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

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

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

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

- Must ensure that their computer, which is remotely connected to PURPLESEC'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-PURPLESEC email accounts (i.e. Hotmail, Yahoo, AOL), or other external resources to conduct PURPLESEC 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 PURPLESEC hardware, all hardware configurations must be approved by IT.

All hosts that are connected to PURPLESEC 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 PURPLESEC 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 PURPLESEC corporate network. This applies to implementations of VPN that are directed through an IPSec Concentrator.

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

Approved PURPLESEC employees, volunteers/directors, and authorized third parties (customers, vendors, etc.) may utilize the benefit of a VPN on a PURPLESEC 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 PURPLESEC 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 PURPLESEC IT.

- All computers connected to PURPLESEC 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 PURPLESEC'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 PURPLESEC-owned equipment or non-PURPLESEC 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 PURPLESEC'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 PURPLESEC approved VPN configured to drop all unauthenticated and unencrypted traffic and will be provisioned with split-tunneling disabled. As with all PURPLESEC computers, Windows or other OS and/or browser Internet proxy settings will be enabled to effectively route Internet access to the device through PURPLESEC 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 PURPLESEC networks is permitted on wireless systems that have been granted an exclusive waiver by IT for connectivity to PURPLESEC'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 PURPLESEC'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 PURPLESEC 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 PURPLESEC Network Procedure.doc]

Virtual Private Network (VPN) Agreement

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

ELIGIBILITY

The use of a mobile device connecting to the PURPLESEC 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 PURPLESEC and to ensure the data remains secure.

In the event of a security breach or threat, PURPLESEC 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 PURPLESEC 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 PURPLESEC network, attack PURPLESEC 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 PURPLESEC and is permitted to connect to internal information services in support of PURPLESEC 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

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

The User assumes full liability including, but not limited to, an outage or crash of any or all of the PURPLESEC 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 PURPLESEC 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 PURPLESEC 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 PURPLESEC must be managed to ensure that access to PURPLESEC's resources for business are performed in a safe and secure manner for participants of the PURPLESEC 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 PURPLESEC BYOD program which contains stored data owned by PURPLESEC, 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-PURPLESEC 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 PURPLESEC 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 PURPLESEC 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 PURPLESEC network.

Audience

This policy applies to all PURPLESEC 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 PURPLESEC has built with its members, suppliers, and other constituents. Consequently, employment at PURPLESEC 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. PURPLESEC 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 PURPLESEC'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, PURPLESEC 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 PURPLESEC 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 PURPLESEC 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 PURPLESEC or IT

Responsibilities of PURPLESEC

- 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 PURPLESEC.
- 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 PURPLESEC and PURPLESEC-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts PURPLESEC'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 PURPLESEC infrastructure. To find out if a preferred device is on this list, an individual should contact the PURPLESEC IT department Service Desk. Although IT currently allows only listed devices to be connected to the PURPLESEC 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 PURPLESEC 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 PURPLESEC network and data.

PURPLESEC'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 PURPLESEC 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 PURPLESEC network

Responsibilities of BYOD Participants

Security and Damages /R

- All potential participants will be granted access to the PURPLESEC network on the condition that they read, sign, respect, and adhere to the PURPLESEC policies concerning the use of these devices and services (see Exhibit A).

- Prior to initial use on the PURPLESEC 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 PURPLESEC, 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 PURPLESEC's infrastructure.

- PURPLESEC data is not to be accessed on any hardware that fails to meet PURPLESEC'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 PURPLESEC 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-PURPLESEC 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 PURPLESEC'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 PURPLESEC 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. /**R**

- BYOD equipment that is used to conduct PURPLESEC 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 PURPLESEC'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 PURPLESEC'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 PURPLESEC's highest priority.

- Employees, Board of Directors, volunteers, contractors, and temporary staff will not reconfigure mobile devices with any type of PURPLESEC owned and installed hardware or software without the express approval of PURPLESEC's IT Department.

- The **end user agrees to immediately report,** to his/her manager and PURPLESEC's IT Department, **any incident or suspected incidents of unauthorized data access,** data loss, and/or disclosure of PURPLESEC 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 PURPLESEC require that the third party and PURPLESEC 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 PURPLESEC.

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

Help and Support

PURPLESEC'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

PURPLESEC may offer a reimbursement of expenses to employees if they choose to use their own mobile devices in lieu of accepting a PURPLESEC-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 PurpleSec LLC (PURPLESEC), effective the date this agreement is executed by PURPLESEC'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 PURPLESEC 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 PURPLESEC and to ensure the data remains secure.

In the event of a security breach or threat, PURPLESEC 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 PURPLESEC network.

REIMBURSEMENT CONSIDERATIONS

PURPLESEC 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, PURPLESEC 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 PURPLESEC network. This includes, but is not limited to, expenses for voice minutes used to perform PURPLESEC business, data charges related to the use of PURPLESEC 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 PURPLESEC, loss related to unavailability of, disconnection from, or disabling the connection of a smart device to the PURPLESEC network, and loss resulting from compliance with this Agreement or applicable PURPLESEC policies.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

Compliance by the User with the following PURPLESEC 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 PURPLESEC network, attack PURPLESEC assets, or violate any of the security policies related to the subject matter of this Agreement.

SUPPORT

PURPLESEC will offer the following support for the personal smart device: connectivity to PURPLESEC 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. PURPLESEC 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 PURPLESEC network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the PURPLESEC 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

PURPLESEC expressly disclaims, and the User releases PURPLESEC 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**

Comprehensive IT Policy

Rev. 2015-08

Policy 17: Password /R

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.

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 PURPLESEC’s entire corporate network. As such, all PURPLESEC employees or volunteers/directors (including contractors and vendors with access to PURPLESEC 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 PURPLESEC facility, has access to the PURPLESEC network, or stores any non-public PURPLESEC information.

Policy Detail /R

User Network Passwords

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

- Passwords must be changed every 90 days
- Passwords must adhere to a minimum length of 10 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

System-Level Passwords

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

- Passwords must be changed at least every 6 months
- All administrator accounts must have 12 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 /R

- 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 PURPLESEC 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”).

- PURPLESEC 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.

- ~~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~~ /**R**

- Security tokens (i.e. smartcards, RSA hardware tokens, etc.) must be returned upon demand or upon termination of the relationship with PURPLESEC.

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 PURPLESEC is required to mitigate risk to the confidential data and the integrity of PURPLESEC'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. PURPLESEC 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 PURPLESEC 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 PURPLESEC 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 PURPLESEC 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 PURPLESEC. This policy applies to all equipment that is owned or leased by PURPLESEC, 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 PURPLESEC 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 PURPLESEC. It is PURPLESEC's policy to ensure all computer devices (including servers, desktops, printers, etc.) connected to PURPLESEC'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 PURPLESEC's network to identify known vulnerabilities

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

- Monitoring Computer Emergency Readiness Team (CERT), notifications, and Web sites of all vendors that have hardware or software operating on PURPLESEC'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 /R

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 /R

Physical access controls define who is allowed physical access to PURPLESEC 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 ~~exits~~ 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 PURPLESEC, 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 PURPLESEC.

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 PURPLESEC, its employees, members, or other third
parties.

Intellectual property: Is any data that is owned by PURPLESEC 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 PURPLESEC.

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

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 PURPLESEC 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 PURPLESEC 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 PURPLESEC to protect the confidentiality, security, and integrity of each member's non-public personal information. PURPLESEC 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 interest of PURPLESEC.

This policy acknowledges the potential use of diligently vetted cloud services, only with:

- Providers who prove, and can document in writing, that they can provide appropriate levels of protection to PURPLESEC data in categories that include, but are not limited to, transport, storage, encryption, backup, recovery, encryption key management, legal and regulatory jurisdiction, audit, or privacy
- Explicit procedures for all handling of PURPLESEC information regardless of the storage, sharing or computing resource schemes

Cloud Computing Services
The category of cloud service offered by the provider has a significant impact on the split of responsibilities between the customer and the provider to manage security and associated risks.

- Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. The provider is supplying and responsible for securing basic IT resources such as machines, disks, and networks. The customer is responsible for the operating system and the entire software stack necessary to run applications and is responsible for the customer data placed into the cloud computing environment. This means most of the responsibility for securing the applications and the data falls onto the customer.

- Software as a Service (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. The infrastructure, software, and data are primarily the responsibility of the provider, since the customer has little control over any of these features. These aspects need appropriate handling in the contract and the Service Level Agreement (SLA).

- Platform as a Service (PaaS) is a cloud computing service that provides a platform allowing customers to develop, run, and manage web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application. Responsibility is likely shared between the customer and provider.

Privacy Concerns
There are information security and data privacy concerns about use of cloud computing services at PURPLESEC. They include:

- PURPLESEC may be limited in its protection or control of its data, potentially leading to a loss of security, lessened security, inability to comply with various regulations and data handling protection laws, or loss of privacy of data due to aggregation with data from other cloud consumers.

- PURPLESEC’s dependency on a third party for critical infrastructure and data handling processes.

- PURPLESEC may have limited SLAs for a given provider’s services and the third parties that a cloud vendor might contract with.

- PURPLESEC is reliant on vendors' services for the security of the computing infrastructure.

Diligence
In evaluating the potential use of a particular cloud platform, PURPLESEC will pay particular attention to the foregoing, and other privacy concerns, in addition to its documented vendor due diligence program.

Exit Strategy
Cloud services should not be engaged without developing an exit strategy for disengaging from the vendor or service and integrating the service into business continuity and disaster recovery plans. PURPLESEC must determine how data would be recovered from the vendor.

Examples
The following table outlines the data classifications and proper handling of PURPLESEC data.

Data Classification	**Public Cloud Computing, Storage or Sharing***	**Private Cloud and On-premise Computing or Storage** User access restricted by username and password or another authentication
Financial Information	Not Allowed	Allowed No special requirements, subject to any applicable laws
Intellectual Property	Allowed but Not Advised	Allowed No special requirements, subject to any applicable laws
Other Non-Public Data	Allowed but Not Advised	Allowed No special requirements, subject to any applicable laws
Other Public Data	Allowed	Allowed No special requirements, subject to any applicable laws
Personally Identifiable Information (PII)	Not Allowed	Allowed No special requirements, subject to any applicable laws

*See Policy 20 Cloud Computing Adoption Appendix A for approved and non-approved services.

POLICY 20: CLOUD COMPUTING

Cloud Computing Adoption

Appendix A

Rev. November 30, 2020

Approved Public Cloud Services
This listing is not represented to be exhaustive and is meant to serve as a point-in-time list of approved or disapproved public cloud services as of the revision date in this appendix. Any cloud service not explicitly listed as approved should be assumed to be not approved until documented otherwise.

Services Approved for PURPLESEC Use	**Services Not Approved for PURPLESEC Use**
Box (Restricted*, Contact IT for access)	Amazon Cloud Drive
Evernote (Sync, restricted*)	Apple iCloud
Microsoft Azure (Hosted Office365)	AWS
Microsoft OneNote (Sync, restricted*)	Citrix Sharefile**
Vendor Due Diligence approved and documented point solutions currently in use and subject to restrictions*	Dropbox
Wrike (SaaS, IT project management, restricted*)	Google Drive
	Microsoft OneDrive
	~~Microsoft Azure (Hosted Office365)**~~
	Mimecast**
	Samanage**
	Sophos Central**
	Text Concierge (MEA Financial)**
	Other public cloud compute, storage, and sharing platforms

* Limited by user and intended use. See restrictions on data classification use in the main policy body
**Approval under review as of the date of this revision

Policy 21: Server Security

Definitions

File Transfer Protocol (FTP): *Is a standard Internet protocol for transmitting files between computers on the Internet.*

Overview

The servers at PURPLESEC provide a wide variety of services to internal and external users, and many servers also store or process sensitive information for PURPLESEC. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the IT Department to secure the hardware against such attacks.

Purpose

The purpose of this policy is to define standards and restrictions for the base configuration of internal server equipment owned and/or operated by or on PURPLESEC's internal network(s) or related technology resources via any means. This can include, but is not limited to, the following:

- Internet servers (FTP servers, Web servers, Mail servers, Proxy servers, etc.)
- Application servers
- Database servers
- File servers
- Print servers
- Third-party appliances that manage network resources

This policy also covers any server device outsourced, co-located, or hosted at external/third-party service providers, if that equipment resides in the PURPLESEC.org domain or appears to be owned by PURPLESEC.

The overriding goal of this policy is to reduce operating risk. Adherence to the PURPLESEC Server Security Policy will:

- Eliminate configuration errors and reduce server outages
- Reduce undocumented server configuration changes that tend to open up security vulnerabilities
- Facilitate compliance and demonstrate that the controls are working
- Protect PURPLESEC data, networks, and databases from unauthorized use and/or malicious attack

Therefore, all server equipment that is owned and/or operated by PURPLESEC must be provisioned and operated in a manner that adheres to company defined processes for doing so.

This policy applies to all PURPLESEC company-owned, company operated, or company controlled server equipment. Addition of new servers, within PURPLESEC facilities, will be managed at the sole discretion of IT. Non-sanctioned server installations, or use of unauthorized equipment that manage networked resources on PURPLESEC property, is strictly forbidden.

Policy Detail

Responsibilities

PURPLESEC's VP of IT has the overall responsibility for the confidentiality, integrity, and availability of PURPLESEC data.

Other IT staff members, under the direction of the Director of IT, are responsible for following the procedures and policies within IT.

Supported Technology

All servers will be centrally managed by PURPLESEC's IT Department and will utilize approved server configuration standards. Approved server configuration standards will be established and maintained by PURPLESEC's IT Department.

All established standards and guidelines for the PURPLESEC IT environment are documented in an IT storage location.

The following outlines PURPLESEC's minimum system requirements for server equipment supporting PURPLESEC's systems.

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the Director of IT or the VP of IT.
- Access to services must be logged or protected though appropriate access control methods.
- Security patches must be installed on the system as soon as possible through PURPLESEC's configuration management processes.
- Trust relationships allow users and computers to be authenticated (to have their identity verified) by an authentication authority. Trust relationships should be evaluated for their inherent security risk before implementation.
- Authorized users must always use the standard security principle of "Least Required Access" to perform a function.
- System administration and other privileged access must be performed through a secure connection. Root is a user account that has administrative privileges which allows access to any file or folder on the system. Do not use the root account when a non-privileged account will do.
- All PURPLESEC servers are to be in access-controlled environments.
- All employees are specifically prohibited from operating servers in environments with uncontrolled access (i.e. offices).

This policy is complementary to any previously implemented policies dealing specifically with security and network access to PURPLESEC's network.

It is the responsibility of any employee of PURPLESEC who is installing or operating server equipment to protect PURPLESEC's technology based resources (such as PURPLESEC data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to PURPLESEC's public image. Procedures will be followed to ensure resources are protected.

Policy 22: Social Media Acceptable Use

Definitions

Anonymous content: *A comment, reply, or post submitted to a PURPLESEC or affiliate site where the user has not registered and is not logged into the site*

PURPLESEC Official: is identified as any employee, officer, Board of Director, or volunteer

Facebook: A free social networking website

LinkedIn: A social networking site designed specifically for the business community

Microblogging: A web service that allows the subscriber to broadcast short messages to other subscribers of the service

Social Media: A form of interactive online communication in which users can generate and share content through text, images, audio, and/or video. For purposes of this policy, "Social Media" includes, but is not limited to, online blogs, chat rooms, personal websites, and social networking sites, such as Facebook, Twitter, MySpace, LinkedIn, YouTube, etc. The absence of, or lack of, explicit reference to a specific social networking tool does not limit the extent of the application of this policy. As new online tools are introduced, this policy will be equally applicable without advance notice.

Twitter: A free social networking microblogging service that allows registered members to broadcast short posts called tweets

YouTube: A video-sharing website on which users can upload, share, and view videos

Overview

The use of external social media (i.e. Facebook, LinkedIn, Twitter, YouTube, etc.) within organizations for business purposes is increasing. PURPLESEC faces exposure of a certain amount of information that can be visible to friends of friends from social media. While this exposure is a key mechanism driving value, it can also create an inappropriate conduit for information to pass between personal and business contacts. Tools to establish barriers between personal and private networks and tools to centrally manage accounts are only beginning to emerge. Involvement by the IT Department for security, privacy, and bandwidth concerns is of utmost importance.

Purpose of Using Social Media

There are several ways PURPLESEC can benefit from using external (public) social media, such as Facebook, LinkedIn, and Twitter.

- **Building a positive image:** PURPLESEC can use social media to promote a positive image. While this is particularly important for organizations generally vulnerable to negative press or consumer discontent, it can also be used to boost PURPLESEC's image within the community.

- **Increasing mind share:** Social media can reach large audiences at very low monetary cost, giving PURPLESEC another medium for promotion and increasing awareness of PURPLESEC.

- **Improving member satisfaction:** Members who receive more timely and personal service, in the medium that they prefer, will be more satisfied.
- **Gaining member insights:** Social media can be used to monitor public opinion about PURPLESEC, its products and services, or its competitors.
- **Increasing member retention:** Using social media builds affinity and loyalty since members are engaged using a medium, they prefer – something PURPLESEC needs to offer to remain competitive.
- **Increasing revenue:** Use of social media to create custom network applications (a.k.a. plug-ins) for product promotion or integration with PURPLESEC's online services.
- **Member acquisition:** Use of social media to quickly and efficiently respond to member service issues. The answer to the problem can be public, making it searchable by other members who have the same request.
- **Disaster Recovery:** Use of social media to quickly and efficiently eliminate fears and communicate accurate information regarding recovery actions in the event of a disaster.

Policy Detail

PURPLESEC encourages the use of social media as a channel for business communication, consistent with BCHHU's corporate marketing and communications strategy. It is the policy of PURPLESEC to establish guidelines for safe social media usage with respect to protecting PURPLESEC information. The safety and confidentiality of information is vital to PURPLESEC's success. PURPLESEC has established this policy to set parameters and controls related to PURPLESEC Official's usage of social media websites.

Terms and Conditions of Use

All requests for a PURPLESEC Official's use of external social media, on behalf of PURPLESEC, must be submitted to the Senior Management Team. PURPLESEC may allow access to select pre-approved social media websites. PURPLESEC Officials may only access these sites in a manner consistent with PURPLESEC's security protocols and PURPLESEC Officials may not circumvent IT Security protocols to access social media sites.

Use of personal social media accounts and user IDs, for PURPLESEC use, is prohibited.

Use of PURPLESEC social media user IDs, for personal use, is prohibited. Use of PURPLESEC email addresses to register on social networks, blogs, or other online tools utilized for personal use is prohibited. Examples of prohibited use of company User IDs include:

- Downloading and installing plug-ins or helper applications such as those that try to access the PURPLESEC e-mail directory

- Joining groups using a company user ID for personal reasons

- Adding personal friends to a PURPLESEC Official's friends list

PURPLESEC Officials are to acknowledge they have reviewed the social media service's Terms of Service (TOS) or Terms of User (TOU), as applicable. Links for sites are below.

Facebook: https://www.facebook.com/terms.php
LinkedIn: http://www.linkedin.com/static?key=user_agreement
Twitter: http://twitter.com/tos
YouTube: http://www.youtube.com/t/terms

Representing PURPLESEC

PURPLESEC Senior Management will designate a person or team to manage and respond to social media issues concerning PURPLESEC and will determine who will have the authority to contribute content. This person(s)'s responsibilities will include, but are not limited to:

- **Managing** social media tools and channels;
- **Responding** to questions internally and externally about the social media site;
- **Addressing** problems/providing direction for staff if a user becomes threatening, abusive, or harassing;
- **Suggesting** changes to this PURPLESEC social media policy when warranted;
- **Working** with other staff to make sure opportunities aren't overlooked in marketing PURPLESEC services; and
- **Training** staff to ensure they understand how to use PURPLESEC's social media program.

PURPLESEC will take the necessary steps to make sure the content complies with applicable laws and regulations.

All PURPLESEC Officials who participate in social media, on behalf of PURPLESEC, are expected to represent PURPLESEC in a professional manner. Failure to do so could have negative impact on PURPLESEC and could jeopardize a PURPLESEC Official's ability to participate in social media in the future.

PURPLESEC owns all authorized social media and networking content. PURPLESEC Officials are prohibited from taking, saving, or sending any PURPLESEC content distributed via social media while employed, separated, serving on the Board of Directors, or terminated by PURPLESEC.

New technologies and social networking tools continually evolve. As new tools emerge, this policy will be updated to reflect the changes.

Platforms for online collaboration are fundamentally changing the work environment and offering new ways to engage with members and the community. Guiding principles for participating in social media should be followed.

- Post meaningful, respectful comments and refrain from remarks that are off-topic or offensive.
- Reply to comments quickly when a response is appropriate.
- Know and follow the state and federal laws that protect member confidentiality at all times.
- Protect proprietary information and confidentiality.
- When disagreeing with others' opinions, keep it professional.
- Know the PURPLESEC Code of Conduct and apply the standards and principles in social computing.

Personal Blogs and Posts

PURPLESEC takes no position on a PURPLESEC Official's decision to start or maintain a blog or personal website or to participate in other online social media activities outside of work. PURPLESEC Officials, identifying themselves as a PURPLESEC Official on a social network, should ensure their profile and related content is consistent with how they and PURPLESEC wish for them to present themselves. This includes what the PURPLESEC Official writes about himself/herself and the type of photos he/she publishes.

PURPLESEC Officials must not reveal proprietary information and must be cautious about posting exaggerations, obscenities, or other characterizations that could invite litigation.

PURPLESEC Officials must not make public reference to any PURPLESEC related cash or security procedures.

PURPLESEC Officials who comment on any PURPLESEC business or policy issue must clearly identify themselves as a PURPLESEC Official in their blog or posting and include a disclaimer that the views are their own and not those of PURPLESEC. When generating content that deals with PURPLESEC or individuals associated with PURPLESEC, PURPLESEC Officials should use a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of PURPLESEC".

PURPLESEC Officials must not use social media websites to harass, threaten, discriminate against, disparage, or defame any other PURPLESEC Officials, members, vendors, PURPLESEC products, services, or business philosophy.

PURPLESEC Officials are prohibited from disclosing confidential, proprietary, or otherwise sensitive business or personal information related to PURPLESEC or any of its PURPLESEC Officials, vendors, or members. PURPLESEC Officials are also prohibited from disclosing any confidential, proprietary, or otherwise sensitive business or personal information that could identify another PURPLESEC Official, vendor, or member without that individual's prior authorization.

PURPLESEC Officials should not take any action via social media websites or personal blogs that would harm, or is likely to harm, the reputation of PURPLESEC or any PURPLESEC Officials, members, or vendors.

Rules of Engagement
Protecting member information is everyone's number one responsibility. Information that can be used to disclose a member's personal information in any way should never be posted. Members trust PURPLESEC to protect their financial assets and information.

Communications in written, audio, or video form will be around for a long time, so consider the content carefully and be judicious. Brand, trademark, copyright, fair use, and privacy laws must be respected. If any employee mentions a financial product in a blog, a tweet, or another form, financial disclosure laws apply online. The employee must comply with advertising disclosure regulations by providing a link back to PURPLESEC's website page that lists the proper disclosures.

What is written, produced, or recorded is ultimately the employee's responsibility. Participation in social computing on behalf of PURPLESEC is not a right and, therefore, needs to be taken seriously and with respect. Failure to comply could put an employee's participation at risk and can lead to discipline. Third-party site's terms and conditions must be followed.

Denigration of competitors, PURPLESEC, or PURPLESEC affiliates is not permitted. Communication should be respectful when inviting differing points of view. Topics like politics or religion are not appropriate for PURPLESEC communications. Communicate carefully and be considerate; once the words or other materials are out there, they cannot be retracted.

Personal information belongs to the members of PURPLESEC. It is their choice to share that information, not PURPLESEC's. PURPLESEC will not publish material without first discussing it with a manager or legal representative.

Rules of Composition

- PURPLESEC Officials should write and post about their areas of expertise, especially as it relates to PURPLESEC.
- Write in the first person. Talk to the reader as if he/she were a real person in a professional situation.
- Avoid overly composed language.
- Consider content that is open-ended and invites response.
- Encourage comments.
- Use a spell-checker.
- Make the effort to be clear, complete, and concise in the communication. Determine if the material can be shortened or improved.

- If a mistake is made, it must be acknowledged. Be upfront and be quick with the correction. If posting to a blog, make it clear if a modification has been done to an earlier post.

Produce material PURPLESEC members will value. Social media communication from PURPLESEC should help its members, partners, and co-workers. It should be thought provoking and build a sense of community. It should help members improve their knowledge or understand PURPLESEC or an affiliate better.

Anonymous content is not allowed on PURPLESEC sites.

Personal Use of Third-Party Sites During Work Hours
E-mail and Internet access is provided to support PURPLESEC business purposes. If these tools are accessed, incidental personal use of them is permitted. In general, PURPLESEC will limit the access of social media sites to PURPLESEC Officials who use it on behalf of PURPLESEC. Excessive personal use of any Internet tool during work time is not permitted and access privileges may be revoked for abuse of the system.

Retaliation is Prohibited
PURPLESEC prohibits taking negative action against any PURPLESEC Official for reporting a possible deviation from this policy or for cooperating in an investigation. Any PURPLESEC Official who retaliates against another PURPLESEC Official for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination of employment at PURPLESEC or removal from the Board of Directors.

Policy 23: Systems Monitoring and Auditing

Overview

Systems monitoring and auditing, at PURPLESEC, must be performed to determine when a failure of the information system security, or a breach of the information systems itself, has occurred, and the details of that breach or failure.

Purpose

System monitoring and auditing is used to determine if inappropriate actions have occurred within an information system. System monitoring is used to look for these actions in real time while system auditing looks for them after the fact.

This policy applies to all information systems and information system components of PURPLESEC. 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
- Firewall, Intrusion Detection/Prevention (IDP) sensors, and other devices that provide dedicated security capabilities

Policy Details

Information systems will be configured to record login/logout and all administrator activities into a log file. Additionally, information systems will be configured to notify administrative personnel if inappropriate, unusual, and/or suspicious activity is noted. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to the VP of IT or COO.

Information systems are to be provided with sufficient primary (on-line) storage to retain 30-days' worth of log data and sufficient secondary (off-line) storage to retain one year's worth of data. If primary storage capacity is exceeded, the information system will be configured to overwrite the oldest logs. In the event of other logging system failures, the information system will be configured to notify an administrator.

System logs shall be manually reviewed weekly. Inappropriate, unusual, and/or suspicious activity will be fully investigated by appropriate administrative personnel and findings reported to appropriate security management personnel.

System logs are considered confidential information. As such, all access to system logs and other system audit information requires prior authorization and strict authentication. Further, access to logs or other system audit information will be captured in the logs.

Policy 24: Vulnerability Assessment

Overview

Vulnerability assessments, at PURPLESEC, are necessary to manage the increasing number of threats, risks, and responsibilities. Vulnerabilities are not only internal and external, but there are also additional responsibilities and costs associated with ensuring compliance with laws and rules, while retaining business continuity and safety of PURPLESEC and member data.

Purpose

The purpose of this policy is to establish standards for periodic vulnerability assessments. This policy reflects PURPLESEC's commitment to identify and implement security controls, which will keep risks to information system resources at reasonable and appropriate levels.

This policy covers all computer and communication devices owned or operated by PURPLESEC. This policy also covers any computer and communications device that is present on PURPLESEC premises, but which may not be owned or operated by PURPLESEC. Denial of Service testing or activities will not be performed.

Policy Detail

The operating system or environment for all information system resources must undergo a regular vulnerability assessment. This standard will empower the IT Department to perform periodic security risk assessments for determining the area of vulnerabilities and to initiate appropriate remediation. All employees are expected to cooperate fully with any risk assessment.

Vulnerabilities to the operating system or environment for information system resources must be identified and corrected to minimize the risks associated with them.

Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources
- Investigate possible security incidents and to ensure conformance to PURPLESEC's security policies
- Monitor user or system activity where appropriate

To ensure these vulnerabilities are adequately addressed, the operating system or environment for all information system resources must undergo an authenticated vulnerability assessment.

The frequency of these vulnerability assessments will be dependent on the operating system or environment, the information system resource classification, and the data classification of the data associated with the information system resource.

Retesting will be performed to ensure the vulnerabilities have been corrected. An authenticated scan will be performed by either a Third-Party vendor or using an in-house product.

All data collected and/or used as part of the Vulnerability Assessment Process and related procedures will be formally documented and securely maintained.

IT leadership will make vulnerability scan reports and on-going correction or mitigation progress to senior management for consideration and reporting to the Board of Directors.

Policy 25: Website Operation

Overview

The PURPLESEC website provides information to members, potential members, and non-members regarding PURPLESEC. It is designed to allow members to transact business with PURPLESEC and assist non-members with information on how to join PURPLESEC. PURPLESEC's website may provide links to websites, outside its website, that also serve this purpose.

Purpose

The purpose of this policy is to establish guidelines with respect to communication and updates of PURPLESEC's public facing website. Protecting the information on and within the PURPLESEC website, with the same safety and confidentiality standards utilized in the transaction of all PURPLESEC business, is vital to PURPLESEC's success.

Policy Detail

To be successful, the PURPLESEC website requires a collaborative, proactive approach by the stakeholders. All stakeholders share the same broad goals and objectives:

- Support the goals and key initiatives of PURPLESEC
- Develop content that is member focused, relevant, and valuable, while ensuring the best possible presentation, navigation, interactivity, and accuracy
- Promote a consistent image and identity to enhance marketing effectiveness
- Periodically assess the effectiveness of web pages

Responsibility

The Marketing Department and Chief Experience Officer (CXO) are responsible for the website content and ensuring that materials meet legal and policy requirements.

The IT Department is responsible for the security, functionality, and infrastructure of the website. The System Administrators will monitor the PURPLESEC website for response time and to resolve any issues encountered. The Core System Analyst will monitor the Online Banking Program for outages and will open a case with the appropriate vendor to log the event.

Links

PURPLESEC is not responsible for, and does not endorse, the information on any linked website, unless PURPLESEC's website and/or this policy states otherwise. The following criteria will be used to decide whether to place specific links on the PURPLESEC website. PURPLESEC will place a link on the website if it serves the general purpose of PURPLESEC's website and provides a benefit to its members. PURPLESEC's website will provide links to websites for:

- Secure member transactions such as bill pay, home banking, and loan applications

- Secure methods for members to receive information such as monthly statements

- Ancillary services that are provided to members through third-parties, such as ordering checks, mortgage loan applications, identity theft protection

- The PURPLESEC website contains a web link disclosure

- The PURPLESEC website will not provide links to websites for:
  - Illegal or discriminatory activities
  - Candidates for local, state, or federal offices
  - Political organizations or other organizations advocating a political position on an issue
  - Individual or personal home pages

Security
When a login is required, various forms of multi-factor authentication are implemented to ensure the privacy of member information and security of their transactions. This process is to be implemented for access to Online Banking.

The PURPLESEC website, as well as linked sites, may read some information from the users' computers. The website or linked transactional websites may create and place cookies on the user's computer to ensure the user does not have to answer challenge questions when returning to the site. The multi-factor authentication process will still be required at the next login. This cookie will not contain personally identifying information and will not compromise the user's privacy or security.

Website Changes
Changes to the website will be executed by the PURPLESEC Marketing Department, another trained and qualified employee, or a specialized firm or individual they may retain, and only with the explicit approval of the President/CEO or senior executive designated. Website changes require two parties in order to implement. On an annual basis, the PURPLESEC website is reviewed by a third-party compliance expert. At the time of any significant changes to the website, a compliance review will be conducted by the Director of Fraud and Compliance, legal counsel, or another reputable 3rd party compliance expert.

Regulatory Compliance
The PURPLESEC website must comply with all regulations dealing with security of member information, including, but not limited to:

- Part 748 of NCUA Rules and Regulations: Security Program;
- Report of Crime and Catastrophic Act;
- Bank Secrecy Act Compliance;
- As well as all other regulations, such as disclosure requirements.

At a minimum, the following disclosures will appear on the website:

- Privacy Policy and Web Privacy Policy
- EStatements and Disclosures
- Electronic Funds Transfer
- Monthly Billing Rights/Error Resolution Notice
- Web Links Disclaimer

Website Design

The PURPLESEC website maintains a cohesive and professional appearance. While a sophisticated set of services is offered on the website, the goal is to maintain relatively simplistic navigation to ensure ease of use. Security on the website and protection of member information is the highest priority in the layout and functionality of the site.

Policy 26: Workstation Configuration Security

Definitions

Domain: In computing and telecommunication in general, a domain is a sphere of knowledge identified by a name. Typically, the knowledge is a collection of facts about some program entities or a number of network points or addresses.

Overview

The workstations at PURPLESEC provide a wide variety of services to process sensitive information for PURPLESEC. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the IT Department to secure the hardware against such attacks.

Purpose

The purpose of this policy is to enhance security and quality operating status for workstations utilized at PURPLESEC. IT resources are to utilize these guidelines when deploying all new workstation equipment. Workstation users are expected to maintain these guidelines and to work collaboratively with IT resources to maintain the guidelines that have been deployed.

The overriding goal of this policy is to reduce operating risk. Adherence to the PURPLESEC Workstation Configuration Security Policy will:

- Eliminate configuration errors and reduce workstation outages
- Reduce undocumented workstation configuration changes that tend to open up security vulnerabilities
- Facilitate compliance and demonstrate that the controls are working
- Protect PURPLESEC data, networks, and databases from unauthorized use and/or malicious attack

Therefore, all new workstation equipment that is owned and/or operated by PURPLESEC must be provisioned and operated in a manner that adheres to company defined processes for doing so.

This policy applies to all PURPLESEC company-owned, company operated, or company controlled workstation equipment. Addition of new workstations, within PURPLESEC facilities, will be managed at the sole discretion of IT. Non-sanctioned workstation installations, or use of unauthorized equipment that manage networked resources on PURPLESEC property, is strictly forbidden.

Policy Detail /R

Responsibilities

PURPLESEC's VP of IT has the overall responsibility for the confidentiality, integrity, and availability of PURPLESEC data.

Other IT staff members, under the direction of the VP of IT, are responsible for following the procedures and policies within IT.

Supported Technology /R
All workstations will be centrally managed by PURPLESEC's IT Department and will utilize approved workstation configuration standards, which will be established and maintained by PURPLESEC's IT Department.

All established standards and guidelines for the PURPLESEC IT environment are documented in an IT storage location.

The following outlines PURPLESEC's minimum system requirements for workstation equipment.

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the VP of IT.
- All patch management to workstations will be monitored through reporting with effective remediation procedures. PURPLESEC has deployed a patch management process; reference the Patch Management Policy.
- All workstations joined to the PURPLESEC domain will automatically receive a policy update configuring the workstation to obtain future updates from our desktop management system.
- All systems within PURPLESEC are required to utilize anti-virus, malware, and data leakage protection. IT will obtain alerts of infected workstations and perform certain remediation tasks.
- All workstations will utilize the PURPLESEC domain so that all general policies, controls, and monitoring features are enabled for each workstation. No system should be managed manually but should be managed through some central tool or model in order to efficiently manage and maintain system security policies and controls.
- ~~Third-party applications need to be updated and maintained. So that software with security updates is not exposed to vulnerabilities for longer than necessary, a quarterly review will be performed.~~
- Third-party applications, including browsers, shall be updated and maintained in accordance with the PURPLESEC patch management program.
- Any critical security updates for all applications and operating systems need to be reviewed and appropriate actions taken by the IT Department to guarantee the security of the workstations in accordance with the PURPLESEC patch management program.

- ~~Internet browsers on workstations will remain up to date. To ensure all browsers are up to date, the IT Department will perform quarterly reviews. If there is a reason the browser cannot be updated, due to conflicts with applications, these exceptions will be recorded.~~

- By default, all workstations joined to the PURPLESEC domain will obtain local security settings through policies.

This policy is complementary to any previously implemented policies dealing specifically with security and network access to PURPLESEC's network.

It is the responsibility of each employee of PURPLESEC to protect PURPLESEC's technology based resources from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to PURPLESEC's public image. Procedures will be followed to ensure resources are protected.

Policy 27: Server Virtualization

Definitions

Virtualization: The creation of a virtual (rather than actual) version of something, such as an operating system, a server, a storage device, or network resources.

Overview

This policy encompasses all new and existing workloads.

Purpose

The purpose of this policy is to establish server virtualization requirements that define the acquisition, use, and management of server virtualization technologies. This policy provides controls that ensure that Enterprise issues are considered, along with business objectives, when making server virtualization related decisions.

Platform Architecture policies, standards, and guidelines will be used to acquire, design, implement, and manage all server virtualization technologies.

Policy Detail

PURPLESEC's VP of IT has the overall responsibility for ensuring that policies are followed in order to establish contracts and the confidentiality, integrity, and availability of PURPLESEC data.

Other IT staff members, under the direction of the Director of IT, are responsible for following the procedures and policies within IT.

PURPLESEC's legacy IT practice was to dedicate one physical server to a single workload. The result of this practice was excessive server underutilization, an ever-expanding data center footprint, and excessive data center power consumption.

Server virtualization software allows the consolidation of new and existing workloads onto high capacity x86 servers. Consolidating workloads onto high capacity x86 servers allows PURPLESEC to reduce the x86 server inventory, which in turn decreases the data center footprint and data center power consumption.

PURPLESEC will migrate all new and existing workloads from physical servers to virtual machines. Hardware will be retired at such time as planned by IT management or required by incompatibility with Operating Systems (OS) and/or workload specific software updates.

Server Virtualization Requirements:

- Support industry-wide open-standards
- Embedded security technology, such as, Trusted Platform Module (TPM) or other technologies
- Single centralized management console
- Support industry standard management tools

- Support industry standard backup and recovery tools
- Interoperate with other platform technologies
- Support industry standard x86 hardware
- Support industry standard storage
- Support unmodified guest operating systems
- Functionality to support virtual server management network isolation
- Migrate running guests without interruption
- Add disks to a running guest
- Automatically detect a hardware failure and restart guests on another physical server
- Functionality to configure role based access for the administrative console
- Support Lightweight Directory Access Protocol (LDAP) for authentication and authorization for administrative console
- Encrypt all intra host and administrative console traffic
- Integrated graphical Central Processing Unit (CPU), memory, disk, and network performance monitoring, alerting, and historical reporting for hosts and guests
- Other industry standard or best in class features as required

Policy 28: Wireless (Wi-Fi) Connectivity

Definitions

Wireless Access Point (AP): A device that allows wireless devices to connect to a wired network using Wi-Fi or related standards.

Keylogger: The action of recording or logging the keystrokes on a keyboard.

Wi-Fi: A term for certain types of wireless local area networks (WLAN) that use specifications in the 802.11 family.

Wireless: A term used to describe telecommunications in which electromagnetic waves, rather than some form of wire, carry the signal over all or part of the communication path.

Overview

This policy addresses the wireless connection of PURPLESEC owned devices in remote locations.

Purpose

The purpose of this policy is to secure and protect the information assets owned by PURPLESEC and to establish awareness and safe practices for connecting to free and unsecured Wi-Fi, and that which may be provided by PURPLESEC. PURPLESEC provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. PURPLESEC grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

Policy Detail

PURPLESEC Wi-Fi Network

The PURPLESEC Wi-Fi network is provided on a best-effort basis, primarily as a convenience to employees and others who may receive permission to access it. For employee business use, it is designed to be a supplement to, and not a substitute for, the production wired local area network. For non-employees, it is also provided as a convenience, primarily as a way for members to access PURPLESEC online products and services. Staff may easily demonstrate PURPLESEC online products and services to members or prospects. Wi-Fi access points, located at the Court Street facilities and in most branch offices, allow for compatible wireless device connectivity.

Microwaves, cordless telephones, neighboring APs, and other Radio Frequency (RF) devices that operate on the same frequencies as Wi-Fi are known sources of Wi-Fi signal interference. Wi-Fi bandwidth is shared by everyone connected to a given Wi-Fi access point (AP). As the number of Wi-Fi connections increase, the bandwidth available to each connection decreases and performance deteriorates. Therefore, the number and placement of APs in a given building is a considered design decision. Due to many variables out of direct PURPLESEC control, availability, bandwidth, and access is not guaranteed.

The PURPLESEC Wi-Fi network and connection to the Internet shall be:

- Secured with a passphrase and encryption, in accordance with current industry practice
    - Passphrases will be of appropriate complexity and changed at appropriate intervals, balancing security practice with the intended convenient business use of the Wi-Fi
- Physically or logically separate from the PURPLESEC production wired local area network (LAN) and its resources
- Provided as a convenience for the use of PURPLESEC employees, their vendors while visiting PURPLESEC, the members of PURPLESEC, and other visitors with PURPLESEC's express permission via provision of an appropriate passphrase
- Optionally provided to members and qualifying visitors, by PURPLESEC staff, with the provision of an appropriate passphrase and may be accessed only with the agreement to acceptable use policy statements provided online or in a written or verbal format
- Accessed by employees only in accordance with the Acceptable Use policy and its cross-referenced policies seen in Policy 1 in this document
- Used for access to the PURPLESEC production LAN only for business use and with the approved use of a PURPLESEC issued virtual private network (VPN) connection

PURPLESEC's Wi-Fi service may be changed, the passphrase re-issued or rescinded, the network made unavailable, or otherwise removed without notice for the security or sustainability of PURPLESEC business

Public Wi-Fi Usage
When using Wi-Fi on a mobile device in a public establishment, there are precautions that should be followed.

Do:

- As with any Internet-connected device, defend your laptop, tablet, phone, etc. against Internet threats. Make sure your computer or device has the latest antivirus software, turn on the firewall, never perform a download on a public Internet connection, and use strong passwords.
- Look around before selecting a place to sit, consider a seat with your back to a wall and position your device so that someone nearby cannot easily see the screen.
- Assume all Wi-Fi links are suspicious, so choose a connection carefully. A rogue wireless link may have been set up by a hacker. Actively choose the one that is known to be the network you expect and have reason to trust.
- Try to confirm that a given Wi-Fi link is legitimate. Check the security level of the network by choosing the most secure connection, even if you have to pay for access. A password-protected connection (one that is unique for your use) is better than one with a widely shared passphrase and infinitely better than one without a passphrase.
- Consider that one of two similar-appearing SSIDs or connection names may be rogue and could have been setup by a hacker. Inquire of the manager of the establishment for information about their official Wi-Fi access point.

- Avoid free Wi-Fi with no encryption. Even if your website or other activity is using https (with a lock symbol in your browser) or other secure protocols, you are at much greater risk of snooping, eavesdropping, and hacking when on an open Wi-Fi connection (such as at Starbuck's, McDonald's, some hotels, etc.).
- Seek out Wi-Fi connections that use current industry accepted encryption methods and that generally will require the obtaining of a passphrase from the establishment.
- Consider using your cell phone data plan for sensitive activities rather than untrusted Wi-Fi, or your own mobile hotspot if you have one or have been provided with one.
- If you must use an open Wi-Fi, do not engage in high-risk transactions or highly-confidential communication without first connecting to a virtual private network (VPN).
- If sensitive information absolutely must be entered while using a public network, limit your activity and make sure that, at a minimum, your web browser connection is encrypted with the locked padlock icon visible in the corner of the browser window, and make sure the web address begins with https://. If possible, save your financial transactions for when you are on a trusted and secured connection, at home, for instance. Passwords, credit card numbers, online banking logins, and other financial information is less secure on a public network.
- Avoid visiting sites that can make it easier or more tempting for hackers to steal your data (for example, banking, social media, and any site where your credit card information is stored).
- If you need to connect to the PURPLESEC network and are authorized to do so, choose a trusted and encrypted Wi-Fi AP or use your personal hotspot. In every case, you must use your PURPLESEC-provided VPN at all times. The VPN tunnel encrypts your information and communications and besides, hackers are much less likely to be able to penetrate this tunnel and will prefer to seek less secure targets.
- In general, turn off your wireless network on your computer, tablet, or phone when you are not using it to prevent automatic connection to open and possibly dangerous APs. Set your device to not connect automatically to public or unknown and untrusted networks.

Finally,

Do Not:

- Leave your device unattended, not even for a moment. Your device may be subject to loss or theft, and even if it is still where you left it, a thief could have installed a keylogger to capture your keystrokes or other malware to monitor or intercept the device or connection.
- Email or originate other messages of a confidential nature or conduct banking or other sensitive activities, and definitely not when connected to an open, unencrypted Wi-Fi.
- Allow automatic connection to or connection to first Wi-Fi AP your device finds, as it may be a rogue AP set up by a thief. Rather, choose the one that is known to be the network you expect and have reason to trust.

Policy 29: Telecommuting

Definitions

Telecommuting: A work arrangement in which employees do not commute or travel by bus or car to a central place of work, such as an office building, warehouse, or store. Telecommuters often maintain a specific office or workspace and usually work from this alternative work site during predefined days of the week. This is differentiated from *teleworking* or *working remotely,* that may refer to *casual* or *occasional* remote work done by a traditional employee while away from their traditional company office.

Overview

Telecommuting allows employees to work at home. Telecommuting is a voluntary work alternative that may be appropriate for some employees and some jobs.

Purpose

For the purposes of this policy, reference is made to the defined telecommuting employee who regularly performs their work from an office that is not within a PURPLESEC building or suite. Casual telework by employees or remote work by non-employees is not included herein. Focusing on the IT equipment typically provided to a telecommuter, this policy addresses the telecommuting work arrangement and the responsibility for the equipment provided by PURPLESEC.

Policy Detail

Telecommuting arrangements are made on a case-by-case basis, focusing first on the business needs of the organization.

The company may provide specific equipment for the employee to perform his/her current duties. This may include computer hardware, computer software, mobile phone, email, voicemail, connectivity to host applications, and other applicable equipment as deemed necessary. In order to purchase, configure, ship, and install the required equipment to the remote location, the IT Department shall be notified in advance of the telecommuting start date.

The use of equipment, software, and data supplies, when provided by PURPLESEC for use at the remote work location, is limited to authorized persons and for purposes relating to PURPLESEC business. PURPLESEC will provide for repairs to or replacement of provided equipment. Damage to equipment owned by PURPLESEC, that is outside the employee's control, will be covered by the organization's insurance policy. In the event of such damage, loaner equipment may be provided when available and must be returned upon request.

The IT Department will be responsible for all equipment installation, maintenance, security access, support, and necessary training related to PURPLESEC equipment and software at the remote site, even in the event IT chooses to outsource services. All provided, qualified equipment will be tracked in the IT asset program.

The employee shall designate a workspace, within the remote work location, for placement and installation of equipment to be used while teleworking. The employee shall maintain this workspace in a safe condition, free from hazards and other dangers to the employee and equipment. All PURPLESEC materials should be kept in the designated work area at home and not made accessible to others. All applicable policies for acceptable use, protection of member information, security, reimbursement of business voice and Internet charges, etc., shall be observed. Personally owned equipment may not be connected to PURPLESEC owned equipment.

The employee must sign the Telecommuting Equipment Agreement document and the Telecommuting Equipment document for all PURPLESEC owned property provided to the employee for telecommuting purposes (see Exhibits A and B). When the employee ceases to telecommute or is terminated, all PURPLESEC owned equipment shall be returned to the IT Department within five (5) business days.
.

EXHIBIT A

[This is a copy of the addendum A in the telecommuting IT procedure]

TELECOMMUTING EQUIPMENT AGREEMENT

Employee ______________________________ Manager ______________________________

Position ______________________________ Telecommuting Start Date_______________

This document is to inventory the equipment used for the employee listed above at a remote location that has been approved by the employee's manager.

The employee's alternative work site is located at the following address:

Address ____

City, State, Zip ____

Phone Number ____

Email address ____

The employee understands and agrees to the following:

1. The employee is responsible for securing the equipment provided to the employee by the PURPLESEC IT Department.

2. No personally owned equipment may be connected to the PURPLESEC owned equipment.

3. This equipment is the sole and exclusive property of PURPLESEC.

4. With the exception of normal wear and tear, the employee is liable for the condition of the equipment and for any damages caused by any misuse, negligence, and/or unauthorized use of the equipment.

5. The employee will not modify any PURPLESEC equipment without written authorization from the IT Department.

6. In the event of equipment failure, the employee will notify the IT Department as soon as possible. PURPLESEC may supply temporary equipment in the event of equipment failure.

7. All equipment provided by PURPLESEC is provided exclusively for use in providing services to PURPLESEC. Only the employee may use the equipment and only for PURPLESEC business-related purposes.

8. Within five (5) business days after the employee ceases to telecommute or after termination of employment at PURPLESEC, the employee shall return all supplied equipment to the IT Department. If it should become necessary for PURPLESEC to resort to legal or other means to recover its equipment, the employee agrees to pay all related costs and attorneys' fees that may be incurred by PURPLESEC.

The employee has read, understands, and acknowledges this agreement by signing below.

____________________________________ _________________
Employee – Signature Date

____________________________________ _________________
Manager – Signature Date

____________________________________ _________________
Director of IT – Signature Date

cc: Manager File

Rev. 2016-00

EXHIBIT B

[This is a copy of the addendum B in the telecommuting IT procedure]

TELECOMMUTING EQUIPMENT

The following PURPLESEC owned equipment is being provided to the employee, for use at the employee's alternate work site, to accommodate the telecommuting arrangement commencing on this date ____________________.

Item Description	Serial No.	Make	Model

All line items above are to be maintained in like condition as when it was provided to the employee.

This PURPLESEC equipment and its use is covered in the PURPLESEC telecommuting policy and procedure, with its Exhibits and Addenda.

Acknowledged:

___________________________________ __________________

Employee – Signature Date

___________________________________ __________________

Manager – Signature Date

Rev. 2016-00

Policy 30: Internet of Things

Definitions

Internet of Things (IoT): Refers to network or Internet connected devices such as appliances, thermostats, monitors, sensors, and portable items that can measure, store, and transmit information. The IoT connects billions of devices to the Internet and involves the use of billions of data points, all of which need to be secured.

Data points: A discrete unit of information. Any single fact is a data point.

Overview

IoT devices may be business oriented, consumer based, or a hybrid of both. The devices may be company provided or employee owned, such as through a BYOD policy.

Purpose

The purpose of this policy is to establish a defined IoT structure to ensure that data and operations are properly secured. IoT devices continue making inroads in the business world; therefore, it is necessary for PURPLESEC to have this structure in place.

Policy Detail

IoT Device Procurement

IoT devices that are to be used for company operations should be purchased and installed by IT personnel.

Employee-owned IoT devices used for business purposes must be used in accordance with Policy 16, Personal Device Acceptable Use and Security (BYOD).

The use of all IoT devices, whether company provided, or employee owned, should be requested via Addendum A, IoT Device Usage Request Form and submitted to the IT department for approval. Only manager level employees and above may request the usage and/or procurement of IoT devices.

The IT department is responsible for identifying compatible platforms, purchasing equipment, and supporting organization provided and authorized IoT devices.

Cybersecurity Risks and Privacy Risk Considerations

It is important for PURPLESEC to understand the use of IoT because many IoT devices affect cybersecurity and privacy risks differently than IT devices do. Being aware of the existing IoT usage and possible future usage will assist PURPLESEC in understanding how the characteristics of IoT affect managing cybersecurity and privacy risks, especially in terms of risk response.

It is important for PURPLESEC to manage cybersecurity and privacy risk for IoT devices versus conventional IT devices, determining how those risk considerations might impact risk management in general, risk response and particularly mitigation, and identifying basic cybersecurity and privacy controls PURPLESEC may want to consider, adapt, and potentially include in requirements when acquiring IoT devices. The IoT Risk Management Guide contains insight as to the differences in risk between conventional IT devices and IoT devices. This document resides in the IT document storage area.

ADDENDUM A

IoT DEVICE USAGE REQUEST FORM

Date ______________________________

Manager Name ______________________________ Branch ______________________________

Type of Device ____________________________________

Describe the need for this device
____
____
____
____

Date Needed _______________________