East Missouri Action Agency Computer and Network Policy

Purpose

To ensure the appropriate use of East Missouri Action Agency (EMAA) computer and network resources by its employees, independent contractors, and other computer users.

Policy

The computers and computer accounts used by employees are provided to assist them in the performance of their jobs. The computer and network systems belong to EMAA, and should be used primarily for EMAA business purposes.

The following policy, rules, and conditions apply to all users of EMAA computer and network resources and services, wherever the users are located. Violations of this policy may result in the loss of computer and network access and/or disciplinary action, up to and including termination, and/or legal action.

Computer users are governed by the following provisions, which apply to all use of computer and network resources and services. Computer and network resources and services include, but are not limited to, the following: servers, workstations, computers, laptops, mobile devices, software, and internal or external communications networks that are accessed directly or indirectly from EMAA computer facilities. The term "users", as used in this policy, refers to all employees, volunteers, parents, family members, independent contractors, and other persons or entities accessing or using EMAA's computer and network resources and services.

All computer users have the responsibility to use computer resources in an efficient, effective, ethical, and lawful manner, and in a manner that is consistent with EMAA's policies and procedures.

1. Fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating, violent, or unlawful material may not be deliberately sent, received, displayed, or stored on any computer or network owned by EMAA. Any access to sexually explicit and prurient material or to gambling related material is specifically prohibited. Users encountering or receiving such material should immediately report the incident to their supervisor.

2. The computer and network resources and services of EMAA may not be used for the display, transmission, or storage of commercial advertisements, solicitations, promotions, destructive programs, or any other unauthorized purpose. Use of the electronic mail systems to distribute advertisements, jokes, chain letters, or any other personal notices or messages to distribution lists or other groups of more than three people either inside or outside of EMAA is prohibited.

3. Users must comply with all relevant federal and state laws regarding political activities of EMAA's grantees and other publicly funded organizations. EMAA computer and network systems may not be used "...in any manner supporting or resulting in the identification of EMAA with any partisan or nonpartisan political activity or any other political activity associated with a candidate or contending faction or group in an election for public or party office" (Head Start Act, Section 656) or "...for
the preparation, distribution, or use of any kit, pamphlet, booklet, publication, radio, television, or video presentation designed to support or defeat legislation pending before Congress or any State legislature" (Section 503 of Public Law 107-116, and other appropriations acts). In addition, no federal funds, program services paid for by federal funds, EMAA agency-owned equipment, facilities, supplies, or employees on program time may be used for voter participation or lobbying activities.

4. Users must exercise reasonable care to prevent loss or damage to computer hardware, software, and information in their possession. This includes, but is not limited to physical damage or loss of hardware or software and the use of reasonable care to prevent the spread of computer viruses, worms, 'Trojan horses', and other malicious code. Users may not connect, disconnect, alter, repair, move, or otherwise modify any EMAA computer, monitor, printer, router, switch, or other hardware without prior express authorization to do so from the Executive Director, Program Director, Tech Team Member or the current computer consultant hired by the agency. Users must comply with all computer and network related instructions from the Executive Director, Program Director, Tech Team Member or the current computer consultant hired by the agency or designee.

5. Users must not bring any media, such as CDs, DVDs, videos or jump (flash or thumb) drives, from outside sources to use on the computer without receiving prior express authorization to do so from the Executive Director, Program Director, Tech Team Member or the current computer consultant hired by the agency. Users must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property.

6. Users may not use or install software of any kind onto any EMAA computer or network without receiving prior express authorization to do so from the Executive Director, Program Director, Tech Team Member or the current computer consultant hired by the agency. Users must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property.

7. Users should seek to ensure that adequate network bandwidth is available for activities related to the mission of the agency. Users may not access digital audio and video, including streaming media, without the prior express authorization of the Executive Director, Program Director, Tech Team Member or the current computer consultant hired by the agency. The use of peer-to-peer file sharing networks is specifically prohibited.

8. Users must restrict personal use of EMAA computer systems and network resources to scheduled breaks and other non-work hours, except with the permission of their supervisor. This includes, but is not limited to, the use of computer games, chat rooms, Instant Message (IM) systems, and the non work-related use of Internet e-mail, the World Wide Web, and newsgroups. The use of personal, web-based e-mail (*e.g.*, Hotmail, Yahoo! Mail), while not prohibited, is discouraged.

9. Users must not attempt to access network or Internet systems unless specifically authorized to do so by the operators of those systems. Users must not alter or copy a file belonging to another user without first obtaining permission from the owner of the file.

10. Users should never include full social security numbers in correspondence to anyone through electronic means including but limited to e-mail, text and instant messaging.

Security

1. EMAA has the right to take any actions that it believes are necessary to ensure the integrity of its computer and network resources. It may, at the sole discretion of the Program Director or designee, edit or delete any program, document, or other information stored on any computer or network, including data stored on any personal computer owned by EMAA. It also has the sole right to determine the appropriate content for the web site and portal, and to edit or delete any material posted there.

2. Users are responsible for safeguarding their passwords for the system. Individual passwords should not be printed, stored on-line, or given to others. Users are responsible for all transactions made using their passwords. Under no circumstances may users allow anyone but themselves to log on to any computer or network owned by EMAA using their password. Users must not leave their computers unattended without logging off or locking the computer or network.

The following password requirements have been adopted by EMAA:

- Minimum Length - 7 characters recommended
- Maximum Length - 14 characters
- Minimum complexity - No dictionary words included. Passwords will use three of four of the following four types of characters:
  - Lowercase
  - Uppercase
  - Numbers
  - Special Characters
- Passwords are case sensitive and the user name or login ID is not case sensitive.
- Maximum password age – This will be dictated by the requirements of funders, but no greater than 90 days.
- Account lockout threshold - 4 failed login attempts

Password protected screen savers will be enabled and will protect the computer within 15 minutes of user inactivity. Computers will not be unattended with the user logged on and no password protected screen saver active. Users will be in the habit of not leaving their computers unlocked. Users will press the CTRL-ALT-DEL keys and select "Lock Computer".

Administrator passwords will be protected very carefully. Administrator accounts will have the minimum access to perform their function. Administrator accounts will not be shared.

Privacy

1. EMAA has the right, but not the duty, to monitor any and all aspects of the computer system, including employee e-mail, to ensure compliance with this policy. Employees should not have the expectation of privacy in anything they create, store, send, or receive on any EMAA computer.

2. Users grant permission to EMAA to include their name, Internet address, business address, and business telephone number in publicly accessible directories, databases, and documents, including a staff directory on the World Wide Web. All other personal information will be considered confidential, and will not be published or released in any form without written permission.

Confidentiality

All information about clients receiving services from EMAA and staff employed by the agency is confidential. *No* information may be shared with any person or organization outside EMAA without the prior written permission of the family or individual, except as mandated by Missouri Law ("Exceptions to Prior Consent", OAR 581-21-340) and EMAA policy. EMAA staff and volunteers should strive to protect the privacy of families in the program and should view or print confidential family information only when it is necessary to do so to better serve the family. Information concerning personnel employed by the agency will not be viewed or utilized except for official and necessary purposes.

In the matter of smartphones and tablets it is prohibited to save any client information to the physical device. This is to protect the confidentiality of our clients.

Personal email accounts are not to be used on EMAA mobile devices (tablets, smartphones).

Responsibility

EMAA is not responsible for the actions of individual users. This policy may be amended or revised periodically as the need arises.

Users must report all lost or stolen devices first to proper authorities and then to East Missouri Action Agency supervisor immediately.

Statement of Understanding

I have read and will agree to comply with the foregoing policy, rules and conditions governing the use of EMAA computer and network resources and services. I understand that a violation of this policy may result in the loss of computer and network access and/or disciplinary action, up to and including termination, and/or legal action.

Signature _____ Date_____