Missouri Office of Information Technology
Gerry Wethington, CIO

Truman Building, Room 560
301 W. High Street
Jefferson City, MO 65102

573.526.7741 Voice
573.526.7747 Fax

Missouri Office of Information Technology

CyberSecurity Awareness Program	**Document Number:** ITGS0012
	Effective Date: 12/23/2004
	Published By: Office of Information Technology

1.0 Purpose

This document is intended to promote CyberSecurity Awareness for State of Missouri employees and computer system users. It contains the minimum requirements for a state agency's security awareness program.

2.0 Scope

Missouri State Agencies shall provide basic cybersecurity awareness training for all of their employees.

3.0 Background

The State of Missouri is providing greater access, more information, and new services to state employees and citizens. As these capabilities increase, cybersecurity becomes an important issue. The CyberSecurity Awareness Program provides general guidelines on protecting information and computer assets. Agencies may use the following outline, or design their own training program that includes the same elements as this outline.

4.0 References

4.1 Executive Orders

- 03-26 Authorizes the OIT to coordinate information technology initiatives for the state
  http://sos.mo.gov/library/reference/orders/2003/eo03_026.asp
- 02-15 Establishes the Missouri Security Council
  http://www.sos.mo.gov/library/reference/orders/2002/eo02_015.asp
- 03-25 Designates OIT as principle forum to improve cyber security policies and procedures
  http://sos.mo.gov/library/reference/orders/2003/eo03_025.asp

4.2 Cyber Security Committee Report June 3, 2003

4.3 March 30, 2003 ITAB Meeting Minutes
http://oit.mo.gov/itab/minutes/ab_03_04.pdf

5.0 Revision History

Date	Description of Change
12/23/2004	Initial Standard Published

6.0 Definitions

Refer to ITAB Security Glossary and Acronyms:
http://siipc.mo.gov/PortalVB/DesktopDefault.aspx?tabindex=7&tabid=8

7.0 Distribution

This document will be distributed to the following:

Cabinet Members
Elected Officials
State Court Administrator
Senate Administrator
Chief Clerk of the House

8.0 Inquiries

Direct inquiries about this document to:

Office of Information Technology
Chief Information Officer
Truman Building, Room 560
301 W. High Street
Jefferson City, MO 65102
Voice: 573-526-7741
FAX: 573-526-7747

User Security Awareness Training

Table of Contents

OBJECTIVES 4
1. ACCEPTABLE USE POLICY (AUP) 4
2. EXPECTATION OF PRIVACY 4
3. UNDERSTANDING RISKS and THREATS 5
4. REPORTING INCIDENTS 5
5. INTERNET 7
6. EMAIL 7
7. SOFTWARE 8
8. WORKSTATION SECURITY 8
9. LAPTOP/PDA SECURITY 10
10. CONFIDENTIAL INFORMATION 10
11. DATA BACKUP AND STORAGE 10
12. PHYSICAL SECURITY 10
13. USER RESPONSIBILITY 11
CYBERSECURITY AWARENESS TRAINING CERTIFICATE 12
GLOSSARY 13

OBJECTIVES

The State of Missouri is providing greater access, more information, and new services to state employees and citizens. As these capabilities increase, cybersecurity becomes an important issue. This course is designed to provide general guidelines on protecting information and computer assets.

The Computer User Security Awareness Training Certificate will provide a record that you have read and understand the minimum requirements to safeguard state information and assets.

1. ACCEPTABLE USE POLICY (AUP)

All users must safeguard State of Missouri information. Employees and other authorized users should be aware that many electronic documents and communications might be subject to disclosure under the Missouri Open Records Act (Sunshine Law). An even broader range of documents would be subject to disclosure in response to a subpoena issued as a part of a lawsuit or a criminal investigation. Therefore, all users must treat electronic documents and communications with a high level of care.

The information technology resources you are assigned to do your job shall be used for agency purposes. In some agencies, incidental personal use is permissible if the use does not interfere with your job functions. You are strictly prohibited from using the State of Missouri information technology resources and other communications systems in connection with the following activities. This list provides examples of prohibited activities, and should not be considered all-inclusive:

- Engaging in illegal, fraudulent, or malicious conduct;
- Working on behalf of organizations with no professional or business affiliation with the State of Missouri;
- Operating or supporting a private or personal business with state resources;
- Gambling or maintaining betting pools;
- Sending, soliciting or storing offensive, sexually explicit or defamatory material;
- Purposely annoying, harassing or harming other individuals;
- Monitoring or intercepting files or electronic communications of others without authorization;
- Using another individual's account or identity without explicit authorization;
- Violating intellectual property rights;
- Intentionally or negligently disrupting normal network use and service;

Your local agency may have stricter rules on acceptable use. Please refer to agency policy.

Failure to comply with the Acceptable Use Policy may result in a loss of access privileges, an action for civil damages, an action for criminal charges, and/or disciplinary action including but not limited to suspension or dismissal.

2. EXPECTATION OF PRIVACY

State of Missouri employees have no expectation of privacy in regards to their computer activities when using state equipment. Monitoring may be conducted, and therefore, employees should behave accordingly.

3. THREAT DEFINITIONS

See Glossary for more detail.

HACKER:

An unauthorized user who attempts to gain or is successful in gaining access to a system. They are sometimes referred to as crackers or black hats.

MALICIOUS SOFTWARE:

Software intended to perform an unauthorized process that will have an impact on the confidentiality, integrity, or availability of a system. Malicious software includes viruses, worms, trojans, back doors, logic bombs, adware, spyware, and malicious cookies.

SOCIAL ENGINEERING:

The process of convincing you to divulge confidential information without authorization. It includes gaining your confidence by name dropping, intimidation, lies, impersonation, tricks, bribes, blackmail, and threats. It is often built on false pretenses and misidentification.

> Social engineering is extremely effective and the quickest, easiest, most cost-effective way for a hacker to get confidential information.

4. REPORTING INCIDENTS

An incident is an adverse event, or threat of an adverse event, in a computer system. Examples of incidents include the following:

- Attempts (failed or successful) to gain unauthorized access to systems. For example, a hacker trying log onto the network;
- Revealing confidential information to someone not authorized to have it;
- Unwanted disruption or denial of service (an overflow of information that keeps the computer so busy it cannot perform other functions);
- Unauthorized use of a system. For example, using agency equipment for private gain;
- Changes to system hardware or software without permission. For example, mutilating a web site or deleting information.

SUSPICION AND INCIDENT REPORTING:

If you are not sure if something unusual is going on, it is best to report it and have the experts check it out. Reporting suspicious activity can prevent an incident.

Do not answer any questions about your network, your data, or how you access your systems, unless you know the person asking the questions is authorized to do so.

VIRUS REPORTING:

Most of us have encountered a computer virus directly or indirectly already. The greatest danger with computer viruses is that if they go unreported and uncontained, they will continue to spread. Computer viruses can spread quickly and need to be eradicated as soon as possible to limit serious damage to computers and data. You must report a computer virus infestation immediately after it is noticed. Do not attempt to remove a virus or malicious software without first contacting your agency technical support staff.

INTERNAL REPORTING:

This reporting structure is internal to your organization and may include one or all of the following:

- Security department (officers, managers, and staff)
- Information Technology Help Desk
- Your manager
- Information owners
- Department managers
- Information system / network administrator(s)

You should initially report problems internally rather than externally, reducing any adverse publicity or loss announcements.

CENTRALIZED REPORTING:

As part of a comprehensive security program for the State, the Information Security Management Office (ISMO) in the Division of Information Services has implemented an Incident Response Plan and Procedures. (See ITGS0010, The Information Security Management Office (ISMO) Incident Response Plan and Procedures)

TYPES OF INCIDENTS & WHEN TO REPORT- (update to match newest version of IRPP)

What type of incident must I report?

- Attempts (failed or successful) to gain unauthorized access to systems or data;
- Unwanted disruption or denial of service;
- The unauthorized use of a system for the transmission, processing or storage of data;
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction or consent.

When should I report an incident?

Report any incident immediately that meets the above definition and criteria or is suspicious in nature. We encourage primary or secondary contacts for Information Technology Advisory Board member agencies to report all suspicious activity, even if the incident is quite old at the time of reporting. Incident reports that are sent shortly after the incident occurred are the most likely to be of value. This does not imply that an incident report becomes useless after some period of time. Remember a report not only is the first step in recovery but it also helps raise awareness and contributes to the overall information security posture of the enterprise.

EXTERNAL REPORTING-

While internal reporting is to be encouraged and required, external reporting is sometimes necessary. Some incidents may in fact be state or federal crimes. Your agency security department may decide to report incidents to external agencies. External reporting agencies include:

- Law enforcement / police,

- State Attorney General,
- Office of Homeland Security,
- FBI,
- External auditors.

INTERFERING WITH INCIDENT REPORTING:

You should never attempt to interfere with, prevent, obstruct, or dissuade another employee from reporting a suspected information security problem or violation. Any form of retaliation against an individual reporting or investigating information security problems or violations is prohibited.

5. INTERNET

The State of Missouri connection to the Internet should be properly used. Personal Internet use may be authorized, but you must consult your departmental policy to confirm this. When authorized, employees should only use the Internet on a limited basis as long as it does not detract from employee tasks. For a more detailed explanation of proper Internet use, please see item 1, Government Use of Computers.

Improper use of Internet resources can result in loss of productivity, create legal liability, cause the loss or destruction of records, and embarrass employees and the agency. Frequent personal use exposes the state network to increased risk. Unauthorized software downloads often contain viruses and other malicious software that can damage computer systems. Therefore, only software approved by your agency may be loaded and/or installed on your assigned equipment.

Downloading and uploading of software that is protected by a license agreement may only be done in strict compliance with the license agreement and applicable policy. Be aware that freeware and shareware applications may not be free for government use. All licensing agreements shall be followed thoroughly. Prior to downloading software, coordinate the activity with your agency's technical and security staff. (See ITGS0004 – Software Piracy - Software License Restrictions and Provisions.)

6. EMAIL

You must not email confidential information unless you encrypt the message. It is your responsibility to confirm the confidentiality of each email message you send. Assume that any message or information sent using the Internet is available to the public. A good way to think of unencrypted email is as a postcard written in pencil. You don't know who actually sent it, who read it along the way, or who erased part of it and wrote in what they wanted it to say.

You should not open email that is of a questionable nature, such as containing an unusual attachment, a message from an unknown sender, or unexpected email. Delete a questionable message without opening it, or call your Help Desk. When opening attachments, macros should be disabled. In addition, the Auto Preview and Preview Pane features should be turned off. If you have any questions regarding the validity of an email you have received, contact your Help Desk. If you receive questionable or unexpected email from someone you know, ask the sender to validate the message.

Depending on your agency's policy, occasional email of a personal nature may be sent and received as long as it does not disrupt operations, detract from work tasks, or otherwise violate departmental or state policy.

EMAIL GUIDANCE:

- Never put confidential information in an email message unless the message is encrypted. Unencrypted email can be intercepted by anyone.
- If you forward or reply to a message you have received, do not change the wording of the original message.
- Never send chain letters.
- Use professional language and courtesy when composing emails.
- Be cautious of scams and hoaxes. If it sounds too good to be true, it is. Do not forward it on to others.
- Do not send insulting or abusive messages, even if provoked.
- Never send, solicit or store offensive, sexually explicit, or defamatory material.
- Be careful when addressing email – know to whom you are sending.
- Remember that the recipient's culture, language, and humor may have different points of reference than your own.
- You are representing the State of Missouri and your agency when sending email, so act accordingly.

7. SOFTWARE

Before you install any software, especially shareware or freeware from any source, obtain the necessary approval. You need to coordinate with your departmental Help Desk in order to install software. Scan approved software for viruses and spyware prior to installation.

Only obtain software from trusted source sites, and always scan downloaded software for viruses, etc.

Anti-virus software should be installed on all desktops, portable computers and personal digital assistants (PDA). You should make every attempt to limit the exposure of computers to viruses and other malicious programs.

You should not change the software settings on your machines. If you think the settings are incorrect, contact your departmental Help Desk or technical personnel.

Software patches and security settings on client system: This is normally a centrally maintained function. Otherwise, follow agency procedure.

Only software officially supported and/or allowed for your agency is acceptable on agency systems.

8. WORKSTATION SECURITY

UNATTENDED WORKSTATIONS:

You are responsible for keeping your computer secure. This includes physically securing the computer hardware, as well as controlling access to your network and information systems.

To prevent unauthorized users from using your workstation, turn it off or lock it every time you leave your desk. You can unlock the workstation with your password. In addition, you should have a password-protected screensaver enabled on your computer to be activated after no more than 15 minutes of inactivity.

Log out of your workstation at the end of each day. If your agency wants your workstation left on, make sure that it is locked.

USER ID and PASSWORD:

Your password is like a personal key that provides access to your network, computer systems and applications. When combined with your unique user ID, it gives you specific permissions and capabilities.

You are responsible for all activity performed by your user ID, so it is very important that you never share your password with anyone, including your supervisor. If you know or suspect that your password has been compromised, change it immediately.

Select passwords according to the following guidelines:

- Passwords shall be at least 7 characters in length.
- Password shall contain characters from at least three of the following four categories:
    - English Uppercase Alphabetic (A - Z)
    - English Lowercase Alphabetic (a - z) (applies to PC/Networks only)
    - Numeric Base-ten digits (0 – 9)
    - Special characters (e.g., the “at” sign [@], pound sign [#], asterisk [*], etc.)
- Passwords are not to be your name, address, date of birth, username, nickname, or any term that could be easily guessed by someone who is familiar with you.
- Passwords are not to be related to your job or personal life, e.g., not a license plate number, spouse's name, telephone number, etc.
- Passwords are not to be dictionary words or proper names, places or slang. Use the first letters of a phrase instead.
- Passwords may not contain all or part (3 or more sequential characters) of your account or login name.
- Passwords shall not contain characters that do not change combined with characters that predictably change. For example, do not choose passwords like "x345JAN" in January, "x345FEB" in February, etc., or identical or substantially similar to passwords you previously chose.
- Passwords must not be written down, or recorded on-line unless encrypted.
- Passwords must be different for your agency (internal) and non-state (external) networks and systems, such as your local Internet service.
- Passwords must be changed at least every 90 days with no repetition of recent passwords.
- A default or initial use password set for you by a system administrator must be changed immediately.
- If the system asks if you want to save your password, you should refuse.

VIRUS and SPYWARE PREVENTION:

Your agency must install anti-virus software on your workstation, which may include an automatic update feature. Your agency may also install anti-spyware or firewall software. Do not disable or remove any software or device that is designed to protect your workstation from attacks or malicious software.

USE OF MODEMS:

You must not use a modem or other device to connect to a remote system, such as an outside Internet provider, while connected to your agency network. Do not allow anyone to dial into your networked computer. Do not use any communication device, such as a modem, or wireless network card, unless first approved by your agency technical group.

9. PORTABLE COMPUTER SECURITY

Portable computing devices include laptop or notebook computers, and Personal Digital Assistants (PDAs). Follow the same security rules for portable computing devices as you would for desktop workstations, with the following additions:

- Confidential data files and applications on portable computing devices must be protected using encryption and password protection
- Portable computing devices not owned by your agency must not be connected to state networks or systems without prior approval from appropriate technical staff.
- Immediately report missing or stolen equipment to your agency.

10. CONFIDENTIAL INFORMATION

Information is classified as either “PUBLIC” or “CONFIDENTIAL.” Confidential information must be protected at all times, whatever the type of media. Protection includes the use of encryption, alarmed facilities, safes, etc.

Printouts of confidential information should be destroyed properly, such as shredding, pulverizing, etc.

11. DATA BACKUP AND STORAGE

All information that is critical should be backed up daily. If the information is confidential, it should also be encrypted when stored/saved on fixed disks, tape, or removable media.

Save Important files to a network server that is backed up daily or on a disk kept in a secure location Users are responsible for ensuring that data stored on the local drives of their equipment is backed-up on a periodic basis, either automatically through the network or remotely with tape drives or similar equipment.

12. PHYSICAL SECURITY

All entrances to areas where confidential information or information technology resources are located should be locked, secured, alarmed, or monitored in some fashion. Do not prop open doors to restricted access areas. Do not allow anyone to follow you through restricted doors ("tailgate").

If identification (ID) badges are required in your department, do not admit other people to the facilities unless they display the appropriate picture ID or agency-issued badge. Personnel from outside your agency who display state-issued ID badges should be considered visitors. Remember to display your state-supplied picture ID badge at all times while in facilities that require it.

Keys and Access Cards are to be used only by the person to whom they are issued. Do not loan out your keys or access cards, and if they are lost or stolen, report it immediately.

If you work after business hours, do not enter offices or other areas where access is not essential to complete your duties.

13. USER RESPONSIBILITY

Adhere to agency standards of conduct and behave in an ethical, professional, and trustworthy manner.

Do not attempt to override technical or management controls (i.e., carrying sensitive data home on a floppy disk without prior approval, etc.).

Do not remove or override virus protection software on your workstation.

Use only systems, software, and data for which you have authorization.

Report security incidents to appropriate officials.

Protect confidential information from disclosure as required by your agency.

Protect your passwords from access by other individuals.

Change passwords frequently, as required by your agency.

Do not remove information technology resources from agency premises unless authorized.

Do not connect non-agency equipment to agency networks without authorization.

Do not use agency facilities and connections to make unauthorized connections to, break in to, or adversely affect the performance of other computer systems.

CYBERSECURITY AWARENESS TRAINING CERTIFICATE

ACKNOWLEDGEMENT

I acknowledge that I have completed the CYBERSECURITY AWARENESS TRAINING.

I understand that this security awareness training is designed to complement, and not replace, my reading and compliance of my agency's security policies, standards, processes, and procedures. I also understand that the written agency security policy takes precedence over any policy or procedure presented in this training program, and I am subject to and expected to comply with all of the security policies and procedures as detailed in those agency security policies, standards, processes, and procedures.

Employee Signature	***Supervisor Signature***
Employee Name (Printed)	Supervisor Name (Printed)
Date	Date

Place the original signed form in the employee's personnel file.

GLOSSARY

Access Control

Security control designed to permit authorized access to an information system or application.

Adware

Any software application in which advertising banners are displayed while a program is running. It usually includes code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge.

Agency

For the purposes of this document, a generic term that refers to a state government entity.

Asset

Something of value such as an application, system, hardware, software, or data.

Availability

The information technology resource (system or data) shall be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes.

Back Door

Hidden software or hardware mechanism used to circumvent security controls.

Computer Security

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Confidentiality

Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Cookie

Data exchanged between a web server and a browser (a client of the server) to store information on the client side and retrieve it later for server use.

CyberSecurity

The protection and defense of Cyberspace, a critical infrastructure made up of digital information that is electronically communicated. CyberSecurity encompasses the people, processes and techniques for protecting and defending cyber assets, so that they are available to authorized users and cannot be compromised by unauthorized individuals.

Hacker

Unauthorized user who attempts to or gains access to a system.

Information

Any communication or representation of knowledge in any medium or form.

Information Owner

Person responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains ownership even when the data/information are shared with other organizations.

Integrity

The assurance that information has not been changed accidentally or deliberately, and that it is accurate and complete.

Intellectual Property

Creative ideas and expressions of the human mind that possess commercial value and receive the legal protection of a property right. The major legal mechanisms for protecting intellectual property rights are copyrights, patents, and trademarks.

Interconnected System

Any system that is connected to another system or network.

Logic Bomb

Resident computer program triggering an unauthorized act when certain conditions are met in an information system.

Logical Access Controls

The system-based mechanisms that limit access to information system resources.

Malicious Cookie

A cookie that performs an unauthorized function on an information system.

Management Controls

Controls that focus on the management of the information system and the management of the risk.

Policy

Senior management directive to establish standards of behavior and assign responsibilities.

Procedures

Documentation of approved processes.

Risk

The possibility of harm or loss to any software, information, hardware, or resource.

Sensitive Information

See confidentiality.

Spyware

Files that allow unknown parties to monitor your browsing activity. Surfing the Internet, reading infected email, downloading music or other files can infect your PC with spyware without the user's authorization or knowledge.

System

A set of processes, communications, storage, and related resources

Technical Control

Focuses on security controls that the computer system executes.

Threat

An event or activity, deliberate or unintentional, with the potential for causing harm to an IT system or activity.

Trojan

Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information.

Virus

A hidden, self-replicating section of computer software, usually malicious, that spreads by infecting another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. The symptoms of virus infection include such things as considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.

Worm

A computer program that can run independently, can propagate a complete working version of itself onto other computers, and may keep a computer so busy spreading the worm that the computer cannot perform other functions. The symptoms of worms include such things as considerably slower response times and programs not being able to start.