

|  |  |
| --- | --- |
| **Document Name** | Computer Usage Policy |
| **Document Number** | M2010p |
| **Last revised** | August 9, 2022 |
| **Purpose** | To define standards of conduct when employing the use of information technologies available through EZ STAK |
| **Connecting Documents** | Not applicable |
| **Connecting Forms** | Not applicable |
| **Connecting Systems** | Not applicable |

**Computer Usage Policy**

The objective of this policy is to define standards of conduct when employing the use of information technologies available through [EZ STAK]. These technologies include, but are not limited to, computers, computer files, software, as well as electronic mail, voice mail, Internet, and Intranet.

**Computer Usage Policy Details**

The [EZ STAK] expects all employees to use these information technologies solely for business purposes. Employees should not assume that any computer equipment or technologies, such as electronic mail and data are confidential or private. [EZ STAK] (Or its designated representatives) maintains the right and ability to enter these computer systems to access and review any information.

This policy applies to all [EZ STAK] employees, contractors, vendors, and agents with [EZ STAK] owned or personally owned computer or workstation used to connect to the [EZ STAK] network.

Disciplinary action will occur whenever a breach of security or hacking is detected and determined intentional or negligent. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

If you are unsure as to an item’s appropriateness, consult the Information Technology department and/or the CEO.

**Security**

To protect the information contained on [EZ STAK] enterprise network there have been a number or security measures implemented. Each user is issued an account and password. This password will grant the user access to information based on their job requirements and security level.

Your password may not be given to anyone for any purpose. If another user is locked out of IT systems, it is their responsibility to contact IT for remediation. Temporarily sharing your access info is not acceptable. If you believe your password is known by another user, you should change it immediately and notify the Administration Assistant for Corporate Records of this compromise. In some instances, you may require IT to amend your credentials. If you require assistance, please contact your supervisor or the Information Technology Department.

If a person has requested the use of your network account, you may direct them to your supervisor or the Information Technology Department. In addition, using another’s account or representing another user is prohibited. You may be held responsible for any abuse if you knowingly providing access to your account.

Ways in which you can help protect the network are:

* Never give your password to anyone.
* Choose passwords that are not obvious and do not write them down. A good password includes a combination of letters, numbers and symbols that are 9 character or more.

**Fraudulent Use or Behavior**

Users must respect the integrity of computing and network systems; for example, users shall not intentionally develop or use programs that harass other users or infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.

Under no circumstances is an employee of [EZ STAK] authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the [EZ STAK] owned resources. An employee that suspects or is aware of such activity is required to notify their department head and the manager’s office immediately.

Network security is a very serious issue. Tampering with data or attempting to circumvent the flow of data is strictly prohibited.

If a user creates any liability on behalf of [EZ STAK] due to inappropriate use of the network, the employee implicitly agrees to indemnify and hold [EZ STAK] harmless~~.~~

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use. An employee aware of any activity or activity by another employee that violates this policy is required to notify their department head and the Information Technology department immediately.

The following activities are strictly prohibited, with no exceptions:

**System and Network Activities**

* 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 the [EZ STAK].
* Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the [EZ STAK] or the end user does not have an active license is strictly prohibited.
* Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
* Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, personal file sharing, etc.).
* Revealing your account password to others or allowing use of your account by others. This includes family and other household members if work is being done at home. All work taken home must meet the approval of a manager
* Using a [EZ STAK] computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
* Making fraudulent offers of products, items, or services originating from any the [EZ STAK] account.
* Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
* Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not
* an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.
* Port scanning or security scanning is expressly prohibited unless authorized by the Information Technology Department.
* Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
* 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.
* Using a system other than those provided by [EZ STAK] to store files. (Examples include personal DropBox, Sharefile, OneDrive, Google Drive, etc)

**Email and Communications Activities**

* Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
* Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
* Unauthorized use, or forging, of email header information.
* Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
* Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
* Use of unsolicited email originating from within the [EZ STAK]’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by [EZ STAK] or connected via the [EZ STAK]’s network.
* Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

To prevent potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of the [EZ STAK], automatic email forwarding to an address outside the organization is unauthorized unless approved by the Information Technology Department.

**General uses and actions that are also prohibited.**

* Any commercial use or any use for personal gain
* Adding, removing, or modifying identifying network header information (aka "spoofing").
* Attempting to impersonate any person by using forged headers or other identifying information.
* Using a proxy server of any kind (other than the [EZ STAK]’s internal proxy server).
* Using any type of Anonymizer or any other means to mask, hide or modify your identity or activities electronically.
* Using any type of program/script/command or other computer related device to send messages of any kind in place of [EZ STAK] Mail Server. To help prevent the transmission of viruses and other hostile programs, and where appropriate, all electronic messages must use and go through the [EZ STAK] Mail Server.
* Facilitating use or access by non-authorized users, including sharing your password or other login information with anyone.
* Obtain and/or use another user’s passwords without their knowledge and consent.
* Attempt to gain access to files and resources to which you have not been granted permission.
* Try to "crash", or unnecessarily retard, the network or computing systems.
* Make copies of another user’s files without their knowledge and consent.  Print or plot posters and banners under another user’s account.
* Steal, vandalize or obstruct the use of computing equipment, facilities, or documentation.

**Software and Hardware**

*Software Piracy*

The illegal use of software is prohibited. Most Pirating is a result of installing software on a computer without the legal right to do so. To use a computer, program the organization must purchase the program from a reputable source and possess the license and software to use the program. The posting or uploading of copyrighted material without the permission of the owner of such material is also prohibited.

It is illegal to copy software or use software without meeting the above-mentioned criteria and legal action may be taken against those not abiding by the law. If you would like more information or a copy of the law, contact the Information Technology Department.

*Games*

All segments of the computer systems remain the [EZ STAK]’s property and are furnished to employees for business use only. Entertainment using computer games is not permitted.

*Installing and/or downloading Software*

You may not install software onto the computer or onto the network without the permission of the Information Technology Department. You may not download any software without the permission of the Information Technology department. Permission must be obtained prior to beginning the process of downloading software. If you require software not owned by the [EZ STAK], you may arrange to purchase it provided the software is required to perform work related tasks and approved by the Information Technology Department. Software includes but is not limited to scripts and commands.

*Installing computer related hardware*

You may not install hardware without permission of the Information Technology Department. Devices such as wireless access points, storage devices and network hardware may present a security risk or impede operations.

*Viruses*

The threat of a virus infection can arise from downloading files from the Internet, loading data into your computer from a diskette, or running an e-mail attachment. If you question the authenticity of data, you may have the Information Technology Department scan it for viruses. Please note that your computer is not immune from a computer virus, so we encourage you to take caution when downloading information

**Intranet/Internet**

The [EZ STAK]’s Information Technology Department will provide approved staff with the ability to use the Internet as a source of global communication and research. The Internet is a powerful research and communication tool, as such; we must assume responsibility for using it in an appropriate manner.

We must remember to focus only on information contained within the scope of our job functions. The Information Technology department will periodically review the information or sites a user has visited. Any user action that violates the appropriate usage policy may result in revoking network privileges and may lead to legal action.

Pornographic Material and Vulgarity – the posting, uploading, or downloading of pornographic or vulgar messages, photos, images, sound files, text files, video files, newsletters, or related materials is strictly prohibited.

**Email**

*Ownership*

The e-mail system is the property of the [EZ STAK]. All data and other electronic messages within this system are the property of the [EZ STAK]. E-mail messages either composed or received on this system may be considered [EZ STAK] records, depending on their content, and therefore may be subject to Freedom of Information Act requests and other legal disclosure.

*Monitoring and Privacy*

The [EZ STAK] reserves the right to monitor all e-mail messages either composed or received in the e-mail system. It is possible that e-mail sent from the [EZ STAK]’s system can be intercepted on the local system and on the Internet; therefore, the user should not expect any degree of privacy regarding e-mail messages of any type. E-mail messages deleted by the user may be retrievable from the hard drive, backups or the receiving or sending e-mail system.

The [EZ STAK] Mail Server may have the ability to automatically forward messages; unless otherwise approved by the Information Technology department, automatically forwarding any type of electronic mail is prohibited. One example would be setting up a rule to have all your work-related email sent to your private account, such as yahoo or msn.

*Major Points*

* Electronic mail is an important resource for communications and is an essential element in the [EZ STAK]’s daily activities. Aside from increased speed and accessibility, electronic mail allows a certain amount of flexibility not experienced
* through memos or other traditional methods of communication. Because of this, we need to acknowledge the following key points:
* Messages can be forwarded and copied very easily. It only takes a few keystrokes for a personal, and perhaps embarrassing, message to be sent to the wrong people. Good advice is not to send messages that could be damaging if made public or that cover sensitive material.
* Know your recipient. Different people have different ideas of what is acceptable. Find out and respect each person's wishes. Be respectful and exercise good taste. An e-mail account is not a license to abuse or insult people.
* Be considerate of the recipient's time. E-mail messages work best if they're short and to the point.
* Don't send copies of e-mail to people unless they need to be copied. In addition to cluttering up their mailboxes, it can place them in an awkward position, making them feel as if they have to do something with the information. Messages unnecessarily copied to others can be intimidating to the main recipient.
* Unsolicited advertising is not acceptable. The selling of personal services or products toward personal financial gain is prohibited.
* Be aware that e-mail can be archived and, under certain circumstances, may not be secure. Many on-line services and public e-mail providers protect the confidentiality of their subscribers' e-mail, but some companies consider e-mail subject to scrutiny.
* Do not "cry wolf." Avoid "Urgent" or "Priority" unless it really is. Employ capital letters sparingly. Using them for an entire message is perceived by many as SHOUTING and is harder to read.
* In face-to-face conversation, we convey emotion and meaning through facial expressions and vocal inflections. That element of speech is absent in e-mail, so take care when expressing yourself, especially with the use of irony or humor.
* Avoid sarcasm, unless you are sure it will work, and think very carefully before using e-mail to express anger. With e-mail, once it is sent, it's gone. If you are posting a message in a public forum, remember it can be read by a wide variety of people.

*Harassment*

E-mail at work is a privilege, not a right. [EZ STAK] is entrusted with a valuable communication tool that holds endless possibilities. If you receive an e-mail message that is harassing or inappropriate, you are expected to report it in writing to your supervisor, or any department head, and send a copy to the Information

Technology Department

**Remote Access**

The purpose of the remote access portion of this policy is to define standards for connecting to the [EZ STAK]’s network remotely. These standards are designed to minimize the potential exposure to [EZ STAK] from damages which may result from unauthorized use of [EZ STAK] resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, or damage to critical [EZ STAK] internal systems, etc.

It is the responsibility of [EZ STAK] employees, contractors, vendors, and agents with remote access privileges to [EZ STAK] network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the [EZ STAK] network.

General Whitelisted access to the Internet for [EZ STAK] related use through the [EZ STAK] network on computers is permitted for employees. [EZ STAK] employee bears responsibility for the consequences should the access be misused themselves, or by anyone with access to the computer.

**Requirements**

Remote access to the [EZ STAK] network system of any kind must first be authorized by the Information Technology department. Secure remote access must be strictly controlled. Control will be enforced via password authentication or public/private keys with strong passwords. For information on creating a strong password see the Password section of this policy.

[EZ STAK] employees and contractors with remote access privileges must ensure that their [EZ STAK] -owned or personal computer or workstation, which is remotely connected to [EZ STAK] 's network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.

When you are finished accessing [EZ STAK] resources remotely for a particular task, you should promptly disconnect from [EZ STAK] network.

[EZ STAK] employees and contractors with remote access privileges to the [EZ STAK] network must not use non- [EZ STAK] email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct [EZ STAK] business.

All hosts that are connected to [EZ STAK] internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers; the anti-virus software must be always running on the device and must be approved by the Information Technology Department.

Personal equipment that is used to connect to [EZ STAK] networks must meet the requirements of [EZ STAK] -owned equipment for remote access.

Organizations or individuals who wish to implement non-standard Remote Access solutions to the [EZ STAK] network must obtain prior approval from the Information Technology Department.

You are accountable for the activities performed under your logon id and are urged, therefore, to safeguard your passwords, charge numbers and data.

**Terms and Definitions:**

Anonymizer: A privacy service that allows a user to visit Web sites without allowing a visited Web site to gather information about them, such as their IP address.

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

DMZ: De-militarized Zone. A network segment external to the production network.

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device. Examples include Being logged into the network via a local Ethernet connection, and dialing into AOL or another Internet service provider (ISP). Being on a [EZ STAK] -provided Remote Access home network, and connecting to another network, such as a spouse's remote access.

DSL: Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone

Email: The electronic transmission of information through a mail protocol such as SMTP. Programs such as Microsoft Outlook use SMTP.

Forwarded email: Email resent from internal networking to an outside point.

Hacking: Widely used to describe people who gain illegal entrance into a computer system

Intranet: The in-house Web site that serves the employees of the [EZ STAK].

Internet: Global network of computers used to communicate and provide information.

Network: The collaboration of computers and shared electronic information.

Packet sniffer or sniffing: A program running in a network attached device that passively receives all data-link-layer (and other) frames passing by the device's network interface.

Piracy: The illegal copying of software for personal or commercial use.

Sensitive information: Information is considered sensitive if it can be damaging to the [EZ STAK] or its customers' dollar value, reputation, or standing.

Remote Access: Any access to the [EZ STAK]’s network.

Split-tunneling: Simultaneous direct access to a non- [EZ STAK] network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into the [EZ STAK]’s network via a VPN tunnel. VPN

Spamming: Sending copies of the same message to large numbers of newsgroups.

Spam: Unauthorized and/or unsolicited electronic mass mailings.

Unauthorized Disclosure: The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

User: Staff, vendor, or citizen employing the use of the information contained within the computer resources owned by [EZ STAK].

Virtual Private Network (VPN) is a method for accessing a remote network via encrypted "tunneling" through the Internet.

Virus: Executable computer program that can attach itself to an item, such as a computer startup area (boot record), executable file or email. A virus may have a number of objectives – most are usually destructive.

**Acknowledgment and Agreement**

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, acknowledge that I have read and understand the Computer Usage Policy of EZ STAK. Further, I agree to adhere to this policy and will ensure that employees working under my direction adhere to this policy. I understand that if I violate the rules/procedures outlined in this policy, I may face disciplinary action.

|  |  |
| --- | --- |
|  Name: |  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  Signature: |  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  Date: |  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |