

NH DEPARTMENT OF CORRECTIONS POLICY AND PROCEDURE DIRECTIVE	CHAPTER <u>Information Technology</u> STATEMENT NUMBER <u>11.03</u>
SUBJECT: INFORMATION TECHNOLOGY NETWORK & SYSTEMS ACCESS MANAGEMENT PROPONENTS: <u>William McGonagle, Assistant Commissioner</u> <i>Name/Title</i> Commissioner's Office 271-5601 <i>Office</i> <i>Phone #</i>	EFFECTIVE DATE 10/01/2011 REVIEW DATE <u>10/01/2012</u> SUPERSEDES PPD# <u>1.37; 11.02; 11.03 & 11.04</u> DATED <u>07/01/01 & 02/15/04</u>
ISSUING OFFICER: <hr/> William Wrenn, Commissioner	DIRECTOR'S INITIALS: _____ DATE: _____
REFERENCE NO:	

I. PURPOSE:

To establish a series of policies that present procedures and provide uniformity and control to ensure safety and integrity of DOC IT Systems, to include agency standards for DOC computer use, network access, DOC business applications and email.

II. APPLICABILITY:

To all Department of Corrections employees, inmates, and on-site contract personnel.

III. POLICY:

A. Safeguarding DOC Networks and Applications

It is the policy of the Department of Corrections (DOC) to control access to departmental databases and computers and to safeguard the privacy of individuals under departmental control. The DOC shall establish common and uniform policies in order to protect authorized users and using entities of DOC computers, systems, and networks.

B. Authorized Users

Authorized Users shall be defined as:

1. All DOC Employees with permitted access.
2. Volunteers or Interns permitted access for conducting DOC Business.
3. DOC Contractors with permitted access under agreed terms and conditions.
4. Inmates with restricted access for performing authorized prison functions.

C. Inmate Access

Unauthorized restricted inmate use of any DOC computers and computer devices with network access is strictly prohibited. Any DOC employee, volunteer, intern or contractor facilitating such access directly or by failing to maintain proper computer security may be subject to disciplinary action.

D. Network Access and Control

1. The DOC shall establish a centralized unit, known as the Business Information Unit (BIU), for the purpose of managing access, control and security of all DOC Computers, business applications, data and networks.
2. The DOC and the BIU reserve the right to monitor user utilization, to check system performance to ensure computers, systems, business application and networks are used properly, and to restrict access on the network when appropriate.

E. Computer Use

1. All DOC computer and network equipment are property of the Department of Corrections and are to be used for DOC business only. The DOC shall establish security and best practices that adequately protect against unauthorized modification, disclosure, or destruction of its computers, business applications, data and networks.
2. DOC supervisors and directors shall ensure the appropriate levels of security and access for the authorized users they are responsible for.
3. Authorized Users have the responsibility to protect information from unauthorized access, misuse, theft, damage, destruction, modification or disclosure. Any person or any use not specifically known by an Authorized User shall be promptly reported to the appropriate supervisor.
4. All DOC equipment, business applications and information property of the DOC shall be used solely for the purpose of conducting official DOC business. All other use is strictly forbidden.
5. At no time shall an Authorized User knowingly access or attempt to access restricted equipment or information with out having the appropriate approval(s) or authority to do so.
6. At no time shall an Authorized User knowingly access or attempt to access restricted equipment or information that is inconsistent with DOC policy, procedures, and/or agreements relating to system entry access.
7. All information developed utilizing DOC resources or facilities shall be the exclusive property of the DOC unless agreed upon by a formal process, i.e., Research Requests and Memoranda of Understanding.
8. Only software owned and licensed or agency approved by DOC may be used by an Authorized User for conducting DOC business. All software owned, licensed or developed for DOC shall not be copied, shared, sub-licensed, distributed, modified, rented or sold.
9. Personal or third party software and computer devices shall not be installed on any DOC equipment without the appropriate authorization(s), approval(s) and certification(s).
10. The DOC shall establish a Computer Password Policy that ensures safe access to all DOC computers, business applications, data and networks that includes, but is not limited to, the use of unique user names and passwords for all Authorized Users.
11. It shall be the responsibility of an Authorize User to manage their assigned unique user name and password. Under no circumstances are user names and passwords or other assigned access privileges to be compromised.
12. It shall be the responsibility of the Authorized User to ensure that all computers and workstations are secure from unauthorized access.

F. E-mail Use

1. The DOC shall provide an E-Mail system to promote open communication and exchange of information. E-mail and other forms of electronic communication conducted on DOC equipment shall be for the purpose of DOC business only and is the property of the DOC and the State of New Hampshire.
2. E-mail is defined as "internal E-Mail system or "state funded e-mail systems." E-mail is not encrypted and is not secure nor does it guarantee personal privacy.
3. The DOC shall develop and implement procedures for managing E-mail resources, this includes but is not limited, management of user accounts, standards and best practices,

- utilization, storage and retention.
4. All E-Mail correspondence should follow the guiding principles of composition and should be relevant, brief and written clearly in a professional tone.
 5. All E-Mail correspondence to a non DOC entity should be composed and attached as a letter sent on official DOC Letterhead and be subject to appropriate supervisory review.
 6. All E-Mail is subject to discovery in legal proceedings so content must meet standards of accuracy and truthfulness.
 7. The following use of E-mail is strictly prohibited:
 - a. Any unlawful purpose
 - b. Content or material that is insulting, demeaning, harassing or threatening,
 - c. Distribution of pornographic, obscene or distasteful materials
 - d. Use abusive or profane language or language that offends or discriminates against race, religion, sex, sexual orientation, age, disability, religion.
 - e. To profess political belief or point of view.
 - f. Personal or commercial business or entertainment
 - g. Any use that reflects poorly on the DOC or State of New Hampshire
 - h. Lobbying
 8. Authorized Users shall not use E-mail to misrepresent their identity or authority, including using another's Authorized User's ID and password.
 9. The BIU may monitor an Authorized User's use of the E-mail system and has the authority restrict or prohibit access for inappropriate or excessive use. The Authorized User's supervisor will be notified for appropriate disciplinary action or training.

G. Internet and Intranet Use

1. The DOC shall provide internet/intranet services to promote open access and exchange of information with the public, governments, DOC employees and other DOC partners for the purpose of conducting DOC business on the world wide web or DOC intranet. DOC internet / intranet access shall be available to DOC employees whose job function(s) and roles and responsibilities demonstrate a business need for access. All access is granted for conducting DOC business only. Personal use, entertainment and other non-DOC business uses are strictly prohibited.
2. Internet /Intranet Accountabilities:
 - a. DOC and the BIU are responsible for all network and DOC systems security. It shall be the responsibility of the DOC to ensure that all safety measures are taken to ensure protection of all DOC systems and networks against unauthorized access, misuse, theft, damage, destruction, modification or disclosure.
 - b. In addition, the DOC shall monitor and control internet and intranet usage and establish standards and measures for ensuring that utilization does not exceed the limits of its resources that include bandwidth, CPU and disk utilization.
 - c. DOC Supervisors and Directors are responsible for monitoring and controlling the methods and appropriateness of Authorized Users access. An Authorized User may be denied internet/intranet access or to the Department's network for inappropriate usage.
 - d. All Authorized Users must demonstrate acceptable internet/intranet conduct and usage that includes, but is not limited to:
 - 1) Only used for official DOC business/communications.
 - 2) Only used for DOC Research or educational purposes.
 - 3) Data communications in accordance with applicable laws.
 - e. Authorized Users who receive internet/intranet browsing privileges must comply with the following:
 - 1) All applicable laws and regulations.
 - 2) Shall not reproduce or transmit any prohibited material or material in violation of any local, state, U.S., or international law or regulation.
 - 3) Shall not violate or infringe any patent, trademark, copyright, statutory, common law

or proprietary rights of others.

- 4) Shall not produce or transmit any obscene, libelous or threatening materials are prohibited.
- 5) Shall defend, indemnify and hold harmless the Department from and against any claims, liabilities and expenses, including attorneys' fees, resulting from employee's use of the Department service or employee's account in an unlawful manner or otherwise in violation of or contrary to employee's agreement with the Department or the Department's Acceptable Use Policies.

H. Inmates and the DOC Network

1. No inmate will have access to the DOC Network; this includes access to internet/intranet or e-mail across the DOC network.
2. Inmates will not work on computers with access or have had access to the Department's network.
3. Inmates will not work on any portion of the Department's networks.
4. Should an inmate's duties require working on a DOC network computer, that computer will not be connected, or be in a position to be connected to the Department's network. wherein such rare circumstances the inmate will perform the required tasks only under the direct supervision of an Authorized User who will assure that the inmate does not access the Department's network or the internet/intranet.
5. No inmate will be selected for computer-based work if that individual has been convicted of computer fraud or has any known criminal activities involving computers anywhere in his or her background.
6. Certain areas including, but not limited to, law libraries, correctional industries, educational venues, Family Connections Centers and discharge planning centers may allow for inmate computer usage.
7. Such access will be limited to stand-alone computers or authorized computer networks that are completely separate from the DOC Network.
8. Internet access may be appropriate with adequate controls and supervision for purposes such as virtual visitation (FCC), distance learning or discharge planning.
9. DoIT will be responsible for periodic review of security equipment, wiring and software to monitor for appropriate usage.

I. Right to Disconnect Non-Dedicated Accounts

1. The Department's Virtual Private Network (VPN) or remote access connections are not intended to be full-time dedicated connections. The Department reserves the right to impose a restriction on accounts deemed by it to be in violation of these conditions.

J. Monitoring/Privacy

1. The Department reserves the right to monitor any and all communications placed over the Department's systems. The Department is not considered a secure communications medium for the purposes of the Electronic Communications Privacy Act, and no expectation of privacy is afforded. It may become necessary for the DOC to examine system accounting logs and other records to determine if privacy violations or other violations of network or computer protocols have occurred. The Department also reserves the right to access an employee's mailbox or other files stored on the Department systems to resolve system problems or mail system errors.

K. Cooperation with Authorities

1. The Department reserves the right to cooperate with law enforcement and other authorities in investigating claims of illegal activity including, but not limited to, illegal transfer or availability of copyrighted material, postings or E-Mail containing threats of violence or other illegal activity.

L. Confidentiality of Personal Employee Information

1. The Department will not release an employee's personal employee information to any third

party except upon presentation of a valid court order of a government or entity within our jurisdiction. Employee agrees that the Department's judgment as to the validity of any court order of subpoena shall be considered proper and final.

M. Right to Damages

1. The Department reserves the right to collect damages (software, hardware and man-hours) if any harm is done to the Department that requires repair or reconfiguration work.

N. Computer and Network Security

1. The Department shall establish password policy that adequately protect against unauthorized access, modification, disclosure, or destruction and complies with all State policy and standards establish by the Department of Information Technology.
2. The Department shall incorporate all Department of Information Technology anti-virus policy and procedures to ensure the protections and safety of all its networks, applications and computer systems against computer viruses intended to disrupt, damage or destroy normal operations.

IV. Procedures:

A. Managing Access to DOC Computers, Systems & Networks

1. To gain access to any secured application/report, to establish a user account on the DOC network, or to receive e-mail/internet access privileges, the user must complete an "IT User Access Request Form" (attachment 1). The form will require:
 - a. User Identifying Information
 - b. Network Access Type
 - c. Secured Application/Report Name
 - d. Specified access /use within of application/report
 - e. Signatures of Authorizing Personnel
2. Once an "IT User Access Request Form" has received the designated levels of approval, the request must be sent to the Business Information Unit (BIU) for final review and submission to the DoIT for technical assistance/services.
3. Each employee of the DOC with access to any DOC computer equipment, the DOC network, DOC business applications, e-mail, internet/intranet and/or data must complete a "DOC User Access Agreement". A completed user agreement with the employee's signature will be a part of the employee's employment record. The "DOC User Access Agreement" should be completed at the time of starting employment with the DOC, when there are significant revisions to the agreement or at any other discretionary point-in-time.
4. The DOC User Agreement may include, but is not limited to, and Authorized Users agree to the following:
 - a. That at no time shall the employee's confidential computer user name(s) password(s) be shared with or used by any other person.
 - b. That at no time shall the employee share or use another person's confidential computer password.
 - c. That at no time shall the employee leave a workstation without first ensuring that the workstation is properly secured from unauthorized access.
 - d. That the employee must report any and all violations of this agreement to the appropriate Supervisor promptly upon learning of such violation.
 - e. That if the employee is found to be in violation of any of the above state rules.
 - f. That at all times utmost care shall be used in protecting departmental information from unauthorized access, misuse, theft, damage, destruction, modification or disclosure.
 - g. That any person or any use not specifically known by the employee as being authorized to access or use departmental information must be promptly called in to the Business Information Unit (BIU).
 - h. That departmental information shall be used solely for the purpose of conducting official department business, and all other use or access is strictly forbidden including, but not

limited to, personal or other private use.

- i. That at no time shall the employee access or attempt to access any departmental information without having the express authority to do so.
- j. That at no time shall the employee access or attempt to access any departmental information in a manner inconsistent with the approved method of system entry.
- k. That all departmental information developed while on the job or while utilizing Department facilities or resources shall be the exclusive property of the Department of Corrections.
- l. That all software licensed, developed or being evaluated by the Department cannot be copied, shared, distributed, sub-licensed, modified, reverse engineered, rented or sold, and that at all times the employee must use utmost care to protect and keep such software strictly confidential in accordance with the license or any other agreement executed by the Department.
- m. That only equipment or software owned, licensed or being evaluated by the Department can be used by the employee.
- n. Use of personal or a third party's equipment or software at Department facilities is strictly forbidden unless prior written approval has been obtained from the BIU Administrator.
- o. The employee may face disciplinary sanctions, including a reprimand, suspension, termination from employment or criminal or civil prosecution if the act constitutes a violation of law.
- p. That from time to time circumstances may require that this agreement be modified by the Department to reflect any changes in procedure or policy. The employee will be notified in writing of any changes and will be required to adhere to such changes.

REFERENCES:

Standards for the Administration of Correctional Agencies
Second Edition Standards

2-CO-1F-06

Standards for Adult Correctional Institutions
Fourth Edition Standards

Standards for Adult Community Residential Services
Fourth Edition Standards

Standards for Adult Probation and Parole Field Services
Third Edition Standards

3-3111

Other:

NH General Court – Revised Statutes Annotated (RSA)

- [Title LXII, Criminal Code; Section 638:16 Computer Crime; Definitions.](#)
- [Title LXII, Criminal Code; Section 638:17 Computer Related Offenses.](#)
- [Title LXII, Criminal Code; Section 638:18 Computer Crime Penalties.](#)
- [Title LXII, Criminal Code; Section 638:19 Venue.](#)

NH Department of Information Technology Policy

- Statewide Standards and Policies;
<http://www.nh.gov/doi/intranet/toolbox/standards/index.php>
- State Standard Procurement Procedures & Guidelines;
<http://www.nh.gov/doi/intranet/toolbox/procurement/index.php>
- Procurement Resources –State Standard Products;
<http://www.nh.gov/doi/intranet/toolbox/procurement/standardproducts.php>

MCGONAGLE/pf
ATTACHMENTS

Sample Network & Systems Access Form – Visit [the IT@DOC Intranet Home Page](#) for the most current form.

Section 1: Requestor's Information		Attention: New users must attach a completed DOC IT User Access Agreement. Visit IT@DOC on the intranet for the agreement.	
Name: [REDACTED]	Title: [REDACTED]		
Location : Building / Facility [REDACTED]	Division/Unit: [REDACTED]		
Telephone (XXX-XXXX): [REDACTED]	E-mail: [REDACTED]		
Request Date: [REDACTED]	Effective Date: [REDACTED]		
Section 2: DOC Network Access (select all that apply)			
<input type="checkbox"/> Network Account	<input type="checkbox"/> New <input type="checkbox"/> Change <input type="checkbox"/> Delete	Set Up Network Account like (name of similar user) [REDACTED]	
<input type="checkbox"/> E-Mail	<input type="checkbox"/> New <input type="checkbox"/> Change <input type="checkbox"/> Delete		
<input type="checkbox"/> Internet	<input type="checkbox"/> New <input type="checkbox"/> Change <input type="checkbox"/> Delete	Specify need for access: [REDACTED]	
Section 3: DOC Applications (select all that apply)			
Application	Access type (name of similar user)	Reason for Access?	
<input type="checkbox"/> CORIS	[REDACTED]	[REDACTED]	
<input type="checkbox"/> CHOICES	[REDACTED]	[REDACTED]	
<input type="checkbox"/> Connections	[REDACTED]	[REDACTED]	
<input type="checkbox"/> RADAR	[REDACTED]	[REDACTED]	
<input type="checkbox"/> SGT. Major	[REDACTED]	[REDACTED]	
<input type="checkbox"/> SNAP	[REDACTED]	[REDACTED]	
<input type="checkbox"/> Secured Report	Name of Report [REDACTED]	[REDACTED]	
<input type="checkbox"/> Other	Other Name: [REDACTED]	[REDACTED]	
Section 4: Authorizations/Approvals			
Requestor:	[REDACTED]	Date:	[REDACTED]
Unit Supervisor:	[REDACTED]	Date:	[REDACTED]
Facility Director/ Warden:	[REDACTED]	Date:	[REDACTED]
BIU Admin	[REDACTED]	Date:	[REDACTED]
Section 5: BIU Use Only			
<input type="checkbox"/> Approved	BIU Comments:	BIU Action:	Date: [REDACTED]
<input type="checkbox"/> Denied	[REDACTED]	<input type="checkbox"/> Sent to requestor's Supervisor	
<input type="checkbox"/> Other	[REDACTED]	<input type="checkbox"/> Sent to Help Desk	
By: [REDACTED]	[REDACTED]	<input type="checkbox"/> Other [REDACTED]	

NH Department of Corrections
Information Technology
USER ACCESS AGREEMENT

Any and all NH Department of Corrections (DOC) employees, volunteers ,contractors or other entities given permitted access to any DOC computer, network, business application, E-mail and internet/intranet browsing access acknowledges by signing this agreement, to comply with all federal and state laws and rules, and DOC policies and procedures governing the use and safeguarding DOC IT systems.

The authorized user agrees:

1. That at no time shall the employee’s confidential computer user name(s) password(s) be shared with or used by any other person.
2. That at no time shall the employee share or use another person’s confidential computer password.
3. That at no time shall the employee leave a workstation without first ensuring that the workstation is properly secured from unauthorized access.
4. That the employee must report any and all violations of this agreement to the appropriate Supervisor promptly upon learning of such violation.
5. That if the employee is found to be in violation of any of the above state rules.
6. That at all times utmost care shall be used in protecting departmental information from unauthorized access, misuse, theft, damage, destruction, modification or disclosure.
7. That any person or any use not specifically known by the employee as being authorized to access or use departmental information must be promptly called in to the Business Information Unit (BIU).
8. That departmental information shall be used solely for the purpose of conducting official department business, and all other use or access is strictly forbidden including, but not limited to, personal or other private use.
9. That at no time shall the employee access or attempt to access any departmental information without having the express authority to do so.
10. That at no time shall the employee access or attempt to access any departmental information in a manner inconsistent with the approved method of system entry.
11. That all departmental information developed while on the job or while utilizing Department facilities or resources shall be the exclusive property of the Department of Corrections.
12. That all software licensed, developed or being evaluated by the Department cannot be copied, shared, distributed, sub-licensed, modified, reverse engineered, rented or sold, and that at all times the employee must use utmost care to protect and keep such software strictly confidential in accordance with the license or any other agreement executed by the Department.
13. That only equipment or software owned, licensed or being evaluated by the Department can be used by the employee.
14. Use of personal or a third party’s equipment or software at Department facilities is strictly forbidden unless prior written approval has been obtained from the BIU Administrator.
15. The employee may face disciplinary sanctions, including a reprimand, suspension, termination from employment or criminal or civil prosecution if the act constitutes a violation of law.
16. That from time to time circumstances may require that this agreement be modified by the Department to reflect any changes in procedure or policy. The employee will be notified in writing of any changes and will be required to adhere to such changes.

Confidential and Non-Disclosure Use

The State of New Hampshire and the Department of Correction’s shall be classified as “Confidential” unless otherwise specified and be protected from unauthorized disclosure.

Under no circumstances shall an Authorized User disclose to the public, or any other individual, any confidential information pertaining to the NH Department of Corrections and its affiliates.

Authorized User’s Signature: _____ Supervisor’s Signature: _____

Date: _____ Date: _____

Computer Password Policy

Policy: State of New Hampshire information technology systems shall be protected with secure password management.

Accountability: This policy pertains to all users and all levels of log in accessing, directly or through an indirect source, the State of New Hampshire IT environment. This policy also applies to anyone who has the responsibility for managing the State of New Hampshire IT environment or any portion of it.

Purpose: Information handled by State of New Hampshire IT systems must be adequately protected against unauthorized modification, disclosure, or destruction. Unique user ids and passwords enable auditing and tracking of user activity.

Description: Passwords are intended to prevent unauthorized access to State of New Hampshire systems and to ensure that users can access only the work they are authorized to. Password standards should reflect the security risks of the system or application they are intended to protect. Agency administrators should assess the risk of their systems and implement an appropriate level of password protection. The DOC shall establish the DoIT *Computer Password Standards* that provide password characteristics for a high-risk system such as a network log in.

To ensure proper password administration, the following good practices should be adhered to:

- passwords should never be written down;
- password history files should be encrypted;
- creation, alteration and termination of accounts should be requested through a formal process;
- awareness of password policies should be promoted periodically;
- user ids and passwords should be deleted in a timely manner;
- passwords should be checked proactively for validity; unauthorized login attempts should be logged;
- users should be required to change passwords upon initial use of the system;
- user verification should be done before resetting passwords;
- common user ids and passwords may be warranted under certain circumstances but should never be allowed when financial or confidential data is involved.

Users must comply with all rules set up by the administrator. Users should only work on a computer system while logged on with their own user id and must never share passwords. Passwords using personal information are not allowed. Passwords should not be easy to spot when typing.

Compliance: Personnel rules 1001.03 (written warning) and 1001.08 (dismissal) should be applied as needed. It may be grounds for dismissal if an administrator or user willingly gives out his or her logon id and password for the express purpose of unauthorized modification, disclosure, or destruction of state information.

The first offense of an administrator or user giving his or her password to another person may result in a written warning along with a training session on password security. Subsequent offenses may result in the withholding of an annual increment, suspension, demotion, or dismissal. Writing a password down where it could be found by another person can be considered to be a violation of this rule.