

STATE OF OHIO



DEPARTMENT OF REHABILITATION
AND CORRECTION

SUBJECT: Internet, Electronic Mail, and Online Services Use	PAGE <u> 1 </u> OF <u> 5 </u>
	NUMBER: 05-OIT-10
RULE/CODE REFERENCE:	SUPERSEDES: 05-OIT-10 dated 02/21/11
RELATED ACA STANDARDS:	EFFECTIVE DATE: September 13, 2011
	APPROVED: 

I. AUTHORITY

This policy is issued in compliance with Ohio Revised Code 5120.01 which delegates to the Director of the Department of Rehabilitation and Correction the authority to manage and direct the total operations of the Department and to establish such rules and regulations as the Director prescribes.

II. PURPOSE

The purpose of this policy is to establish security requirements for the appropriate use of Ohio Department of Rehabilitation and Correction information technology system assets.

III. APPLICABILITY

This policy applies to all employees of the Ohio Department of Rehabilitation and Correction (DRC) and other individuals such as DRC contractors and DRC volunteers who by virtue of their job duties, roles, responsibilities or assignments, request and/or receive access to Ohio Department of Rehabilitation and Correction information technology system assets.

IV. DEFINITIONS

DRC Information Technology Governance Group (ITGG) – The multi-disciplinary leadership group, chaired by the Deputy Director of the Office of Administration and comprised of DRC executive staff and administrators from the Office of Administration, Bureau of Information Technology Services (BITS), charged with the responsibility of guiding DRC’s information technology biennial plan to ensure that information technology system assets are identified, obtained, and utilized in an efficient and effective manner to achieve and sustain DRC’s mission and business continuity.

Highly Secure System Access - DRC information technology access given to users whose duties, roles, responsibilities, or assignments require access to highly secure and controlled DRC system assets such as mental health and medical data and systems.

Non-DRC System Access - Non-DRC information technology access given to users whose duties, roles, responsibilities, or assignments require access to non-DRC networks, data and/or services or resources such as LEADS and OHLEG.

Regular System Access - DRC information technology access given to users whose duties, roles, responsibilities, or assignments require access to basic, standardized DRC system assets such as DOTS Portal, OSP, ORAS or FOT.

Specialized System Access - DRC information technology access given to users above the regular system asset level whose duties, roles, responsibilities, or assignments require access to additional DRC system assets such as the internet, virtual privacy network (VPN) or air cards.

System Assets - Computer hardware, software, networks, data and/or services or resources that are necessary to support the information technology requirements of the Ohio Department of Rehabilitation and Correction and, therefore, must be protected by the appropriate security requirements to ensure business continuity.

V. POLICY

It is the policy of the Ohio Department of Rehabilitation and Correction to establish security requirements to protect DRC information technology system assets such as the internet, electronic mail, online services, and the virtual private network in order to ensure business continuity.

VI. PROCEDURES

- A. DRC information technology system assets contain data that is the property of DRC. Said data is subject to inspection and, depending upon its content, may be subject to public records laws.
- B. DRC has the capability to monitor the use of all DRC information technology system assets and shall do so when deemed appropriate. Any suspected misuse of DRC system assets shall be reported to the DRC Office of the Chief Inspector.
- C. DRC reserves the right to limit and restrict access to all DRC information technology system assets. In order to protect the security of DRC information technology system assets, all access requests from DRC employees and others, such as DRC contractors and DRC volunteers, shall be documented via submission of a System Access Request Form (DRC3424) and shall be reviewed and approved by one or more management levels as follows:
 1. For regular system access, the immediate supervisor, or appropriate supervisor if a DRC contractor, DRC volunteer or other external individual, shall review and approve the request.
 2. For specialized system access, the immediate supervisor, or appropriate supervisor if a DRC contractor/volunteer or other external individual, and the Managing Officer/designee shall review and approve the request.
 3. For highly secure system access, the immediate supervisor, or appropriate supervisor if a DRC contractor/volunteer or other external individual, and the Managing

Officer/designee shall review and approve the request. In addition, the appropriate Operation Support Center administrator representing the data owner shall review and approve the request.

- D. Approved System Access Request Forms (DRC3424) shall be submitted by the final approving supervisor/manager/administrator to the DRC Information Service Center at the Operation Support Center where Help Desk staff shall create the appropriate user account.
- E. In order to obtain access to non-DRC information technology systems, networks or data, DRC employees and other individuals, such as DRC contractors and DRC volunteers, shall follow all access request policies and procedures of the non-DRC agency that owns or hosts the information technology systems, networks or data.

The DRC employee or other individual shall complete the appropriate access form from the non-DRC agency and submit the form to the immediate supervisor, or appropriate supervisor if a DRC contractor, DRC volunteer or other external individual, for review and approval. Upon approving the request, the immediate/appropriate supervisor shall submit the form to the non-DRC agency for creation of the account.

- F. The system access request/approval process outlined in this policy for regular, specialized, and highly secure DRC system asset user groups and non-DRC user groups can be modified only with the approval of the DRC Information Technology Governance Group.
- G. DRC employees and other individuals, such as DRC contractors and DRC volunteers, who receive access to DRC information technology system assets shall follow all DRC security requirements:
 - 1. All DRC information technology system assets, including the internet, electronic mail, on-line services, and VPN access shall be used for business purposes only. Signature lines on electronic mail shall be restricted to business-related information such as name, title, and contact information.
 - 2. Employees and other individuals with DRC system asset accounts, such as the internet, electronic mail, online services, and the VPN, shall not:
 - a. Use any system asset for operating a business or for personal gain; supporting a non-DRC activity or organization; sending chain letters; soliciting money or services; purchasing non-business goods or services or for religious or political purposes.
 - b. Send or distribute any unsolicited electronic mail, commonly referred to as "spam," to individuals who have no direct interest in the subject matter of the electronic mail, including employees of DRC and other state agencies.
 - c. Use an electronic mail "global distribution list" unless they are a member of the list or are using the distribution list for a legitimate business purpose.
 - d. Use electronic mail for non-business communications.

- e. Create or distribute communications, including images, that contain offensive or harassing statements, including disparaging or derogatory statements about others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.
- f. Create or distribute communications including images that contain incendiary statements which might incite violence or describe or promote the use of weapons or devices associated with illegal activities.
- g. Use their DRC accounts for recreational purposes such as downloading or playing computer games, gambling, or to send, distribute or solicit sexually oriented messages, materials or images.
- h. Use their DRC accounts to download, distribute, or print copyrighted materials including articles, books, software, or images in violation of copyright laws.
- i. Use their DRC accounts to download or order non-DRC software, software service packs, or software updates to any State of Ohio owned or leased computer, peripheral device, communication line or network.
- j. Use a DRC account or any non-DRC information system account for non-business purposes to access personal or confidential information about an individual.
- k. Use another DRC system asset user's account or signature line.
- l. Share their DRC system asset user account information with another individual or display their DRC system asset user account information in a location that can be viewed by others.
- m. Share confidential data from DRC system assets with individuals that do not have a legitimate, business need for the data.
- n. Misrepresent their duties, roles, responsibilities or assignments to obtain a DRC system asset user account.

H. Workstation Management Procedures for DRC Facilities

1. Security

- a. Any internet workstation in a correctional facility must be located in a secure area (in a locked cabinet or behind a locked door).
- b. Operation Support Center and Division of Parole and Community Services staff shall take the necessary precautions to secure their computer from offenders who may be in the area. This may include locking the computer, logging off the computer, or shutting the computer down when leaving the area.

2. Laptop Computers

- a. DRC employees or other individuals who are authorized to use State of Ohio owned or leased computer equipment outside of DRC sites shall inform the Chief of the Bureau of Information and Technology services, in writing using an Incident Report (DRC1000) pursuant to Department Policy 01-COM-08, Incident Reporting and Notification, in the event of theft or loss of any state computer.
- b. DRC employees or other individuals who are authorized to use State of Ohio owned computer or leased equipment outside of DRC sites shall inform the Chief of the Bureau of Information and Technology services in writing using an Incident Report (DRC1000) pursuant to Department Policy 01-COM-08, Incident Reporting and Notification, in the event that the security (passwords) of the computer or laptop is compromised.

Related Department Forms:

Incident Report

DRC1000

Systems Access Request Form

DRC3424