

**PRISONER ACCESS TO INTERACTIVE COMPUTER SERVICES:
Report to the U.S. Attorney General**

**Constance Clem
LIS, Inc.**

April 1999

**National Institute of Corrections
Information Center
Longmont, Colorado**

Contents

Project Overview 1

Findings in Brief 1

Project Findings 2

 Current Agency Practice 2

 Statutory Restrictions on Access 3

 Correctional Policies 3

Conclusion 7

Appendix A. State Statutes and Correctional Agency Policies on Inmate Access to Interactive Computer Systems

Project Overview

This research was undertaken by the National Institute of Corrections (NIC) pursuant to Title VIII of H.R. 3494, the Protection of Children from Sexual Predators Act of 1998, “Restricted Access to Interactive Computer Services.” Among its other provisions, that act directed the U.S. Attorney General “. . . to determine to what extent each State allows prisoners access to any interactive computer service and whether such access is supervised by a prison official.” The legislation specifically described an occurrence in a state prison system in which an inmate was found to be distributing child pornography via the World Wide Web.

For purposes of the research, an “interactive computer service” was defined as “any computer resources, such as the Internet, World Wide Web, electronic bulletin board systems, e-mail, listservs, chat rooms, pagers, voice mail, computer terminal emulation, facsimile, electronic imaging/video transfers, file transfers, external printing, or similar, which facilitate direct or indirect communications between inmates and external individuals or entities outside a controlled correctional environment and supervision.” Excluded from the definition were computers that provide policy, legal, educational, or training resources via CD-ROM, computer terminals, and/or local computer networks, provided that such a system does not include the specific interactive capabilities identified.

To conduct the research, the NIC Information Center distributed a written survey to state departments of corrections (DOCs), obtaining responses from all 50 states and the District of Columbia Project staff contacted the survey respondents in some DOCs by email or telephone to clarify or update the information received.

Anecdotal information was also obtained via an Internet listserv managed by the Correctional Education Association. Though postings from correctional agency staff to this listserv were not considered formal communications for purposes of this research, they provided useful corroboration of findings combined with an operations-level perspective on agencies’ conflicting concerns about potential programmatic benefits and security.

Findings in Brief

The study found:

- DOCs in only two states-South Carolina and Washington-reported that any inmates have access to interactive computer systems. In each of these DOCs, small numbers of inmates have controlled access to interactive systems in work settings.
- Half the DOCs (25 agencies) indicated that their agencies have placed some type of restriction on inmates’ access to interactive computer systems. Policies in at least nine agencies specifically restrict or prohibit inmate access to computers with telephone, modem, or Internet connections.

- The Minnesota DOC was the only agency to report that a state legislature has passed legislation addressing inmates' access to interactive computer systems. Bills have been introduced in other states but either were unsuccessful or were pending action at the conclusion of this project.

Project Findings

Current Agency Practice

Is interactive access available to inmates?

Correctional systems are nearly uniform in denying inmates access to interactive computer systems. DOCs in only two states-South Carolina and Washington-reported any inmate access to interactive computer systems. In each of these DOCs, controlled access is provided to inmates in job program settings:

- In one South Carolina prison industry program, inmate workers who package products for shipment use a computer connection for exchanging inventory information with the private-sector manufacturer. There is no connection with the DOC's computer system. The manufacturer provides the computer system, including assurance of computer security compliance, and has assumed all liability for the program.

A second South Carolina private work program uses inmates to make travel reservations for corporate clients. The telephone system provided for this program takes only inbound calls. The inmate workers access an online reservations system that has been modified with special protocols and security add-ons. Inmates do not see or enter credit card data. Their work is monitored by correctional and civilian staff in the work area and a civilian who monitors workers' computer screens and telephone calls. Inmates are prevented from removing any papers or other work materials at the end of their work day. The private operator has assumed all liability for the program.

- In the Washington State and South Carolina DOCs, inmate workers in correctional industry programs can send product information to customers by fax. The Washington system uses a pre-programmed dialer.

Other correctional systems are using technologies such as local area networks and stand-alone personal computer (PC) workstations equipped with CD-ROMs to provide educational and training opportunities to inmates while avoiding the use of computers with outside interactive capabilities.

Statutory Restrictions on Inmate Access

Do state statutes prohibit access to interactive computer systems?

One DOC, in Minnesota, reported the passage of legislation restricting inmates' access to interactive computer systems. (The complete text of the statutes is provided in Appendix A.)

- Minnesota Statute 243.556, 1997, states, "No adult inmate in a state correctional facility may use or have access to any Internet service or online service, except for work, educational, and vocational purposes approved by the commissioner."
- Minnesota Statute 243.055, 1997, defines conditions and usage restrictions that may be imposed on offenders on parole, under state probation supervision, and in supervised release programs to restrict or monitor their access to the Internet or other online services.

In the majority of states (31 states), survey respondents reported that no legislation has been introduced that would restrict inmates' access to interactive computer systems. An additional 14 respondents did not indicate whether relevant legislation has been considered. Relevant legislation has been unsuccessful in Iowa.

According to survey respondents, bills had been introduced in the current legislative session in two (2) states at the time of the survey. These states include Ohio and Wisconsin.

Correctional Policies on Inmate Access

Do correctional agency policies prohibit access to interactive computers?

Twenty-five (25) DOCs gave information on current prohibitions.

Responses from nine (9) DOCs indicated that their agencies have explicit prohibitions against inmate access to the Internet, to modem-equipped or telephone-connected computers, or to other forms of interactive computer technology. Copies of available policies are included in Appendix A.

- In the Florida DOC, policy and procedure directive 4.08.10 IV D states: "No inmate or other offender under supervision of the Department shall be allowed access to the Department's Internet capability."

Louisiana DOC regulations state, "No offender in the custody or supervision of the Department is to have access to state-owned equipment that is capable of accessing the Internet or using e-mail." (Regulation No. A-05-007, June 12, 1998.)

- Policy 303.040 of the Minnesota DOC, dated November 1, 1998, states that offenders may only use state electronic equipment for authorized educational, vocational, or work purposes. Offenders are not permitted access to the Internet, nor are they permitted to obtain access to the Internet through third parties.

The New Jersey DOC's June 1998 microcomputer policy on Internet access states, "Inmates will not access PCs with Internet capabilities in any manner and are not permitted to view screens without the written permission of the Manager, Office of Information Technology, or a designee."

The Ohio DOC's policy 112-01, effective January 2, 1997, states, "Inmates will not have access to modems, dial-up lines, file servers, network software or any other data communications equipment that is part of a Local or Wide Area Network," except for "approved Ohio Prison Industries WAN/LAN systems including CADD and data entry systems" or other exceptions approved in writing by the DOC director.

- The Pennsylvania DOC Policy 6.3.30, effective January 19, 1999, states that inmate computers cannot be connected to a network outside of the educational programming area or to any telephone line.
- Washington State DOC Policy no. 280.925, Offender Access to Electronic Data, effective December 31, 1996, prohibits "direct access, either physically or logically, to information technology systems that will allow access to any outside or non-local electronic media, such as, but not limited to, mainframe applications, Internet, electronic bulletin boards, E-Mail, or on-line services." Policy no. 280.820, Internet Access, effective June 1, 1998, further states that no inmate or other offender under the supervision of the Department shall be allowed access to the Department's Internet capability.

Policies in five (5) states prohibit inmates from accessing computer networks, effectively eliminating their access to the Internet and any other connected interactive systems. Policy text was provided by four (4) agencies and is included in Appendix A.

- The Connecticut DOC's Administrative Directive 4.6, Oct. 1, 1998, states: "Inmates shall not use any computer that is connected to a network of any kind. Inmates shall be prohibited from using computers except when necessary for specific education or work assignment, in accordance with Administrative Directive 10.1, Inmate Work and Pay Plan. No inmate shall be allowed personal use of a computer for any reason."

The Montana DOC's policy no. 1.6.25, Computer Network Security, effective January 8, 1999, states: "It is the policy of the Montana Department of Corrections to prevent offenders from accessing the State of Montana's information systems, and to comply with state laws and policies which regulate the use of state computers and information technology." Procedure IV(1) further states: "Inmates incarcerated in a

state prison will not be allowed access to any computer connected to the State of Montana's network for any reason."

Oklahoma DOC policy OP-021001, effective April 9, 1998, specifies that it is unacceptable for staff to allow inmates access to the state's OneNet/Internet.

Policy 6.02 DOC in the Rhode Island DOC, effective July 15, 1996, states that PCs used by inmates, probationers, or parolees are not to be attached to the department's information systems, operational networks, or to any other computer networks.

Responses from 11 other states indicated that some type of prohibition exists. Because the actual policies were not provided for review, the exact nature of these prohibitions is not clear. Some policies may explicitly prohibit either Internet or network access. Some restrictions may exist as formal policies or operational directives, while in other states, they may be widely understood as a critical security issue without having been formalized in written policies.

The comments provided by survey respondents in these states make it clear that security concerns are of primary importance:

- "[Access is prohibited by] state Information Services Division rule."
- "[We] prohibit interactive computer use by prohibiting modems. We have computers, but prisoners cannot access the World Wide Web."

"Our department has taken the position that inmates having access to the Internet will present a security concern analogous to the unrestricted use of telephones. That is, potentially harassing the public, misusing access to view and download prurient materials, misuse in the development of schemes designed to defraud persons on the basis of money or other 'favors.' This is an extremely conservative position, but one that has served us well to this point. We have not had a single incident with inmates and computer based communications."

"We have a policy which prohibits inmate access."

"Inmates should not access Internet as a security issue. They should never access a computer with modem and phone access."

"Our policy doesn't specifically prohibit Internet access, but it says inmates cannot have access to the agency's computer network. Since they have no access to the network, they have no access to the Internet and no access outside of the facility."

DOCs in the remaining 25 states and the District of Columbia did not indicate that any restrictions exist against inmate access to interactive computers. In at least one of these agencies, the issue of such access has

been discussed by top agency managers, though no formal policy has resulted. Security concerns have been given precedence over program interests for the present time in that agency, and access will not be provided in the foreseeable future.

Do restrictions exist that affect other offender populations?

DOC respondents were also asked whether their agencies' policies on inmate access to interactive systems apply to persons released from secure institutional settings. Several DOCs indicated that their restrictions do extend to populations outside the secure, institutional environment.

- Eleven (11) DOCs that reported some form of restriction in institutional settings also indicated that the restrictions apply to inmates placed in community-based programs or facilities while remaining under DOC jurisdiction.
- In seven (7) agencies, the restrictions do not extend to these offenders.

Agencies' specific methods of supervising or controlling this access were not described. Notes concerning the nature of the restrictions include:

- "The administrative directive applies to all DOC facilities."
- "There is no blanket policy in existence, although individual exceptions might be made based on the crime or relevant circumstances."
- "Community corrections clients in our facilities do not have interactive access. Persons on street supervision are not barred from access via systems they own or have legal access to."
"Inmates placed/housed at community-based halfway house facility are not permitted access to the facility's interactive computers. This ban does not extend to the inmates' community-based employment or school."

Regarding inmates released on parole or to other forms of post-release supervision, six (6) DOCs reported that restrictions can or do apply. Respondents observed:

- "Sex offenders may have restrictions imposed as a condition of parole."
- "Restrictions could be ordered as a special restriction, but at this time the need has not arisen."
- "The court or Indeterminate Sentence Review Board can place a prohibition on an offender to not access pornography or participate in chat room discussions on the Internet. If a prohibition is ordered, we will monitor. If not, we cannot monitor."
- "In regard to those convicted of sex related crimes, the Probation and Parole Division will seek an order from the sentencing court or parole board restricting the inmate's access. This order is then enforced as a condition of parole."

Conclusion

The primary concern of state corrections agencies is the safety and security of their institutions and the citizenry they serve. As more U.S. citizens gain connections to the Internet, World Wide Web, and other interactive computer services, it can be expected that more persons under correctional supervision will have experience with using these technologies and would have the ability to use them if provided access by correctional agencies. Though such access could potentially be used for beneficial purposes in educational, programmatic, and work settings and despite the interest being expressed by some correctional program staff, it is clear that DOCs today do not believe such access can be provided safely.


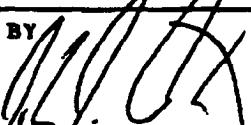
This study found evidence that correctional agencies are well aware of the security risks that interactive computer systems can pose if access is not carefully managed, that agencies are particularly concerned with the issue of inmate access to such systems, and that agencies are using prudent measures to control inmates' access. That more DOCs did not cite related policies may be due to the relative recency of these technologies' use at an operational level in U.S. prisons.

The study also found that there is considerable interest in providing inmates access to interactive technologies for educational, work, and other purposes. The methods proposed for control of such access will need to meet the most rigorous standards of correctional management.

APPENDIX A.

State Statutes and Correctional Agency Policies on Inmate Access to Interactive Computer Systems

(Statutes and agency policies are appended in alphabetical order by state.)

State of Connecticut Department of Correction	DIRECTIVE NUMBER 4.6	EFFECTIVE DATE October 1, 1998	PAGE 1
 ADMINISTRATIVE DIRECTIVE	SUPERSEDES:		
APPROVED BY  9/11/98	TITLE: Use of Computers and Related Technologies		

1. **Policy.** Computers and related technology shall be utilized for authorized agency purposes consistent with state and Federal law.
2. **Authority and Reference.**
 - A. Connecticut General Statutes, Sections 1-18, 1-18a, 7-109 and 18-81.
 - B. Office of the Public Records Administrator and State Archives, "General Letter 98-1", June 1, 1998.
 - C. Administrative Directives 6.6, Reporting of Incidents and 10.1, Inmate Work and Pay Plan.
3. **Definitions.** For the purposes stated herein, the following definitions apply:
 - A. **Electronic Mail (email).** Messages transmitted by computer technology.
 - B. **Software Package.** Any program or application that can be installed on a computer.
4. **Use of Computers and Software.** The use of computers shall be for departmental business purposes only. Department employees shall comply with the following principles regarding the use of computers:
 - A. Any computer or software utilized by agency staff shall be authorized by the Department's Research and Management Information Systems (M.I.S.) unit. The use of personally owned hardware or the installation of shareware, freeware, personal or demonstration software, to include non-approved screen savers and computer games, shall be prohibited. The Director of M.I.S. may issue a memorandum allowing specific departmental units to install shareware, freeware or demonstration software when, in the Director's view, the unit would benefit from the use of such software.
 - B. A software package shall be used on one computer at a time, unless the individual software license specifies otherwise.
 - C. A software package may be copied to diskette for the purpose of making a back-up disk(s) to protect from loss.
 - D. Software purchased for network use shall be subject to the maximum number of simultaneous users specified by the software license. Under no circumstances shall a Department employee download an application from the Department's network server to an individual hard-drive without the written approval from the Director of M.I.S.
 - E. The Director of the M.I.S. shall issue a list of software that may be used on Department computers. Requests to purchase any software package shall be forwarded to the M.I.S. unit, which will coordinate the purchase.
 - F. The use of utilities that modify computer hardware configurations shall be prohibited.
 - G. Inmates shall not use any computer that is connected to a network of any kind. Inmates shall be prohibited from using computers

DIRECTIVE NO. 4.6	EFFECTIVE DATE October 1, 1998	PAGE OF 2 2
----------------------	-----------------------------------	----------------

TITLE
Use of Computers and Related Technologies

except when necessary for specific education or work assignment, in accordance with Administrative Directive 10.1, Inmate Work and Pay Plan. No inmate shall be allowed personal use of a computer for any reason.

H. The Department of Correction shall perform periodic audits to ensure that all software standards are maintained.

5. Use of Electronic Mail. The use of email shall be for departmental business purposes only. Email shall not be used to report incidents in accordance with Administrative Directive 6.6, Reporting of Incidents. Using email to solicit support for personal, political, or religious causes shall be prohibited. The routine monitoring of email by the Research and M.I.S. Unit shall normally be prohibited; however, the Commissioner or designee may direct the Research or M.I.S. unit to monitor, access and/or review employee email if deemed appropriate. Email transmissions, excepting transitory messages, shall be backed up to tape which shall not be deleted or destroyed without the signed approval of the Office of the Public Records Administrator.

6. Use of the Internet. The use of any Internet service for business unrelated to the Department shall be prohibited. The Research and M.I.S. unit shall monitor each individual Internet account to prevent excessive or improper use. The following principles shall be in effect with regard to Internet usage:

- A. Use of the Internet to gain unauthorized access to any computer system, application or service shall be prohibited. The Department may monitor and audit the agency's computers to determine which sites are being accessed.
- B. Use of the Internet for private commercial purposes, to include business transactions between individuals and/or commercial organizations shall be prohibited.
- C. All electronic mail communication via the Internet shall be governed by the procedures included in Section 5 of this Directive.
- D. The downloading of any software products via the Internet shall be subject to state and Federal copyright laws. Any software downloads shall require the prior written approval of the Director of Research and M.I.S.
- F. Any file downloaded from the Internet shall be scanned for computer viruses.
- G. Use of the Internet that interferes with or disrupts network users, services or computers shall be prohibited. Such disruptions may include, but not be limited to distribution of unsolicited advertising or propagation of computer viruses.
- H. Use of the Internet to engage in acts that are deliberately wasteful of computing resources or which unfairly monopolize resources to the exclusion of others shall be prohibited. These acts may include, but not be limited to, broadcasting unsolicited mailings or other messages, creating unnecessary output, or creating unnecessary network traffic.

7. Exceptions. Any exceptions to the procedures included in this Administrative Directive shall require the prior written approval of the Commissioner.



Minnesota Statutes

Minnesota Statutes 1998 Display Document 1 of 1



Chapter Title: CORRECTIONS; ADULTS
Section: 243.556

Text:

243.556 Restrictions on inmates' computer access.

Subdivision 1. Restrictions to use of online services. No adult inmate in a state correctional facility may use or have access to any Internet service or online service, except for work, educational, and vocational purposes approved by the commissioner.

Subd. 2. Restrictions on computer use. The commissioner shall restrict inmates' computer use to legitimate work, educational, and vocational purposes.

Subd. 3. Monitoring of computer use. The commissioner shall monitor all computer use by inmates and perform regular inspections of computer equipment.

HIST: 1997 c 239 art 9 s 23





Chapter Title: CORRECTIONS; ADULTS

Section: 243.055

Text:

243.055 Computer restrictions.

Subdivision 1. Restrictions to use of online services.
If the commissioner believes a significant risk exists that a parolee, state-supervised probationer, or individual on supervised release may use an Internet service or online service to engage in criminal activity or to associate with individuals who are likely to encourage the individual to engage in criminal activity, the commissioner may impose one or more of the following conditions:

- (1) prohibit the individual from possessing or using a computer with access to an Internet service or online service without the prior written approval of the commissioner;
- (2) prohibit the individual from possessing or using any data encryption technique or program;
- (3) require the individual to consent to periodic unannounced examinations of the individual's computer equipment by a parole or probation agent, including the retrieval and copying of all data from the computer and any internal or external peripherals and removal of such equipment to conduct a more thorough inspection;
- (4) require consent of the individual to have installed on the individual's computer, at the individual's expense, one or more hardware or software systems to monitor computer use; and
- (5) any other restrictions the commissioner deems necessary.

Subd. 2. Restrictions on computer use. If the--
commissioner believes a significant risk exists that a parolee, state-supervised probationer, or individual on supervised release may use a computer to engage in criminal activity or to associate with individuals who are likely to encourage the individual to engage in criminal activity, the commissioner may impose one or more of the following restrictions:

- (1) prohibit the individual from accessing through a computer any material, information, or data that relates to the activity involved in the offense for which the individual is on probation, parole, or supervised release;
- (2) require the individual to maintain a daily log of all

addresses the individual accesses through computer other than for authorized employment and to make this log available to the individual's parole or probation agent;

(3) provide all personal and business telephone records to the individual's parole or probation agent upon request, including written authorization allowing the agent to request a record of all of the individual's outgoing and incoming telephone calls from any telephone service provider;

(4) prohibit the individual from possessing or using a computer that contains an internal modem and from possessing or using an external modem without the prior written consent of the commissioner;

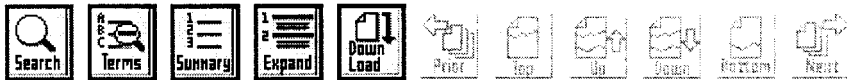
(5) prohibit the individual from possessing or using any computer, except that the individual may, with the prior approval of the individual's parole or probation agent, use a computer in connection with authorized employment;

(6) require the individual to consent to disclosure of the computer-related restrictions that the commissioner has imposed to any employer or potential employer; and

(7) any other restrictions the commissioner deems necessary.

Subd. 3. Limits on restriction. In imposing restrictions, the commissioner shall take into account that computers are used for numerous, legitimate purposes and that, in imposing restrictions, the least restrictive condition appropriate to the individual shall be used.

HIST: 1997 c 239 art 9 s 18



USE OF ELECTRONIC EQUIPMENT BY ADULT OFFENDERS

AUTHORITY: Minn. Stat. §243.556.

PURPOSE: To establish controls that ensure facility security and the protection of the public from the misuse of electronic equipment by adult offenders.

APPLICABILITY: All facilities.

DIRECTIVE: Adult offenders will have controlled access to and use of electronic equipment.

DEFINITIONS:

Electronic equipment - includes computer hardware and software, fax machines, modems, telephones, typewriters with memory, storage media, interactive television or any devices capable of transferring data; but excludes offender property maintained and utilized in living units (i.e., televisions, radios, games), which is controlled under a separate policy/directive.

Internet or on-line services - external computer networks.

Quarterly inspection - the physical inspection for unauthorized files and peripherals of all storage media on, and including, the electronic equipment hardware that is accessible to offenders.

PROCEDURES:

A. Inspections

1. The inventory controller will maintain current inventories of all electronic equipment utilized by staff, the education department and in offender work areas in accordance with established state fixed asset inventory procedures.
2. The warden/superintendent will designate a qualified person to conduct quarterly inspections of all electronic equipment accessible to offenders, as well as conduct inspections when requested for intelligence processes. Inspections will be conducted by formatting hard drives or searching for and deleting unauthorized files.
3. The warden/superintendent will designate a qualified person to review the use and security of electronic equipment prior to purchase.

B. Equipment/Software Safeguards

1. Offenders may only use state electronic equipment for authorized educational, vocational or work purposes.
2. No programming, code, job control language, or batch code will be developed by any offender within a facility without the prior approval and the direct supervision of a technically qualified department staff person designated by the warden/superintendent.

USE OF ELECTRONIC EQUIPMENT BY ADULT OFFENDERS

3. Offenders may not use password protection, encryption, hidden files, or any other software technology or technique that would prevent inspection.
4. All voice and data communication lines located within a facility will be under the direct physical control of the facility staff.

C. Unauthorized Use of Electronic Equipment

1. Offenders are not permitted access to the Internet.
2. Offenders are not permitted to obtain access to the Internet through third parties.
3. Offenders may not purchase or possess any personal electronic equipment, with the exception of typewriters allowed by department directive 302.250.
4. Offenders may not possess electronic equipment outside the authorized area of use.
5. Offenders may not operate an staff networked electronic systems, including that which has access to any department management information systems.

D. Violations of this directive will be processed under the discipline policy.

REVIEW: Annually

REFERENCES: Adult Male Institutions Division Policy memo "Inmate Property"
Vol. 9, no. 1, November 1995
Department Directive 302.250 "Offender Property"

SUPERSESION: Policy 3-230," Use of Electronic Equipment by Inmates"
All facility policies, memos or other communications whether verbal, written, or transmitted by electronic means regarding this topic.

ATTACHMENTS: None



**Erik Skon, Assistant Commissioner
Adult Facilities**

**DEPARTMENT OF CORRECTIONS
POLICIES AND PROCEDURES**

Policy No.: DOC 1.6.25	Subject: COMPUTER NETWORK SECURITY
Chapter 1: ADMINISTRATION AND MANAGEMENT	Page 1 of 2
Section 6: Information and Research	Revision Date:
Signature: /s/by Director Rick Day 1/8/99	Effective Date: Jan. 8, 1999

**THIS IS AN EMERGENCY INTERIM POLICY DRAFTED PURSUANT
TO D.O.C. POLICY 1.1.2(IV)(i)**

IT IS EFFECTIVE ONLY FOR 90 DAYS FOLLOWING THE ABOVE EFFECTIVE DATE

I. POLICY:

It is the policy of the Montana Department of Corrections to prevent offenders from accessing the State of Montana's information systems, and to comply with state laws and policies which regulate the use of state computers and information technology.

II. AUTHORITY:

2-15-114, MCA, Security responsibilities of departments for data and information technology resources.

2-17-503, MCA, Security responsibilities of department of administration

45-2-101, MCA, General Definitions

45-6-311, MCA, Unlawful use of a computer

1-0250.00 M.O.M., Information Security System

Department of Administration Enterprise-wide Policies as follows:

S-GEN40 - User ID Password and Access

S-GEN50-User Responsibilities

S-GEN60-Work Station and Portable Computer Security

S-LG50-Logging On and Off the network *ITM Policy Committee*

III. DEFINITIONS:

1. "**Firewall**" means a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Subject: COMPUTER NETWORK SECURITY**IV. PROCEDURES:**

1. ~~Offenders Inmates incarcerated in a state prison~~ will not be allowed access to any computer connected to the State of Montana's network for any reason.
2. Log in ID's at secure facilities will be limited to the workstation(s) that an employee needs to access in order to perform the employee's job duties.
3. Any computer logged onto the State of Montana's network may not be left unattended ~~for any reason. Users leaving their computers unattended for 15 minutes or longer should either log off the network or have~~ unless the screen is protected with by a password. ~~and Each employee must log off the network at the end of the employee's shift.~~
4. Users must enter a valid login ID to successfully gain access to any networked computer located in a secure facility. The operating system will not complete its startup procedure until a user has successfully logged on.
5. Request for access to any information system outside of a firewalled area must be approved and documented by the Department's network security officer.
 - A) These requests must be submitted to the Department's network security officer in writing by the employee's immediate supervisor.
 - B) Upon approval, the Department's network security officer will forward these requests to the State Network Security Officer for implementation.

V. CLOSING:

Questions concerning this policy shall be directed to Department Network Administrator.

**MICROCOMPUTER
POLICY & PROCEDURES
USERS' MANUAL**



**STATE OF NEW JERSEY
DEPARTMENT OF CORRECTIONS
OFFICE OF INFORMATION TECHNOLOGY
JUNE 1998**

TABLE OF CONTENTS

Scope and Purpose	1
General PC Guidelines	2
Local and Wide Area Network Control	4
Assigning PCs	6
Internet Access	8
E-mail	10
Virus Protection	11
Procurement & Disposition	12
Glossary of Information Technology Terms	13
Internet Access	
Internet Mail Access form	Attachment A
WWW Access form	Attachment B
DOC PC-Micro System Access and Security Agreement Form	Attachment C
Microcomputer Acquisition Request	Attachment D

INTERNET ACCESS

The Internet comprises many different interconnected networks and computer systems, each **having** its own rules and limitations. Users on these systems have an obligation to learn and abide by these rules, customs, and courtesies.

The Internet is an unsecured system with little or no security controls and should never be used to transmit confidential information unless the transmissions are encrypted.

The State of New Jersey maintains a secure, coordinated, and cost effective approach to Internet access and use by State employees. An Internet Service Provider has been established by the State. Separate access contracts are only permitted with the approval of the Director, Office of Policy and Planning, Manager, Office of Information Technology, or their designee and OTIS. Permission will only be granted if technical incompatibility has been identified and/or special functional requirements exist.

State provided Internet access is considered State property and is for State business only.

Use of State provided Internet access is a privilege that can be revoked at any time for violation of these policies and procedures. Misuse of the privilege can result in one or all of the following: disciplinary action, reassignment of duties not requiring access to a computer, criminal prosecution, civil suit, or termination from state service.

Use of the Internet is a privilege that constitutes the acceptance of responsibilities and obligations that are subject to federal, state, and local laws.

The Internet is a prime source for introducing viruses into the PC and LAN environment. Procedures to minimize the risk are detailed in the section titled "VIRUS PROTECTION".

Much of the information on the Internet is provided "as is". Check the information with other sources to ensure its accuracy.

The Department's policy on access to the Internet is very restrictive. Only authorized staff members are permitted to access and use the Internet and only those employees with a true business need will be given this privilege. All users who request such access must provide documentation to justify the need. There are two kinds of Internet access that are offered by the DOC: WWW (World Wide Web) and Internet Mail. Listed below are the required documentation, authorization and specific policies for each type of access.

WWW access:

- Requests for access require signoff by the employee, employee's supervisor and Assistant Commissioner or Director. If the request is from a division other than Administration, a copy of the request must be sent to the Assistant Commissioner of

Administration and the Director, Office of Policy and Planning. See the attached “Request for Staff Access to the World Wide Web (WWW)” document.

- Specific business needs and examples must be provided with the request for access, including the types of sites it is anticipated the employee will access (If specific URL's are known, they should be provided also).
- When web access is required, supervisors should only approve access for one person and a backup unless justification for more users can be provided.
- Browsers (e.g., Netscape) should only be running while in use actively navigating the web. When not accessing the web, these programs should be terminated.
- “Push” agents (e.g. Pointcast) or any Internet software which maintains a continual data stream to the PC are not permitted. These agents consume bandwidth, significantly degrading LAN performance.
- There is a significant amount of inappropriate information on the WWW. Care should be taken to avoid this information.
- The viewing, downloading or printing of adult or pornographic material is expressly prohibited unless it is directly related to a business need (e.g., research on sex offenders).
- The downloading of copyrighted material for distribution is prohibited unless permission is received from the author and it is for a stated business need.
- Any personal use of the Internet on DOC equipment is prohibited even if it occurs outside of normal working hours (e.g., during lunch or break periods, after work).
- DOC monitors staff access and utilization to ensure it is appropriate and consistent with the organization’s mission. All Internet activity will be tracked and reports will periodically be made available to managers indicating the amount of time each user has spent on the Internet and the sites visited.
- Inmates will not access PCs with Internet capabilities in any manner and are not permitted to view screens without the written permission of the Manager, Office of Information Technology, or a designee.
- Users need to identify themselves properly and be careful about how they represent themselves. Extreme caution must be taken not to convey information that might be misinterpreted as a DOC and/or State opinion or policy. Users are cautioned not to act as spokespersons for DOC by attempting to answer questions on the Internet unless authorized to do so.
- The use of fee-for-service providers on the Internet is not permitted unless the necessary approvals and funding have been obtained in advance by the Director, Office of Policy and Planning, Manager, Office of Information Technology, or their designee.
- Anyone obligating DOC to pay for services without prior approval is personally liable for these charges and is subject to disciplinary action.

DEPARTMENT OF REHABILITATION AND CORRECTION POLICY 112-01	SUBJECT: Computer Installation Requirements & Inmate Access to Computer Resources	Section: 112 Number: 01
	RULE/CODE REFERENCE: A.R. 5120-9-49	SUPERCEDES: 112.01 MICROCOMPUTER POLICY
	RELATED ACA STANDARDS: 3-4097 and 3-4098	EFFECTIVE DATE: January 2, 1997
	RELATED AUDIT STANDARDS: N/A	APPROVED: <i>Reginald Q. Wilkinson</i>

i. AUTHORITY

This policy is issued in compliance with the authority of the Director of the Ohio Department Rehabilitation and Corrections to manage and direct the total operations of the Department as described in the Ohio Revised Code, Section 5120.0.

ii. PURPOSE

Provide direction for installation, maintenance and access to computer hardware and software. Provide direction on the access and use of computer hardware and software by the inmate population.

iii. APPLICABILITY

This policy applies to all ODRC locations where access to computer data will assist in the management and operational requirements of the facility. This applies to all current and future ODRC sites.

DEFINITIONS

Inmate Progression System (IPS) -A relational database system managing Inmate, parole, probation and community offender database applications used in the Ohio Department of Rehabilitation and Correction.

Employee Relations System (ERS) -A relational database system designed for the Ohio Corrections Assessment Center. Primary functions include tracking of employee grievances, disciplinary information, EEO and employee training Information.

Office Automation System (OASYS) -A relational database system providing automation of various administrative functions including strategic databases, supply management and directories. Provides on-line access to ODRC policies, strategic plan and other departmental documentation.

Training Industry and Education (TIE) - A server based tracking system that specializes in inmate education, job and training functions for ODRC.

Computer Hardware - Physical components used in electronic data processing operations at the mainframe, midrange and microcomputer levels, e. g. computer processing unit, modem, printers, etc.

Local Area Network System (MNS) -A group of microcomputers that can communicate with each other, e-g- file and printer sharing, and if desired, access to remote hosts or ether networks. A network consists of one or more file servers workstations and peripherals. Network users may share the same data and program files, send messages directly between individual workstations, and protect files by means of an extensive security system.

Microcomputer - A computer built around a microprocessor; a personal computer (PC) with a monitor,

keyboard and central processing unit (CPU).

Peripheral - Hardware that is attached to the CPU via cables and driven by system software, e.g. modems, printers, tape backup systems or a mouse.

Server - A device on a LAN that provides some type of service to other workstations on the LAN. A file server provides access to shared programs and data files. A printers server provides access to one or more shared printers. A database server provides access to shared database files, which may include data on other LANS, mainframe and minicomputers. An application server offers access to shared software applications.

Software - An operating system, application program, routine or symbolic language consisting of written or printed instructions that control basic computer hardware functions and tasks, e.g. word-processing, database, graphics, spreadsheet, etc.

Wide Area Network System (WANS) - A networking system that covers a large geographic area and includes any computing device that may be permanently or temporarily integrated into a LAN.

Workstation - A microcomputer used by an individual to do his or her work tasks. In a LAN the term often distinguishes an individual user's PC from PC used as a shared resource such as a file server.

Programming Approval Requirements - All software and hardware acquisitions shall be evaluated by MIS staff. Use of inmate labor for programming projects require the written authorization of the manager of the application area and the Deputy Director of OMIS.

Security Approval Requirement - Security requirements shall be evaluated according to the confidentiality and sensitivity of the data, user base and location. Network systems software must be adaptable to existing security requirement of ODRC.

V. POLICY

It is the policy of this Department that on-line microcomputer workstations will be provided access to systems such as the Inmate Progression System (IPS) and the Training, Industry and Education database (TIE), only when it is in the best interests of ODRC. All systems will maintain security measures to insure only authorized access to these systems.

VI. PROCEDURE

PROCESS

All computer hardware/software acquisitions whether purchased or donated must conform to the established ODRC standards as set forth by the Office of Management Information Systems. All hardware and software procurements must be reviewed and approved by the Bureau of Information and Technology Services and meet OMIS standards prior to procurement. Pre-approval must be obtained from OMIS/BITS for all hardware and software regardless of funding source including equipment purchased from salvage.

If there is a question as to the standard hardware/software configuration, the manager of the respective application area must be contacted.

IPS: Located at 970 Freeway Drive North. 614-752-1302

OPI: Located at 315 Phillipi Road in Columbus, Ohio 614-752-0252

TIE: Located at the Correctional Training Academy, 614-877-4345- x322

- Installation of on-line computer hardware/software is to be coordinated with the appropriate managers

noted above.

- Non-standard software must be justified in writing and reviewed by OMIS prior to installation on any departmental computer system.
- Non-standard software that has not been approved or which interferes with the proper and efficient operation of primary business functions is subject to removal by OMIS/BITS technical staff. Examples include: screen-savers, game programs, etc.
- Computer applications access codes (passwords) are required for all on-line applications and any computer accessible by inmates. The use of common or "public passwords" invalidates audit trails and is not acceptable under any circumstances.

INMATE ACCESS

- Inmates are **NOT** to be involved in specifying, designing, purchase, installation or operation of any computer/network equipment or software that will be used in the administrative operations of ODRC.
- Inmates will not have access to modems, dial-up lines, file servers, network software or any other data communications equipment that is part of a Local or Wide Area Network, except as noted below.
- Inmates may only have access to stand alone inmate education systems and approved OPI WAN/LAN systems including CADD and data entry systems. Exceptions will be reviewed by OMIS/BITS and approved in writing by the Director. Access to floppy disks will be strictly controlled through the use of sign in and sign out logs under supervision. There shall be a maximum of five (5) floppy disks in the possession of an inmate at anytime. Under no circumstances will an inmate be permitted to remove a floppy disk from the assigned training area.
- Inmates are not permitted to receive or utilize a personal computer, peripheral device or typewriter with memory capacity outside of a training environment.
- Access to computers designed for inmate training do not require passwords.
- Floppy disks are considered contraband and are not permitted for possession or receipt by an inmate.
- The Warden, field supervisors and/or Central Office Executive Staff shall designate a supervisor(s) of the area(s) utilizing the equipment, to be responsible for computer access and floppy disk control. All violations are to be reported to the Chief Inspector's office for investigation.

Section-02 information Management	OP-021001 Page: 1 Effective Date: 04/09/98
Internet Standards	ACA Standards: None

Department of Corrections OneNet/Internet Standards

This procedure is intended to both identify the circumstances under which the Department of Corrections (DOC) employees may access the OneNet/Internet through state facilities, or be identified as state of Oklahoma employees, and define what the DOC considers acceptable use and conduct once an employee is connected to the network. Its purpose is to clearly communicate the DOC's expectations with respect to what is and what is not "acceptable use" and to minimize the risk of offensive or inappropriate behavior on the network.

I. Overview of the Internet

Although the Internet represents a potentially valuable resource, it also exposes the DOC 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. Therefore, all aspects of DOC's OneNet 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 DOC's employees is suitable for business purposes and accomplished in a cost-effective manner.

A. OneNet Privilege

OneNet services are provided by the state of Oklahoma to support open communications and exchange of information, and the opportunity for collaborative government-related work. DOC 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 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 on the Internet in general. The burden of responsibility is on the user to inquire as to acceptable and unacceptable uses prior to use.

C. Employee Use

Employees should use state provided Internet services for state related activities and not for personal business.

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

E. Employee Agency Consideration

Employees should avoid uses of the network that reflect poorly on DOC or on the state of Oklahoma.

F. Employee Ethical Behavior

Users should remember that existing rules, regulations, and guidelines on ethical behavior of DOC employees and the appropriate use of state resources apply to the use of electronic communications systems supplied by the state of Oklahoma,

G. Employee Discontinuance of OneNet/Internet Services

If, at some future point, Internet access is no longer necessary, the employee must notify the unit head within two business days

II. Information Exchange

A. Specifically Acceptable Uses (Include, but are not limited to):

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

2. Communication and exchange for professional development, to maintain currency of training or education, or to discuss issues related to the user's DOC activities.
3. Use in applying for or administering grants or contracts for DOC 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
6. Any other governmental administrative communications not requiring a high level of security.

B. Specifically Unacceptable Uses (Include, but are not limited to):

1. Use of the Internet for any purposes which violate a federal or state law.
2. Use for any for-profit activities unless specific to the charter, mission, or duties of the DOC
3. Use for purposes not directly related to the mission, charter, or work tasks of DOC during normal business hours
4. Use for private business, including commercial advertising.
5. Use for access and distribution of indecent or obscene material.
6. Use for access to and 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 so as 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, in fact, permissible. Any efforts to obtain permission should be adequately documented.
10. Users misrepresenting themselves as other persons either on OneNet or elsewhere 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 of same.
12. Use for fund raising or public relations activities not specifically related to state government activities
13. Allow inmates access to OneNet/Internet.

C. Additional Guidelines:

1. Any software/files downloaded should be virus checked prior to use
2. Use passwords associated with DOC computer services only on that system. When setting up an account on a different information system that will be accessed using the Internet, choose a password that is different from ones used on DOC computers.
 - a. Do not use the same password for both local and remote Internet-accessed systems, 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 90 days
3. Always make a reasonable attempt 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. The Internet connection is a shared resource. While routine electronic mail and file transfer activities will not impact other users much, 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, to be considerate of other users, schedule these activities early or late in the day or, better, after business hours.
6. Users should avoid being drawn into discussions where disclaimers such as "this represents my personal opinion and not that of my department or the state of Oklahoma" need to be used.
7. The sites visited on the Internet can capture the addresses of those who visit the site.

D. Non-State Employees

Contractors and other non-state employees may be granted access to state provided OneNet/Internet services at the discretion of the contracting authority. Acceptable use by contractors and other non-state employees working for the state of Oklahoma is the responsibility of the contract administrator. The contract administrator is expected to provide contractors who use state of Oklahoma OneNet/Internet services with this information.

III. Responsibilities

A. Non-Compliance

The unit heads are responsible for their employees' compliance with the provisions of these procedures and for investigating non-compliance.

When an instance of non-compliance with this procedure is discovered or suspected, the unit will proceed in accordance with DOC and state of Oklahoma personnel policies. Suspension of serviceto 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 knowingly violates the acceptable use procedure. Discipline may be appropriate in some cases of noncompliance with this procedure. Criminal or civil action against users may be appropriate where federal or state laws are violated.

B. Responsibility

The 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 that unit,
2. Reviewing, verifying, processing, and recording all employee requests for OneNet/Internet access;
3. Enabling employee access when approved. By approving such a request, the unit agrees to:
 - a. Acquire hardware or software that is necessary to enable access to the OneNet/Internet.
 - b. Request access authorizations from Computer Services.
 - c. Assure that the employee approved for access has read and understands, the procedure and requirements

C. Notification

Within two business days of an employee's death, disability, or termination, the unit head is responsible for notifying Computer Services of the need to terminate access or change the user information,

IV. Statewide Administration

A. IP Addresses and Domains

Computer Services has the responsibility to properly manage all OneNet/Internet Protocol (IP) addressing and assignments within the assigned class B license for the DOC. This includes the central node and peripheral nodes using this license. This responsibility includes the proper management of

1. Statewide Security
2. Routing Topologies
3. Transport Levels and Traffic Monitoring

B. Orientation

Computer Services will provide basic orientation for managers and supervisors who carry the responsibility for overseeing the use of the OneNet/Internet and assuring compliance with these procedures at their facility.

C. Administrative Issues

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

V. References

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

Title 62, Section 45, State Resolution

VI. Action

The regional director/division head will be responsible for compliance with these procedures.

The deputy director, Administrative Services will be responsible for the annual review and revisions.

Any exceptions to this operations memorandum will require prior written approval of the director.

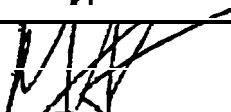
These procedures will be effective 30 days after signing.

Distribution: *Policy and Operations Manual*

James L. Saffle, Director
Oklahoma Department of Corrections



POLICY STATEMENT
Commonwealth of Pennsylvania • Department of Corrections

Policy Subject: Inmate Use of Computers	Policy Number: 6.3.30	
Date of Issue: December 19, 1997	Authority: 	Effective Date: January 19, 1998

I. Authority

The authority of the Secretary of Corrections to direct the operation of the Department of Corrections is established by sections 201, 206, 506, and 901-B, of the Administrative Code of 1929, act of April 9, 1929, P.L. 177, No. 175, as amended.

II. Purpose

The purpose of this document is to establish department policy and procedures relative to inmate access to and use of computer systems.

III. Applicability

This policy is applicable to all Department of Corrections (hereafter referred to as DOC) employees, inmates, contractors and individuals who use computer equipment or systems within a State Correctional Institution, Community Corrections Center or other DOC facility.

IV. Definitions

- A. **Automation Equipment:** All controllers, communications equipment, mainframe computers, file servers, microcomputers, monitors, modems, multiplexors, printers, switch boxes, terminals, workstations, etc. that are used with or connected to any of the equipment mentioned above.
- B. **CD-ROM:** Compact Disk-Read Only Memory. High capacity information storage media used with a microcomputer to read information or programs. Usually a flat circular plastic platter on which information or programs have been recorded optically by a commercial firm and which can be read on a CD-ROM Drive/Jukebox.
- c. **Computer.** An electronic, magnetic, optical, hydraulic, organic or other high-speed information processing device or system that performs logic, arithmetic or memory

functions, and includes all input, output, processing, storage, software or communications facilities which are connected or related to a network, For the purpose of this document, the definition of a computer does not include word processors (i.e. typewriters with memory functions).

- D. Computer Services Division: Unit in-the Bureau of Management Information Services at Central Office.
- E. Educational and Vocational Programs: Any program provided under the auspices of the School Principal. This includes academic, computer training, electronics, arts & crafts, barber school, library. and similar programs-
- F. Education Computers; Computers that have been specifically approved and designated for use by inmates within educational and vocational programs.
- G. External Computer Storage Media: Magnetic, optical, or other media used with a computer device to record and store computer-based information external to the computer device. Examples of external computer storage media include 3.5" and 5.25" diskettes. magnetic tape cartridges, CD-ROM disks, and removable hard disks.
- H. Facility Manager: Includes Superintendents, Regional Community Corrections Directors, and the Boot Camp Commander.
- I. Information/Program Back-up Routines: The process of recording a copy of information of programs from a computer onto external computer storage media for the purpose of ensuring the information or programs are not lost in the event of an equipment failure, disaster,, etc.
- J. Modem: Modulator-Demodulator. A device that transforms a computer's electronic pulses Into audible tones for transmission over a phone line to other automation equipment.
- K. Network: A telecommunications medium and associated components responsible for the transfer of information.
- L. Network Adapter: A device installed in or connected to a computer that facilitates the physical connection of that computer to a communications network. Examples of network adapters in use in the DOC include IBM 3270 coax adapters, IBM 3270 SDLC adapters, Token-Ring network adapters, and Ethernet network adapters.
- M, Program: Related instructions that, when followed and executed by a computer, perform a set of operations or tasks.
- N, Secure Area: An area in which inmates are not assigned to work and which is always locked when staff members are absent.

- O. Secure Storage: A locking desk, file cabinet or similar non-portable storage.
- P. Software: The programs used to control computer operations-
- Q. Staff; Any employee of the Commonwealth of Pennsylvania or any person working under contract with the Commonwealth-
- R. Workstation: An independent microcomputer connected-to the network for the purpose of utilizing network resources.

V. P o l i c y

It is the policy of the Department of Corrections to limit inmate access to automated equipment in order to ensure the integrity of departmental management, security, and operational information and to prohibit inappropriate access.

VI. Procedures

A. Access

1. Inmates are permitted access to automated equipment'
 - a. For educational purposes while being supervised in inmate classrooms, school libraries, and laboratory settings provided that access is restricted to other computers installed within a single educational area of a facility which are not connected to a computer network outside the educational area or to any telephone line.
 - b. Located in Correctional Industries, Education, the Inmate Library and other areas which do not store information concerning facility security and/or operations provided that the computer:
 1. Is not connected to any telecommunication network or phone line,
 2. Is not used to transfer information or programs to other computers,
 3. Has the external computer storage media (e.g. diskettes) maintained and/or stored away from the machine,
 4. Has an external computer storage media (e.g. backup diskettes) designated for use only with that machine.
 - c. To access Project Workplace applications designated for inmate use.
 - d. To access CD-ROM directories of library reference materials available through the inter-library loan system-

2. Inmates are not permitted to access automated equipment except as listed in **IV.A.1.** above and inmates are not permitted to access automated equipment that;
 - a. Contains a network adapter or other internal telecommunications devices such as a modem, except for Self-contained networks within a single education area. Inmate access to this automation equipment is prohibited at all times regardless of whether or not the network adapter or internal telecommunications devices active at the time-the inmate is accessing the automation equipment
 - b. Transfers information to other automated equipment except for educational purposes in inmate classrooms, school libraries, and laboratory settings.
 - c. Provides access to CD-ROM telephone directories or mapping software.
 - d. Controls or interacts with security systems that regulate door access, fire alarms, perimeter detection, or other security related systems.
 - e. Is located in an unsupervised office or area where a network-connected device is installed, powered-on, and/or otherwise ready for use.

3. Inmates are not permitted to:
 - a. Develop computer programs and/or applications for production use.
 - b. Perform information or program back-up routines on automation equipment except in conjunction with education and vocational programs.
 - c. Access communication network components including LAN hubs, routers, and Intranet or Internet cabling component, which are connected to a functional cabling system. Inmates are permitted to perform work on the installation of new network cables under the direct supervision of DOC staff. Inmate involvement in the installation of new network cables must be restricted to conduit installation and cable pulling tasks.
 - d. Enter or maintain data that could compromise effective facility operation or security including, but not limited to: inmate call-outs, appointments, work schedules; custody level tracking; digitized/electronic photos; inmate grades, diplomas, or course completion certificates; inmate payroll; inmate property records; and tool inventories.
 - e. Access, handle, possess, transport or use storage media except in an educational or vocational program.

B. Security

All automated equipment must be secured when staff is not present; to prevent unauthorized access by inmates. Each staff member must log-off when work has been completed and also when he/she is leaving, the general area for any reason. Where appropriate, doors to the room(s) in which equipment is located are to be dosed and locked when staff is leaving the area.

c. External Computer Storage Media

Disks, used with computers to which inmates have access, must be scanned for viruses on a regular basis.

A formal system of accountability must be established for all computer disks used by inmates in educational or vocational programs. These disks shall remain within the physical confines of the specific educational or vocational program area. Inmates shall be required to return all storage media after each use to the appropriate staff. Any missing disks shall be reported immediately in accordance with local policy. Master copies of program disks shall be kept in a locked cabinet and will not be issued to inmate students. However, working copies of educational program disks (software) may be utilized by inmates in an educational setting under the direct supervision of the teacher.

D. Use of Passwords

Inmates are prohibited from initiating or using passwords on computer systems and/or files.

E Violation of Policy

Inmates who violate the provisions of this policy shall be subject to a misconduct in accordance with DC-ADM 801-

F. Responsibilities

1. **Facility Managers** are responsible for ensuring this policy is adhered to at each facility.
2. **Automation Coordinators** are responsible for:
 - a. Reviewing all DOC supported equipment to ensure it is being used in compliance with this policy. These reviews, at a minimum, must be performed semi-annually. A record of these reviews is to be documented in an audit log. The log shall list discrepancies, actions taken, results accomplished, and the findings of follow-up inspections.

- b. Ensuring computer virus detection software is available to staff for all supported computer systems.
 - c. Reporting any instances, of virus detection to the Computer Services Division.
 - d. Assisting staff in determining if equipment or information has been misused or damaged by inmates.
 - e. Conducting random, unannounced audits of computers to ensure policy compliance. A record of these audits and follow-up inspections is to be documented in the same log as regular reviews.
 - f. Contacting the Institutional Security office in cases of suspected misuse of equipment or software or other violation of policy.
 - g. Ensuring that the original and a back-up copy of all programs on supported computers are maintained in secure storage in a secure area separate from on-going back-up copies.
3. **Institutional Staff** are responsible for the supervision and monitoring of inmate computer access within their area.
 4. **Education Department** Staff are responsible for the supervision and monitoring of inmate computer access within the education department. This includes implementing the appropriate safeguards to ensure education computers with communication capabilities, to which inmates have access, are restricted from accessing computer systems outside education and vocational programs.
 5. **Library** Staff are responsible for the supervision and **monitoring** of inmate computer access within their area.

VII. Suspension During Emergency

In an emergency situation or extended disruption of normal institutional operation, any provision or section of this policy may be suspended by the Secretary of Corrections, or her/his designee, for a specified period of time.

VIII. Rights Under This Policy

This policy does not create rights in any person nor should it be interpreted or applied in such a manner as to abridge the rights of any individual. This policy should be interpreted to have sufficient flexibility to be consistent with law and to permit the accomplishment of the purpose of the policies of the DOC.

IX Superseded Policy and Cross Reference


A. Superseded

This policy supersedes the previous policy, Inmate Access to Computer Systems 3.8.1 (028-06), dated December: 8,1989.

B. Cross Reference

1. DOC Administrative Manuals: DC-ADM 601

2. A C A : N / A

	NUMBER: 6.02 DOC ✓	EFFECTIVE DATE: 07/15/96 ✓	PAGE 1 OF 9
	REPEALS: N/A	DIRECTOR: <i>Abel T. Wall II</i> <i>Acting Director for</i> <i>Henry A. Vose, Jr., Director</i>	
SECTION: INFORMATION SYSTEMS AND RESEARCH		SUBJECT: ACCESS AND SECURITY - COMPUTERIZED INFORMATION SYSTEMS	
REFERENCES: ACA Standard 3-409B (Staff access, training, and responsiveness to security requirements)		AUTHORITY: Rhode Island General Laws (RIGL) 42-56-10 (v), Powers of the director	

I. PURPOSE:

To ensure protection of the security and integrity of all computer information systems and equipment maintained by the Rhode Island Department of Corrections (RIDOC). These systems include tiny information system operated by or connected to RIDOC's computers.

II. POLICY:

- A. Computerized information is protected from unauthorized access. Any external organization granted access to RIDOC's information systems is required to follow and enforce the security guidelines of this policy. The Associate Director of the Management information Systems (MIS) Unit grants such access.
- B. RIDOC operates and maintains all its automation resources, including multi-user computer systems, terminal devices, personal computers (PC's), workstations, networks, and communication devices to ensure:
 - 1. Accuracy and reliability of information regardless of whether it is stored or processed on RIDOC's information systems or on other computer systems;

2. Protection of each individual's right to privacy, where provided by law, concerning information about him/her which may be stored on RIDOC information systems;
 3. Accessibility to information by authorized users of RIDOC information systems;
 4. Denial of access to RIDOC information systems and information for all unauthorized persons;
 5. Detection of and intervention in attempted or actual system break-ins, information tampering and destruction, and all other forms of misuse of RIDOC information systems, computer equipment, computer networks, and information.
- C. Violation of the security requirements and procedures outlined in this policy may result in disciplinary action, up to termination.

III. PROCEDURES:

- A. This policy covers the following tangible assets of the Rhode Island Department of Corrections.
1. Any and all information regarding or related to RIDOC's business and mission, where that information is encoded as data contained in or on any information system or produced for display, and review by that system.
 - a. Such data may be recorded on a number of different media such as magnetic tapes, magnetic or optical disks, hard or floppy disks, a variety of printed forms, etc.
 - b. This data may be stored, processed, accessed, and displayed on any number of computer systems, including but not limited to those owned and operated by the RIDOC, its employees, contractors, and consultants.
 - c. The information systems equipment, specifically the computer hardware and software, peripheral devices, network components, data communication devices, terminals, personal computers, and printers which are owned, leased, and/or operated by the RIDOC store, process, and display information.
 - d. Access to and use of RIDOC's information systems.

- B. This policy covers the range of misuse from innocent accidents which cause little or no damage to malicious acts which cause data corruption, loss of information, and/or denial of services. It specifies the means to detect and prevent misuse and/or loss of any of these assets.
- C. Computer Security Oversight Committee
- I. Members of the Computer Security Oversight Committee, hereafter known as the Committee, are appointed by the Director. The Associate Director of MIS or designee chairs and provides staff support and technical guidance to the Committee. Committee membership includes representatives from the Office of Legal Counsel, Security, and Institutions and Operations Warden level).
 2. Security policies, procedures, and Department-wide compliance are reviewed annually by the Committee. All policies, procedures, guidelines, and inmate access exemptions in effect are the subject of an annual review. The annual review may result in revised policies; a review of exemptions to assure continued applicability; improved procedures and practices; and a report which summarizes findings, submitted to the Director or designee.
 3. The Committee reviews security policies and procedures whenever:
 - a. Significant technological operational changes occur, including but not limited to the introduction of major new computer installations, new networking and/or communications technologies, new applications and databases, and major upgrades to systems software components.
 - b. Significant Department organizational changes occur which affect the flow and distribution of work among groups, personnel reporting structures, or other changes which impact automation security.
 4. The Committee reviews the annual -physical security evaluations performed by functional unit managers and system operators within their functional units. The Committee also reviews and approves the physical security guidelines used for evaluation.
 5. The Committee reviews all interagency agreements, including:
 - a. Access to RIDOC's data by another agency or organization:
 - b. Transfer of data to or from another agency (data sharing);

Use of RIDOC's information systems resources (computers, networks, and other equipment *or* software).

- c. The Committee reviews all audit processes and reports which involve Information systems.

D. Access Authorization

1. Only authorized users are allowed access to RIDOC information systems
2. Authorized users are granted access to RIDOC information systems on a need-to-use basis by passwords.
3. Requests for user access and termination of user access are accepted by RIDOC's MIS Unit from functional unit managers. MIS personnel handle all written requests for access and termination from each functional unit. Letters of Agreement with external organizations for access to RIDOC information systems must clearly indicate the process and authority or user access authorization. Users from external organizations must comply with this rule.
4. Functional unit managers or their designees identify staff members with the need to use RIDOC information systems and are responsible for the following authorization process.

a. Security Agreement

- (1) Persons requesting access to RIDOC information systems must sign Request for Computer Access (Attachment 1) indicating they understand they are responsible for protecting agency assets, including computers and information, in accordance with the provisions of RIDOC's rules on release of public information, files, and records; computer information system access and security, in compliance with RIDOC's Code of Ethics and Conduct and Mission Statement. Functional Unit Managers approve such requests.
- (2) All Request for System Sign-On forms are maintained by the MIS Unit.

b. Training

Users receive instruction on access and security requirements (eg. ID's, passwords) for RIDOC information systems through:

- (1) MIS instructor;

- (2) peer trailing;
- (3) printed manual or instructions.

C. Termination of Access

Notice of termination of employment or transfer to a position not requiring access under these rules results in retirement or suspension of an individual user's identification by the MIS Security Officer. Prompt notice of termination or transfer is sent to RIDOC's MIS Unit by the Human Resources Office or designee who handles user authorization. Users from external organizations are bound by their organizations' security rules and regularions. Functional unit managers or their designees review a list of users from their respective units annually for accuracy. RIDOC's MIS Unit provides the list.

E. User Password Management and Responsibility

1. Authorized users shall comply with the following rules to create and manage their passwords.
 - a. All user accounts are protected by use of passwords at system sign-on time. The passwords are generated by and known only to individual users and the MIS Security Officer.
 - b. Passwords do not consist of vulgar words or have a personal association to the user, i.e., user name, family name, pet's name, child's name, etc.
 - c. Users are instructed that synthetic or nonsense, yet pronounceable sequences make good passwords (for example: "Bigblue" or "BUWBAH").
 - d. A minimum password length of four (4) characters is required.
 - e. Maximum password length is eight (8) characters.

2. Password Duration

- a. All users' passwords are subject to automatic retirement after a given time. Password expiration is as follows.
 - (1) An authorized user who has an account which allows him/her to modify information on the system has a password life of one hundred and eighty (180) days (Inmate

Accounts tellers, count board and visitation officers, data entry operators, to name a few).

(2) An authorized user who has an account which allows him/her inquiry only access has a password life of three hundred and sixty-five (365) days (Probation and Parole counselors, most administrative support and managerial staff).

- b- After said time, the user is required to supply a new password in compliance with the above rules.
- c. A user may not supply a previously used password since the system keeps a record of the last ten (10) passwords and rejects any repeats.
- d. Any account not used for a period of thirty (30) days will be deactivated- After ninety (90) days the account will be deleted.

3. Remote Computer Passwords

Since all remote computer systems (BCI, PROMIS, RILETS, etc.) do not fall under RIDOC's jurisdiction, these rules do *not* apply to those systems. However, RIDOC's MIS Unit determines who will have access to these remote systems,

4. Password Violation

Violation of the rules outlined above is a disciplinary matter, up to and including dismissal as a consequence. The following password management rules apply to all authorized users:

- a. Passwords should never be recorded on any media including paper, tape, or disk or embedded in software.
- b. Passwords are never shared with anyone, nor do users sign on to the RIDOC information system with their passwords so that other users may access the system.
- C. Neither authorized nor unauthorized persons shall use a password belonging to another *user*.

5. Result of Violation of Password Rule

- a. Suspected violation of password rules is reported immediately to RIDOC's MIS Unit.

- b. The supervisor or functional unit manager is notified by MIS of suspected violations in his/her unit.
- c. A user's account is disabled immediately by RIDOC's MIS Unit when a violation is confirmed.
- d. A user's account is automatically disabled when there have been more than three (> 3) unsuccessful attempts at sign-on within fifteen (15) minutes.

6. Personal Computer Network Access

- a. Users with personal computers (PC's) connected to network resources for the purpose of accessing and using file, disk, application, and printer services treat their PC's with the same care and diligence afforded terminals connected directly to a mini-computer system.

F. Management Information Systems Unit's Responsibilities for User Identification

To implement user accountability, the following rules are strictly enforced by the MIS Unit:

1. The same user identification (numeric value and/or user name) is never assigned to more than one user. Each user is assigned his/her own password.
2. Each user is authorized to use a unique account.
3. Generally, group accounts are not allowed. [A group account is a log-on or sign-on user name or password which is shared by more than one (> 1) person] If a user does not have a password, s/he contacts an MIS staff person, who will assign one. Exception: Floater codes are assigned to specific Main Control Centers (MCC's) and utilized by correctional officers assigned to those particular posts.
4. Open user accounts are not allowed. (An open user account is a log-in user name for which there is no password or for which the password is publicly known.)
5. Automatic log-in or sign-on is restricted to situations where access to applications by users from outside agencies (such as the Attorney General, Public Defender) is required and cannot be implemented by other means. Users from outside agencies pick from a menu, and the system automatically logs them into INFACTS.

6. Once an authorized user has logged on and no activity is detected for thirty (30) consecutive minutes, the terminal connection is automatically cancelled, and the user must log onto the system utilizing his/her identification and/or password.

G. Physical Security Guidelines

1. Computer equipment is protected from unnecessary risk of access, - damage, or theft.
2. Physical security guidelines for computer and telecommunications equipment shall be developed by the MIS Unit and reviewed and approved by the Associate Director of MIS before implementation.
3. An annual evaluation of physical security for computer and telecommunications sites is conducted by MIS staff. The findings of this evaluation are reported to the Associate Director of MIS.
4. Annual evaluations of physical security for computer equipment used by their respective staffs are conducted by functional unit managers or their designees; The findings of these evaluations are reported to the Associate Director of the MIS Unit.

H. Inmate/Probationer/Parolee Access

1. No inmate/probationer/parolee is permitted to enter, view, update, or manipulate information on RIDOC information systems EXCEPT by written exemption from the Corrections Director.
2. No inmate/probationer/parolee is issued or has access to a password. Sanctions are enforced for inmates/probationers/parolees who make unauthorized use of RIDOC information systems or computer equipment. Applications to which inmates/probationers/parolees have access, i.e., stand-alone systems, shall not include a system command line. Stand-alone personal computers may be used by inmates/probationers/parolees under the following conditions:
 - a. Inmates/probationers/parolees are only allowed to use computers provided by Education and Industries under the direct supervision of a unit staff member.
 - b. PC's are not to be attached to RIDOC information systems, operational networks, or to any other computer networks.
 - c. No confidential data is stored on the personal computer.

- d. Removable storage such as diskettes are restricted to necessary usage for the software application.

I. General Staff Responsibilities

Authorized users of RIDOC's information systems will ensure:

1. No external communication devices which allow exchange of computerized information over telephone lines (such as modems and fax machines) are connected, without MIS approval.
2. Personal computers are physically secured (keyboard locks, passwords). Physical security guidelines are provided by the MIS Unit, and the implementation of physical security is reviewed by MIS staff.
3. No inmate/probationer/parolee is granted access to RIDOC information systems without written permission from the Corrections Director.

J. Audits - MIS Security Officer

The MIS Security Officer conducts audits of user compliance with this policy on a random basis, at regular intervals. S/he submits audit reports to the Assistant Director of Administration via the Associate Director of MIS: Records and Identification.

K. Employee Discipline

The Associate Director of MIS: Records and Identification may refer staff who violate the provisions of this policy for discipline, consistent with RIDOC's established progressive discipline procedures.

L. Glossary

Attachment 2 contains a list of terms used throughout the policy and their definitions.



TITLE

OFFENDER ACCESS TO ELECTRONIC DATA

Page 1 of 2

EFFECTIVE DATE: December 31, 1996

SUPERSESSION:

None.

AUTHORITY:

General authority of the Secretary of Corrections to manage and direct the Department, RCW 72.09,050.

PURPOSE:

To establish guidelines for the access of electronic data by offenders.

APPLICABILITY:

Department-wide.

DEFINITIONS:

Electronic Data - Data stored electronically by a computer or data that is accessible by a computer.

Information Technology System - includes LAN, WAN, or stand alone computer is defined below.

Local Area Network (LAN) - A data transmission facility connecting computers and other communicating devices over a short distance (typically within a building or campus) under some form of standard control.

Administrative LAN - A LAN used to support general office and facility operational applications.

Correctional industries LAN - A LAN used to support operations of correctional industries operations.

Educational LAN - A LAN designed to support the Department's educational programs for offenders. It includes on-line testing of offenders and provides on-line instruction.

Offender - Those persons committed to the custody/supervision of the Department and offenders transferred from other states or the federal government.

Stand Alone Computer - Any computer not physically or logically connected to any other computer.

System Administrator - A person responsible for administering and controlling the local area network by assigning logon ids, establishing logical barriers, etc.

Wide Area Network - A data transmission facility connecting geographically dispersed (typically across the state, nation, or world) computers and peripheral devices under some form of standard control. Physically separate LANs are often logically linked through a WAN to allow transparent access to remote information (i.e., ODS, AFRS, ITAS, EMS).

POLICY:

- i Offenders using information technology systems shall not have direct access, either physically or logically, to information technology systems that will allow access to any outside or non-local electronic media, such as, but not limited to, mainframe applications, Internet, electronic bulletin boards, E-Mail, or on-line services.
- ii Access will be granted to local information technology systems as outlined below.



TITLE

OFFENDER ACCESS TO ELECTRONIC DATA

Page 2 of 2

- A. Offenders may have, upon local supervisory approval, access to local information technology systems for the purpose of performing their assigned work duties or education functions.
- B. If the local information technology system is connected logically or physically to the LAN/WAN, access rights to those applications available on the LAN/WAN will be restricted by the system administrator for any offender having direct access to the local information technology system.
- C. Any site where offenders are granted access must have in place appropriate physical and logical security protocols, such as password protection, keyboard locks, or other physical or logical barriers that are strictly enforced.
- D. Offenders will work only on designated workstations that will be physically and logically restricted from any outside applications referenced in I. above

REVIEW:

The Policy Coordination Committee shall coordinate the review of Department policies at least every two years and update as needed.

REFERENCES:

DOC Policy 801.001.

ATTACHMENTS:

None.

A handwritten signature in black ink, appearing to read "Chase Riveland".

Chase Riveland, Secretary



TITLE

EFFECTIVE DATE: June 1, 1998

SUPERSESION:

DOC 280.820 dated 12/13/96

AUTHORITY:

General authority of the Secretary of Corrections to manage and direct the Department, RCW 72.09.050.

PURPOSE:

To establish clear policies and procedures for Department of Corrections employees on the proper use of the Internet

APPLICABILITY:

Department-wide.

DEFINITIONS

Internet - The Internet is a collection of worldwide computer networks that allow computers anywhere in the world to link up with each other. The most common use of this network is to contact people with similar interests and exchange information, data, and E-mail. The Internet is not owned by anyone, nor sponsored by any country or corporation. It is largely unregulated and unpoliced. Since international borders are transparent to the Internet user; laws, customs, and morals of the user's own country may be contrary to the country the user is communicating with. For example: What may not be considered pornography in this country may be considered pornography in the country to whom the user is communicating. Also, copyright laws may not be honored in another country.

Local Area Network (LAN) - A network of computers in the same area or building connected together for the purpose of sharing files, peripherals, etc.

Stand-alone Computer - A computer that is not connected to a LAN or any wide area network

Electronic Mail (E-mail) - A process whereby a message is composed by a person and "mailed" electronically to another person over a computer network using specialized E-mail software. E-mail exchange has generally been the *most* popular Internet application. It is a fast, inexpensive way to communicate interactively with single or multiple users across the globe.

News Group/BBS Bulletin Board Service - A discussion group on the Internet in which participants with similar interests leave messages or other information for participants to read,

Worldwide Web (WWW) - Interactive links that form a web of connections across a worldwide computer network

Hyperlink - Each WWW page is linked to other WWW pages with hyperlinks. These are words, phrases, or graphics that are underlined, highlighted, or otherwise indicated. Each hyperlink is linked to the WWW address of a page containing additional information on the particular subject, it is basically a way of using an indexing system that allows Internet users to connect to linked documents along a route they select. When a topic is selected, the user is taken directly to the document that contains that information,



TITLE

INTERNET ACCESS

Page 2 of 5

Worldwide Web (WWW) Server - A computer attached to the Internet that provides a repository for WWW pages. A web server could be owned by the organization (Corrections for instance) to house only that organization's web pages. it could also be a multi-organizational server provided by a web page service provider, usually on a fee basis, that houses various organizations web pages

Worldwide Web (WWW) Home Page - The first document that generally appears upon accessing a WWW server is the 'Home Page.' A typical Home Page contains current information about a company, organization, or individual. it provides instant access 24 hours a day to organization information, press releases, data, pictures, or anything graphics or text oriented.

POLICY:

- A; Access to the Internet is established for the express use of Department personnel to enhance their ability to develop, design, and implement improved methods for delivering Department information and services to the public. it is intended to encourage and promote improved use of technology and information services for government. The Internet is unregulated and is open to unethical and illegal use. The only real safeguard lies in the informed, ethical, and responsible use of the Internet and the observance of existing laws by its users. Improper use by a Department employee could subject individual employees to disciplinary actions, and the Department to lawsuits and financial penalties.
8. The following general policies are to be observed by all persons using the Department's Internet **access** capability:
- 1, Business Use - Department-owned computers are to be used for the purpose of carrying out the 'official business' of the state. Employees, contract employees, and consultants may not use computers for private benefit or gain. Any private use of any and all state-owned property will be utilized in accordance with WAC 292-110-010 (Use of state resources) of the AGENCY SUBSTANTIVE RULES.
 2. A state officer or employee may make occasional but limited use of state resources only if;
 - a. there is no cost to the state;
 - b. the use of state resources does not interfere with the performance of the officer's or employee's official duties;
 - c. the use is brief in duration and does not disrupt or distract from the conduct of state business due to volume or frequency, and
 - d. the use does not compromise the security or integrity of state information or software; or
 - e. the agency has authorized a use that promotes organizational *effectiveness* or enhances the job-related skills of a state officer or state employee.
 3. Responsibility/Compliance/Termination of Access - Approving supervisors and employees are responsible for ensuring that employees use Internet resources in an effective, ethical, and lawful manner. Access to the Internet, therefore, must be conducted only in accordance with the requirements in this policy. Any employee found to be accessing the Internet in a manner not in compliance with this policy may have their Internet access immediately terminated and may be subject to disciplinary action. The information Technology (IT) Chief, Regional IT Manager, or the employee's approving authority may terminate the access of any employee abusing their Internet privileges.



TITLE

I N T E R N E T A C C E S S Page 3 of 5

4. Non-Employee Access - Access to the Department's Internet capability may be granted to non-employees (Le. consultants, contract staff, temporary help, etc.) when there is a clearly legitimate Departmental need to provide access to these type users. The approval and connection process is the same as for employees. All requirements contained in this policy apply-to this group of users as well as Department employees.
5. Inmate Use - No inmate or other offender under the supervision of the Department shall be allowed **access** to the Department's Internet capability.
6. Public Record - All Department generated Internet transactions (Le., messages, web pages, files, documents, etc.), that are carried out while conducting Department business using Department-owned computer resources are considered 'official' Department and state business and subject to the Public Records Law, Chapter 42.17.260 RCW. E-mail messages arc **not** to be considered 'private' communications between two or more people. A record of all WWW servers and net addresses contacted via Department owned resources will be maintained as necessary.
7. Message Content - All Department Internet users are responsible the the **content** of their messages and files. Fraudulent, harassing, or obscene messages and/or other materials must not be transmitted over the Internet. Messages that harass an individual or group because of their 'sex, race, religious beliefs, national origin, physical attributes, or sexual preference must not be transmitted over the Internet.
8. Internet Network Resource Integrity - Department Internet users must not deliberately attempt to degrade the performance of a computer system on the Internet or to deprive authorized personnel of resources or access to any computer system. Users must not attempt to gain unauthorized entry to resources **or** attempt to disrupt the intended use of the Internet. Department Internet users must not destroy the integrity of computer based information contained on the Internet.
9. Bypassing Security Systems - Department Internet users must not use loopholes in computer security systems or knowledge of a special password to damage computer systems, obtain extra resources, take resources from another user, gain **access** to systems, or use systems for which proper authorization has not been granted. Messages must not be sent under an assumed name or modified address or with the intent to obscure the origin of the **message**.
10. Use of Disclaimers - It is not acceptable when accessing the Internet to express personal views end opinions as if they constitute official policy of the Department of Corrections. Internet users must clearly indicate, by disclaimer, that non-official information contained in postings, E-mail messages, and other information disseminated through the Department's Internet connection does not necessarily represent the views and position of the Department of Corrections. (EXAMPLE: "The information contained herein is a personal opinion or position and is not intended to represent the views and/or position of the Department of Corrections').
11. Personal Gain - Department Internet users must not use the Internet to directly Initiate negotiations with others for personal financial gain. Department Internet users must not use a Departmental Internet E-mail account to acquire **contacts** for personal financial gain.
12. Illegal Activity - Department Internet users must not access the Internet for purposes that are illegal. Information and resources accessible via the Department Internet access are considered the property of the individuals and organizations that own the rights to those resources and these rights are to be protected.



13. Only the methods and providers of internet connection approved by Information Services shall be permitted. Such methods apply to both LAN connected personal computers and stand-alone computers. Only remote access and Internet software approved by DOC shall be used to access the Internet. Employees acting in their official capacity are to connect to the Internet only through DOC access entry points. The employee shall request the appropriate Internet-related software through the department's existing information technology resource approval process.
 14. All personal computers used to access the Internet shall utilize approved DOC virus scanning software in the start-up and operational processes of computing. Non-program files, such as documents or spreadsheets, have the ability to activate and spread virus programs when they are used. Therefore, all files, software, etc., downloaded from the Internet must be scanned with the approved virus scanning software. The downloading of executable files is expressly prohibited on computers without the standard virus protection software installed.
 15. The Department's policies and procedures regarding the proper use of electronic mail systems shall also apply to Internet mail. Department Internet users who wish to establish a personally identifiable Internet E-mail address may do so by requesting it through the procedures established by Information Technology. Email addresses will be provided when the technology is available.
 16. News groups are designed to be a source of discussion on the Internet. Because what is said in these news groups may be taken as an official Department position, approval to participate in a news group and the clearance of information provided as a participant in a news group must be given by the employee's supervisor. If an employee wishes to participate in a news group of a controversial nature, he/she is encouraged to include a disclaimer within the text of any document that the author is speaking for himself/herself and not as a representative of the Department of Corrections.
 17. The Department shall have only one WWW site and a single, central home page. Information Technology shall determine and arrange for the specific web site. Anyone who wants to add documents or information to the Department's Web Page must first submit the material to the Public Information Chief for approval. If approved, the appropriate IT staff shall prepare the material for inclusion into the department's Web Page and have it placed there.
- C. An employee requesting access to the Internet shall submit the 'Internet Access Request' E-form for approval. The approval process is the same throughout the Department.
1. The immediate supervisor shall review the employee's job requirements to verify that access would assist in job performance and provide clear benefit to the Agency. If so, the supervisor will forward the request to the approving authority for final approval.
 - a. In the OCO regions the approving authority shall be the Superintendent or Field Administrator;
 - b. OAS Field and Headquarters staff approval shall be the appropriate administrator;
 - c. OOS staff approval shall be the Secretary;
 - d. OCO Headquarters staff approval shall be the Assistant Deputy Secretary.
 2. After final approval is given the supervisor will establish the parameters for Internet use consistent with the employee's job requirements, monitor that use, and periodically review the continued need for access.
 3. After approval, the E-form shall be sent to the 'Internet Access Request' mailbox in EMS. A connection will then be coordinated with regional IT staff and the employee will be notified when it can be used.



TITLE

INTERNET ACCESS

Page 5 of 5

4. If the employee ceases to be employed by the Department, or a job change occurs whereby the employee no longer requires Internet, then the access must be terminated. An E-mail deletion request from the supervisor to the HQ Network IT manager is required.,
 5. Prior to accessing the Internet staff are required to have submitted the appropriate E-mail request acknowledging their responsibility with regard to Internet use and to have received area approval. In addition, access will not be granted until the proper training is administered.
- D. The electronic monitoring of all Internet use and activity is ongoing and continuous. Any and all misuse will be reported.

REVIEW:

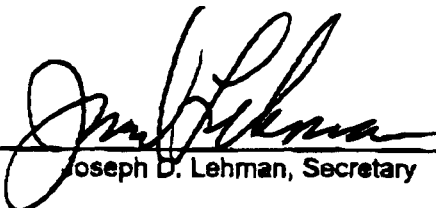
The Policy Review Committee shall coordinate the review of Department policies at least every two years and update as needed.

REFERENCES:

RCW 42.17; WAC 292-110-019 DOC 150.200,280.100, 830.300

ATTACHMENTS:

None



Joseph D. Lehman, Secretary



Date