

ADMINISTRATIVE POLICY 12-2004

ECONOMIC SECURITY CORPORATION OF SOUTHWEST AREA

Computer Usage, Electronic Mail and Security Policy

Adopted: August 6, 1998

Amended: August 3, 2006

SCOPE

This policy applies to all employees of the agency, contractors, vendors, partners, associates, and all others accessing and/or using the Economic Security Corporation of Southwest Area (ESC) computer network through any means.

TERMS AND DEFINITIONS

Computer hardware, software, and data circuits are provided at great expense by the agency for creating, researching, and processing agency business. By using the company's hardware, software, and networking systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable company policies, as well as City, State, and Federal laws and regulations. Employees are expected to adhere to Internet and computer program use for business purposes appropriate to each employee's specific job duties.

An ESC e-mail address is defined as any e-mail address that is used primarily for business use. This includes, but is not limited to, all yahoo, hotmail, g-mail, or similar free web-based email accounts set up with the intent to use as a primary business account.

GENERAL PROVISIONS

All files created by an employee on the company's time and computers are considered property of ESC.

Any data transmitted, received, printed, copied from or contained in the ESC computer network, including *all* e-mail correspondence, is the exclusive property of the company. The company reserves the right to monitor *all* computer related data and activity on the ESC computer network and any connected devices as needed. This includes but is not limited to Internet usage, electronic messages, AccuTerm data, Excel spreadsheets, MS Word documents, printed data and images, etc. ***Employees have no expectation of privacy for any type of computer transaction whenever accessing a company computer or any part of the ESC computer network either remotely, or when working inside an ESC physical location.***

State of Missouri Law, RSMo. 569.094-569.099

Missouri state law makes unauthorized access and interference with computer systems, computer data, and other computer users illegal. Unauthorized use of passwords and the breach of security of any computer system are illegal.

Employees may not purchase, download, or install software or hardware on the ESC computer network without prior written approval from the Computer Network Manager. Employees are reminded that almost *all* freely downloadable software, including screen savers, games; weather-reporting utilities from the Internet may contain spyware that can become a severe performance and security issue.

The level of network access allowed to any employee will depend on the employee's individual user account permissions

ESC RULES AND REGULATIONS

- Use of ESC's computer system or computer network for illegal purposes is prohibited.
- Occasional personal internet surfing and use of the corporate email system for personal email is acceptable so long as it is not excessive, does not interfere with your normal job duties, and does not violate any part of the ESC computer usage policy. Any problems related to the receipt or delivery of non-ESC company business emails will be evaluated on a case-by-case basis to determine need. ESC does not guarantee delivery or receipt of any emails.
- Yahoo Messenger is the instant messaging software to be for business communication. All other messaging software is prohibited without the approval of the Computer Network Manager, Deputy Director or Chief Executive Officer.
- Chain letter, pyramid selling, and multi-level marketing schemes are prohibited.
- No obscene, threatening, or harassing messages are allowed on the ESC computer network.
- Employees are not permitted to transmit, receive, or retain communications or data that contains obscene, profane, pornographic or threatening language or pictures.
- Always apply normal standards of ethics and conduct while using any ESC computer or while accessing the ESC network.
- E-mail users bear responsibility for his/her e-mail. ESC accepts no responsibility or liability for any actions of the address recipient or user, or for any consequences resulting from use of e-mail messaging.
- Respect the equipment and privacy of employees.
- No person may send a message in such a way that it appears to be sent by another person.
- Using @escswa.org address for the purpose of promoting an election campaign is forbidden.

- ESC attempts to control virus and worm transmission. However, users should not open unknown e-mail attachments.
- It is a grave abuse of the e-mail system if a message is sent that implies the sender can be contacted at an e-mail, postal, or fax address that is not under the direct control of the sender.
- Unsolicited/unnecessary e-mail, commonly referred to as Spam, is advertising material sent without the recipient either requesting or denying receipt of such information or otherwise expressing an interest in the material advertised. Such activity is prohibited.
- Electronic mail bombing is sending multiple e-mail messages, or one or more large e-mail messages, with the sole intent of annoying and/or seeking revenge on a fellow Internet user. This type activity is prohibited.
- When accessing information, exercise care in protecting the confidentiality of the individual(s) for whom the information applies.
- Do not use ESC computers for personal profit or commercial gain.
- Playing games during normal business hours is prohibited.
- Do not install unnecessary programs onto an ESC computer. If in doubt, consult the Computer Network Manager.
- Use password protected screen savers with the screen saver time set to 10 minutes.
- The level of network access allowed to any employee will depend on the employee's individual user account permissions. An employee may not access another employee's login or computer in order to gain a higher level of system access than is granted by their own user account permissions.
- Do not divulge ESC computer account passwords to anyone other than the person to whom the account is assigned without the approval of the Computer Network Manager, Deputy Director or Chief Executive Officer.
- High bandwidth applications are prohibited. These applications slowdown the Internet connection for all employees trying to access the Internet. Bandwidth is defined as "The amount of data that can be passed along a communications channel (our internet connections) in a given period of time". Questions regarding this item should be addressed to the Computer Network Manager.
- No software that allows the trading of copyright materials without the consent of the copyright holder (such as software classified as "peer-to-peer") is allowed.
- Do not look at, copy, alter or destroy anyone else's personal files without explicit permission (unless authorized to do so by law or policy).

EXAMPLE OF ACTIVITIES TO AVOID

- Excessive printing.
- Setting up a personal web server, file transfer site or other unauthorized services.
- Listening to streaming music and/or watching streaming video over the Internet that isn't job related without the approval of the Computer Network Manager.
- Installing applications downloaded from the Internet without the consent of the Computer Network Manager.

- Sending annoying, threatening or obscene messages or email to any other user.
- Knowingly introducing a computer virus to the ESC computer network.
- Abusive use of computer accounts, networks or other resources.

DENIAL OF SERVICE ATTACKS

Denial of service is any activity that prevents a host on the Internet from making full and effective use of their facilities.

MAILING LIST SUBSCRIPTIONS

Never subscribe anyone other than yourself to a mailing list.

SUMMARY

If unsure about any of the above, please contact the Computer Network Manager.

Abuse or failure to adhere to *any* item(s) within this policy will result in disciplinary action. The action taken will depend upon the supervisor's judgment. Punishment can range from loss of Computer and/or Internet privileges to employee termination.

In addition, in extreme cases, violation of these rules could lead to legal and/or civil penalties.



Economic Security Corporation of Southwest Area

P.O. Box 207 • 302 South Joplin • Joplin, Missouri 64802

(417)781-0352 • fax (417)781-1234

EMPLOYEE ACKNOWLEDGMENT

Receipt of ESC Computer Usage, Electronic Mail and Security Policy

I, _____, hereby acknowledge that I have
(Employee Name)

read and understand the ESC agency computer usage and security policy. I agree to obey the guidelines stated in the ESC computer usage and security policy. I understand that failure to comply could result in disciplinary action ultimately leading to and including termination of employment.

Employee Signature

Date

Location

Please return signed and dated copy to Human Resources.

Acknowledgment will be maintained in Personnel File.