Section-02 Information Management	OP-021001	Page: 1	Effective Date: 09/11/2017
Internet Standards	**ACA Standards: 2-CO-1C-04**		
Joe M. Allbaugh, Director **Oklahoma Department of Corrections**	**Signature on File**		

Department of Corrections Internet Standards

The purpose of this procedure is to identify the circumstances under which Oklahoma Department of Corrections (ODOC) employees may access Internet through state facilities, be identified as State of Oklahoma employees, and define what ODOC considers acceptable use and conduct once an employee is connected to the network. This procedure communicates the agency's expectations with respect to what is, and is not, "acceptable use" and to minimize the risk of inappropriate behavior on the network. (2-CO-1C-04)

I. Overview of the Internet

Although the Internet represents a potentially valuable resource, it also exposes the ODOC and its employees in an unprecedented and highly visible fashion. The Internet is a public forum, as opposed to a private or secure network. The state of Oklahoma may be held accountable for abusive, inappropriate, or unethical behavior of employees accessing the network from state facilities. The protection of proprietary information, the isolation and security of internal systems and the

productivity of the work force are also of the utmost importance. All aspects of ODOC's Internet presence must be carefully managed to ensure that the State of Oklahoma's image is properly protected, its liability is limited and that access and use of the Internet by ODOC's employees is suitable for business purposes and accomplished in a cost-effective manner.

A. Internet Privilege

Internet services are provided by the State of Oklahoma to support open communications, the exchange of information and the opportunity for collaborative, government-related work. ODOC encourages the use of electronic communications by its units and employees. Although access to information and information technology is essential to the mission of our agency, use of OneNet/Internet services is a revocable privilege.

B. Employee Compliance

Employees will make a reasonable effort to inform themselves of this procedure and acceptable and unacceptable uses of the Internet in general. The burden of responsibility is on the user to inquire as to acceptable and unacceptable uses prior to use.

II. Employee Use

Misuse or abuse of agency computer systems for tasks of a personal nature is prohibited.

A. Employee Etiquette

Employees should know and follow the generally accepted etiquette of the Internet. For example:

1. Use civil forms of communication;

2. Respect the privacy of others;

3. Respect the legal protection provided by copyright and license to programs and data;

4. Respect the privileges of other users; and

5. Respect the integrity of computer systems connected to the Internet.

B. Employee Agency Consideration

Employees will avoid uses of the network that reflect poorly on the ODOC or on the State of Oklahoma.

C. Employee Ethical Behavior

Users should remember that existing rules, regulations and guidelines on the ethical behavior of ODOC employees and the appropriate use of state resources also apply to the use of electronic communications systems such as the telephone, web and e-mail access as provided by the State of Oklahoma.

III. Information Exchange

A. Acceptable Uses

Acceptable uses include but are not limited to:

1. Communication and information exchange directly related to the mission, charter, or work tasks of ODOC;

2. Communication and exchange for professional development, to update training or education, or to discuss issues related to the user's ODOC activities;

3. Use in applying for or administering grants or contracts for ODOC research or programs;

4. Use for advisory, standards, research, analysis, and professional society activities related to the user's work tasks and duties;

5. Announcement of new laws, procedures, policies, rules, services, programs, information or activities; or

6. Any other governmental administrative communications not requiring a high level of security.

B. Unacceptable Uses

Unacceptable uses include, but are not limited to:

1. Use of the Internet for any purpose which violates a federal or state law;

2. Use for any for-profit activities unless specific to the charter, mission, or duties of ODOC;

3. Use for private business, including commercial advertising;

4. Use for access and/or distribution of indecent or obscene material;

5. Use of the Internet to access websites containing visual

representations that contain actual or simulated sexual activity to include intercourse, sodomy (oral or anal), bestiality, sadomasochism, and child pornography is strictly prohibited and will result in termination in accordance with OP-110215 entitled "Rules Concerning the Individual Conduct of Employees";

6. Use for access to and/or distribution of computer games that have no bearing on the agency's mission. Games that help teach, illustrate, train, or simulate agency-related issues may be acceptable;

7. Use of Internet services to interfere with or disrupt network users, services, or equipment;

8. Use to seek out information, distribute information, obtain copies of, or modify files and other data, which are private, confidential, or not open to public inspection or release;

9. Use to copy software, electronic files, programs or data without a prior, good faith determination that such copying is permissible. Any efforts to obtain permission should be adequately documented;

10. Users misrepresenting themselves as other persons either on the Internet without the express consent of those other persons. Users will not circumvent established policies defining eligibility for access to information or systems;

11. Intentionally developing programs designed to harass other users, or infiltrate a computer or computing system, and/or damage or alter the software components;

12. Use for fund raising or public relations activities not specifically related to state government activities; or

13. Allow inmate/offender access to Internet, except for educational or vocational testing under the management and control of an authorized instructor. Testing access will be site specific, under the direct supervision of an authorized instructor, with no access to the Internet beyond the test site. Physical and logical security will be imposed to restrict any unsupervised inmate/offender access to any computer connected to the Internet.

C. Additional Guidelines

1. Any software/files downloaded shall be virus checked prior to use.

2. Passwords associated with ODOC information systems will only be used on the authorized ODOC system. When setting up an account

on a non-ODOC information system, passwords should be chosen that are different from ones used on the ODOC systems.

a. Use of the same password for both local and remote Internet-accessed systems is prohibited. If the password used at the Internet-accessed remote site were to be compromised, the different password used locally would still be secure.

b. Passwords should not be so obvious that others could easily guess them. Passwords should be changed at least every 60 days.

3. A reasonable attempt will be made to complete the logoff or other termination procedure when finished using a remote, Internet-accessed system or resource. This will help prevent potential breaches of security.

4. Electronic mail sent or received on the Internet cannot be expected to be secure.

5. Employees utilizing electronic mail will ensure the electronic mail signature block does not include graphics, logos, clip art, quotes or any additional sayings. The signature block will include the employee's name, title, work unit, work address, office phone and fax number. Default Microsoft Outlook settings for font, styles, colors and backgrounds will be used in both the body of the email and the signature blocks. Messages containing confidential inmate/offender or staff information may only include the following disclaimer statement:

   DISCLAIMER - This electronic transmission and any attachments may contain confidential, proprietary, or protected information, including but not limited to law enforcement sensitive information, medical information protected by federal and state privacy laws, information that is protected by the attorney-work-product rule, or communication that is subject to the attorney-client privilege. It is intended solely for the named recipient(s). If you have received this electronic transmission or any attachments in error, please contact the sender immediately and destroy all copies of the original message and any attachments. If you are not the intended recipient or their agent, you are hereby notified that any review, dissemination, distribution, or duplication of this electronic transmission and any attachments is strictly prohibited. Please note, all electronic transmissions and any attachments sent to or from a public body are subject to the Oklahoma Open Records Act and may be disclosed to the public.

6. The Internet connection is a shared resource. While routine electronic mail and file transfer activities will not normally impact other users, large file transfers and intensive multimedia activities will impact the

service levels of other users. Users contemplating file transfers over 10 megabytes per transfer or interactive video activities should be considerate of other users, and schedule these activities early or late in the day or after business hours. Such file transfers should be for work related business only and not for personnel use.

7. Users should avoid being drawn into discussions where disclaimers such as "this represents my personal opinion and not that of my agency or the State of Oklahoma" need to be used.

8. The sites visited on the Internet can capture the addresses of those who visit the site.

IV. Non-ODOC and Non-State Employees

In the event non-state or non-ODOC employees require access to state provided Internet services, the ODOC coordinating authority shall submit the request to the Information Technology (IT) Unit. The IT Unit shall determine the method and level of access that is granted. Acceptable use by non-state and non-ODOC employees working for the State of Oklahoma is the responsibility of the coordinating authority. The coordinating authority is to provide those personnel who use state of Oklahoma OneNet/Internet services with this information. Notification responsibilities in the event of separation of service or transfer to a position no longer requiring system access are to be reported as outlined in this procedure in order to maintain system security.

Volunteers may be granted Internet access only with the approval of the facility/district/unit head and the Religious and Volunteer Services Coordinator.

V. Unit and Supervisor Responsibilities

A. Non-Compliance

1. Employees are responsible for their compliance with the provisions outlined in these procedures and facility/district/unit heads are responsible for investigating non-compliance.

2. When an instance of non-compliance with this procedure is discovered or suspected, the facility/district/unit heads will proceed in accordance with OP-110415 entitled "Progressive Disciplinary Procedures." Suspension of service to users may occur when deemed necessary to maintain the operation and integrity of the State of Oklahoma network. User accounts and password access may be withdrawn without notice if a user violates the acceptable use procedure.

3. Criminal or civil action against users may be appropriate where federal or state laws are violated.

B. Responsibility

Facility/district/unit heads are responsible for establishing and maintaining practices and programs in support of this procedure, as well as being responsible for adherence to the requirements of this procedure. Adherence includes:

1. Publishing and implementing guidelines for their area;

2. Reviewing, verifying, processing, and recording all employee and non-ODOC requests for Internet access;

3. Enabling employee access when approved. By approving such a request, it is agreed to:

   a. Acquire hardware or software that is necessary to enable access to the Internet;

   b. Request access authorizations from IT; and

   c. Assure that the employee approved for access has read and understands this procedure and requirements.

4. Enforcement of Standards

   a. Upon admission or discovery of abuse by an employee, appropriate progressive disciplinary action shall be taken.

   b. Upon reasonable suspicion of use for personal profit or accessing of pornographic materials, the information shall be forwarded to the Office of Inspector General for investigation.

C. Notification

Within two business days of an authorized employee, non-ODOC employee, non-state employee, or volunteer's death, disability, or termination, the facility/district/unit head is responsible for notifying the IT Help Desk of the need to terminate access or change the user information.

VI. Statewide Administration

A. IP Addresses and Domains

IT has the responsibility to properly manage all Internet addressing and assignments within the assigned range for the ODOC. This includes the central node and peripheral nodes using this license. This responsibility includes the proper management of:

1. Statewide security;

2. Routing topologies; and

3. Transport levels and traffic monitoring.

B. Orientation

IT will provide basic orientation for managers and supervisors who carry the responsibility for overseeing the use of the Internet and assuring compliance with these procedures within their affected areas.

C. Administrative Issues

IT will assist with administrative issues that may impact the delivery or access to/from the Internet.

D. Social Networking and Social Media

The State of Oklahoma Social Networking and Social Media Standards, Development Methodology, and Guidelines are published at the following URL:http://www.ok.gov/cio/documents/isd_SNSMDevelopmentMethodology_1.0.doc and ODOC personnel shall adhere to the following standards and guidelines:

1. The director of Communications shall be responsible for:

   a. Initiating and moderating all ODOC social networking and media;

   b. Ensuring all open records and records retention requirements are met;

   c. Establishing and maintaining all ODOC social networking and media accounts;

   d. Ensuring all ODOC social networking and media meets the state standards; and

   e. Providing all account information (user id, password, etc.) to the IT Unit security officer.

   f. Establishing and maintaining the social networking and media links on the ODOC webpage in accordance with state standards and guidelines; and

g. Securely storing ODOC social networking and media account information.

VII. References

Policy Statement No. P-020700 entitled “Oklahoma Department of Corrections Information System”

OP-110215 entitled “Rules Concerning the Individual Conduct of Employees”

OP-110415 entitled “Progressive Disciplinary Procedures”

Oklahoma OneNet Acceptable Use Policy

State of Oklahoma, Information Security Policy, Procedures and Guidelines

State of Oklahoma Social Networking and Social Media Standards, Development Methodology, and Guidelines

VIII. Action

The region/division/unit head is responsible for compliance with this procedure.

The director of Technology and Emergency Operations is responsible for the annual review and revisions.

Any exceptions to this procedure will require prior written approval of the agency director.

This procedure is effective as indicated.

Replaced: Operations Memorandum No. OP-021001 entitled “Department of Corrections OneNet/Internet Standards” dated December 3, 2014

Deleted: OP-021001 Revisions-01 dated March 31, 2016

Distribution: Policy and Operations Manual
Agency Website