



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.



ACCEPTABLE USE OF INFORMATION SYSTEMS

Overview

Data, electronic file content, information systems, and computer systems at {COMPANY-NAME} must be managed as valuable organization resources.

Information Technology's (IT) intentions are not to impose restrictions that are contrary to {COMPANY-NAME}'s established culture of openness, trust, and integrity. IT is committed to protecting {COMPANY-NAME}'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 {COMPANY-NAME}.

These systems are to be used for business purposes in serving the interests of {COMPANY-NAME} and of its clients and members during normal operations.

Effective security is a team effort involving the participation and support of every {COMPANY-NAME} 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 {COMPANY-NAME}. These rules are in place to protect the authorized user and {COMPANY-NAME}. Inappropriate use exposes {COMPANY-NAME} to risks including virus attacks, compromise of network systems and services, and legal issues.

PurpleSec, LLC

Last Updated: April 29, 2021

Sales@PurpleSec.us | [Request A Consultation](#)



ACCEPTABLE USE OF INFORMATION SYSTEMS

Scope

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

All employees, volunteer/directors, contractors, consultants, temporaries, and other workers at {COMPANY-NAME}, 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 {COMPANY-NAME} policies and standards, local laws, and regulations.

Policy Detail

Ownership of Electronic Files

All electronic files created, sent, received, or stored on {COMPANY-NAME} owned, leased, or administered equipment or otherwise under the custody and control of {COMPANY-NAME} are the property of {COMPANY-NAME}.

Privacy

Electronic files created, sent, received, or stored on {COMPANY-NAME} owned, leased, or administered equipment, or otherwise under the custody and control of {COMPANY-NAME} are not private and may be accessed by {COMPANY-NAME} 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.



ACCEPTABLE USE OF INFORMATION SYSTEMS

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 {COMPANY-NAME}. Because of the need to protect {COMPANY-NAME}'s network, there is no guarantee of privacy or confidentiality of any information stored on any network device belonging to {COMPANY-NAME}.

For security and network maintenance purposes, authorized individuals within the {COMPANY-NAME} IT Department may monitor equipment, systems, and network traffic at any time.

{COMPANY-NAME}'s IT Department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

{COMPANY-NAME}'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.



ACCEPTABLE USE OF INFORMATION SYSTEMS

Security and Proprietary Information

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

- Account Management
- Anti-Virus
- Owned Mobile Device Acceptable Use and Security
- E-mail
- Internet
- Safeguarding Member Information
- Personal Device Acceptable Use and Security
- Password
- Cloud Computing
- Wireless (Wi-Fi) Connectivity
- Telecommuting

System level and user level passwords must comply with the Password Policy. Authorized users must not share their {COMPANY-NAME} 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 {COMPANY-NAME} proprietary information only to the extent it is authorized and necessary to fulfill the users assigned job duties.

PurpleSec, LLC

Last Updated: April 29, 2021

Sales@PurpleSec.us | [Request A Consultation](#)



ACCEPTABLE USE OF INFORMATION SYSTEMS

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.

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

All users must report any weaknesses in {COMPANY-NAME} 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 {COMPANY-NAME} 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.



ACCEPTABLE USE OF INFORMATION SYSTEMS

Unacceptable Use

Users must not intentionally access, create, store, or transmit material which {COMPANY-NAME} may deem to be offensive, indecent, or obscene.

Under no circumstances is an employee, volunteer/director, contractor, consultant, or temporary employee of {COMPANY-NAME} authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing {COMPANY-NAME}-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 {COMPANY-NAME}.
- 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 {COMPANY-NAME} 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 {COMPANY-NAME} computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

PurpleSec, LLC

Last Updated: April 29, 2021

Sales@PurpleSec.us | [Request A Consultation](#)

ACCEPTABLE USE OF INFORMATION SYSTEMS

- Attempting to access any data, electronic content, or programs contained on {COMPANY-NAME} 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 {COMPANY-NAME} IT.
- Installing or using non-standard shareware or freeware software without {COMPANY-NAME} IT approval.
- Installing, disconnecting, or moving any {COMPANY-NAME} owned computer equipment and peripheral devices without prior consent of {COMPANY-NAME}'s IT Department.
- Purchasing software or hardware, for {COMPANY-NAME} use, without prior IT compatibility review.
- Purposely engaging in activity that may;
 - degrade the performance of information systems;
 - deprive an authorized {COMPANY-NAME} user access to a {COMPANY-NAME} resource;
 - obtain extra resources beyond those allocated; or
 - circumvent {COMPANY-NAME} 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, {COMPANY-NAME} users must not run spyware, adware, password cracking programs, packet sniffers, port scanners, or any other non- approved programs on {COMPANY-NAME} information systems. The {COMPANY-NAME} IT Department is the only department authorized to perform these actions.



ACCEPTABLE USE OF INFORMATION SYSTEMS

- 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 {COMPANY-NAME}-owned computer, must adhere to all the same policies that apply to use from within {COMPANY-NAME} facilities. Authorized users must not allow family members or other non-authorized users to access {COMPANY-NAME} computer systems.

{COMPANY-NAME} information systems must not be used for personal benefit.



ACCEPTABLE USE OF INFORMATION SYSTEMS

Incidental Use

As a convenience to the {COMPANY-NAME} 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 {COMPANY-NAME} approved users; it does not extend to family members or other acquaintances.
- Incidental use must not result in direct costs to {COMPANY-NAME} 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, {COMPANY-NAME}.
- Storage of personal email messages, voice messages, files, and documents
- within {COMPANY-NAME}'s information systems must be nominal.
- All messages, files, and documents — including personal messages, files, and documents — located on {COMPANY-NAME} information systems are owned by {COMPANY-NAME}, may be subject to open records requests, and may be accessed in accordance with this policy.



ACCEPTABLE USE OF INFORMATION SYSTEMS

Review and Acceptance

All {COMPANY-NAME} staff is responsible for review and acceptance of *Policy 1: Acceptable Use* upon starting work at {COMPANY-NAME} (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.]

Receipt of Acceptable Use of Information Systems

Please sign this form and return it to Information Systems

I have received a copy of the {COMPANY-NAME} 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.

PurpleSec, LLC

Last Updated: April 29, 2021

Sales@PurpleSec.us | [Request A Consultation](#)



ACCEPTABLE USE OF INFORMATION SYSTEMS

I further understand the content of the Comprehensive IT Policy supersedes all policies previously issued. I also understand that {COMPANY-NAME} 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.***

PurpleSec, LLC

Last Updated: April 29, 2021

Sales@PurpleSec.us | [Request A Consultation](#)