EasySec®
CyberSecurity
Consulting Company

ACCEPTABLE USE OF INFORMATION SYSTEMS

EasySec, LLC
Last Updated: March 3, 2025
Office@EasySec.us | Request A Consultation

ACCEPTABLE USE OF INFORMATION SYSTEMS

Overview

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

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

These systems are to be used for business purposes in serving the interests of EasySec and of its clients and members during normal operations.

Effective security is a team effort involving the participation and support of every EasySec 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.

ACCEPTABLE USE OF INFORMATION SYSTEMS

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at EasySec. These rules are in place to protect the authorized user and EasySec. Inappropriate use exposes EasySec 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 EasySec business or interacts with internal networks and business systems, whether owned or leased by EasySec, the employee, or a third party.

All employees at EasySec, 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 EasySec policies and standards, local laws, and regulations.

Policy Detail

Ownership of Electronic Files

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

Privacy

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

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

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

EasySec'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:

- Account Management Policy
- Owned Mobile Device Acceptable Use and Security Policy
- E-mail Policy
- Internet Policy
- Personal Device Acceptable Use and Security Policy
- Password Policy
- Wireless (Wi-Fi) Connectivity policy

System level and user level passwords must comply with the Password Policy. Authorized users must not share their EasySec 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.

ACCEPTABLE USE OF INFORMATION SYSTEMS

Authorized users may access, use, or share EasySec 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.

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

All users must report any weaknesses in EasySec computer security and any incidents of possible misuse or violation of this agreement to their immediate supervisor and/or the 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 EasySec may deem to be offensive, indecent, or obscene.

Under no circumstances is an employee, volunteer/director, contractor, consultant, or temporary employee of EasySec authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing EasySec-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 EasySec.
- 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 EasySec 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 EasySec 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 EasySec 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 EasySec IT.
- Installing or using non-standard shareware or freeware software without EasySec IT approval.
- Installing, disconnecting, or moving any EasySec owned computer equipment and peripheral devices without prior consent of EasySec's IT Department.
- Purchasing software or hardware, for EasySec use, without prior IT compatibility review.
- Purposely engaging in activity that may;
    - degrade the performance of information systems;
    - deprive an authorized EasySec user access to a EasySec resource;
    - obtain extra resources beyond those allocated; or
    - circumvent EasySec 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 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 EasySec-owned computer, must adhere to all the same policies that apply to use from within EasySec facilities. Authorized users must not allow family members or other non-authorized users to access EasySec computer systems.

EasySec information systems must not be used for personal benefit.

I further understand the content of the Comprehensive IT Policy supersedes all policies previously issued. I also understand that EasySec 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:_____