

SUBJECT: Internet, Electronic Mail, and Online IT Services Use	PAGE <u> 1 </u> OF <u> 10 </u>
	NUMBER: 05-OIT-10
RULE/CODE REFERENCE:	SUPERSEDES: 05-OIT-10 dated 01/08/18
RELATED ACA STANDARDS:	EFFECTIVE DATE: February 4, 2019
	APPROVED: 

I. AUTHORITY

Ohio Revised Code 5120.01 authorizes the Director of the Department of Rehabilitation and Correction, as the executive head of the department, to direct the total operations and management of the department by establishing procedures as set forth in this policy.

II. PURPOSE

The purpose of this policy is to establish security requirements for the appropriate use by authorized users of Ohio Department of Rehabilitation and Correction and Ohio Department of Administrative Services, Office of Information Technology (DAS OIT) information technology (IT) system assets, pursuant to the DAS OIT Policy 700-001, Information Technology Resource Usage.

III. APPLICABILITY

This policy applies to all Ohio Department of Rehabilitation and Correction (ODRC) authorized users of ODRC and DAS OIT system assets.

IV. DEFINITIONS

Authorized User - An ODRC employee, contractor, intern, volunteer or other agent of the State who is authorized at a technical level to administer and support/maintain state computing IT systems and telecommunications technology systems or is authorized at an end user level to have access to and use State computing IT systems and telecommunications technology systems for business purposes on behalf of the State of Ohio.

Cloud Computing - The “cloud” is a metaphor for the internet; therefore, cloud computing is a type of internet-based computing that utilizes shared internet resources, such as servers, applications, and storage, rather than local services or personal computing devices. Cloud infrastructure is maintained by the cloud provider, not the individual cloud customer.

Cloud File Sharing Solutions - Online, internet-based services in a cloud infrastructure that allow users to store and synchronize documents, photos, data, videos and other files, and share them with multiple users across multiple computing devices, such as desktops, notebooks, smartphones and media tablets.

DRC Information Technology Governance Group (ITGG) - The multi-disciplinary leadership group, chaired by the deputy director of the Office of Administration and comprised of ODRC executive staff and administrators appointed by the Office of Administration deputy director and Bureau of Information Technology Services (BITS), charged with the responsibility of guiding ODRC's IT biennial plan to ensure IT system assets are identified, obtained, and utilized in an efficient and effective manner to achieve and sustain ODRC's mission and business continuity.

eDiscovery - The production of files or other data held in an electronic form, such as e-mail, wherein "discovery" refers to the process of complying with legal obligations to produce relevant documents and information to opposing counsel in the course of civil litigation or to prosecutors or government investigators in criminal or regulatory proceedings.

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

Instant Messaging (IM) - A software tool that allows real-time electronic messaging or chatting. IM services use "presence awareness," indicating whether people on an authorized user's list of contacts are currently online and available to IM/chat.

Internet - A worldwide system of computer networks (a network of networks) in which computer users can get information and access services from other computers. The internet is generally considered to be public, untrusted and outside the boundary of the State of Ohio enterprise network.

Internet Forum - An online, internet discussion site where individuals can hold conversations in the form of posted messages. Examples include message and discussion boards and their associated threads, blogs and listserv applications.

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

Office 365 - Also called "Microsoft 365" or "Microsoft Office 365" is a Web-based version of the Microsoft Office suite of enterprise productivity applications, such as Exchange Online for e-mail and Skype for Business, provided to users through Cloud Computing infrastructure. Office 365 is a mission critical tool used by Authorized Users.

Peer-to-Peer (P2P) File Sharing - The direct sharing of content like audio, video, data software or anything in digital format between two computers connected to a network without the need for a central server.

Personally Identifiable Information (PII) - Information that can be used directly or in combination with other information to identify a particular individual. PII includes:

- A name, identifying number, symbol or other identifier assigned to a person.
- Any information that describes anything about a person.
- Any information that indicates actions done by or to a person.
- Any information that indicates that a person possesses certain personal characteristics

Portable Computing Device - Any mobile electronic computer or mechanism that allows a person to move from place to place and use or access information technology services, products and resources. Portable computing devices include air cards, laptops, tablet personal computers, smartphones and other similar handheld mobile electronic instruments or mechanisms.

Portable Computing Media - Any device that is capable of storing data and not necessarily required to be capable of processing data such as CD's, CD-R discs, DVD's, flash memory cards, USB jump drives and diskettes, magnetic tapes, solid state drives, external/removable hard drive, etc.

Privilege User Accounts - Passwords associated with user accounts, which are assigned to individuals (commonly referred to as named accounts), that have elevated access to make changes to system parameters. In DRC, only Authorized Users authorized at a technical level to administer and support/maintain State computing IT systems and telecommunications technology systems are issued Privilege User Accounts.

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

Save Password Option - An option on some IT systems that, when enabled, allows the user to choose to have the user password retained within the system so that it will not have to be reentered by the user upon subsequent access to the IT system.

Sensitive Data - Any type of data that presents a high or medium degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a medium risk and potentially a high risk in cases for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The data may be certain types of PII that is also sensitive, such as medical information, social security numbers and financial account numbers. In addition, the data may be other types of information not associated with a particular individual such as security and infrastructure records, system administrative passwords, trade secrets and business bank account information.

ServiceNow - An on-demand, cloud-based, enterprise IT service management software tool hosted by the Ohio DAS OIT. ServiceNow is used to report IT incidents, problems and issues, request specific ODRC products and services, document the actions taken in response to said reports and requests and track said requests, reports and associated responses in a standardized manner in order to generate data that can be used for ODRC IT resource forecasting and allocation. ServiceNow is commonly referred to by ODRC authorized users as the ODRC IT ticket system.

Social Media - Websites that facilitate user participation, networking and collaboration through the submission of user generated content, such as blogs, wikis, microblogging sites, video sharing sites, bookmarking sites and social networking sites, such as Facebook, WhatsApp, YouTube, Facebook Messenger, WeChat, Instagram and LinkedIn.

Social Networks - Websites promoting a “circle of friends” or “virtual communities,” where participant users are connected based on various social commonalities, such as familial bonds, hobbies or dating interests.

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

System Assets - Computer hardware, telecommunications hardware and systems, digital devices such as digital copiers and facsimile machines, software, networks, the internet, IT information or data and/or IT services or IT resources that are made available by ODRC or DAS OIT to authorized users and are necessary to conduct state government business and support the IT requirements of the ODRC and, therefore, must be protected by the appropriate security requirements to ensure business continuity.

Text Messaging - The process of sending or receiving written text messages or multimedia messages, such as pictures or audio, using a cellular telephone, smartphone or another mobile electronic device. This process is commonly referred to as texting.

Ticket - The term commonly used by authorized ODRC users to describe a report of an IT incident, problem or issue or a request for a specific ODRC IT product or service entered into ServiceNow.

Unified Communications (UC) - An online, IT, enterprise service delivered in a unified user interface, that offers a variety of communication and productivity tools, such as Instant Messaging (IM), voice, audio and desktop sharing. ODRC provides two levels of UC to Authorized Users: Skype for Business, a UC service limited to approved executive level Authorized Users and specialized program Authorized Users and Jabber, an UC service available to other approved Authorized Users.

Wiki - A Web application that allows one user to add content and any other user to edit the content, such as Wikipedia, an online encyclopedia.

V. POLICY

It is the policy of the Ohio Department of Rehabilitation and Correction (ODRC) to establish security requirements to protect all ODRC and DAS OIT IT system assets assigned to authorized users in order to ensure business continuity, pursuant to DAS OIT Policy 700-001, Information Technology Resource Usage.

VI. PROCEDURES

- A. System assets that contain data, text, images or other information created, stored, transmitted, received, displayed or archived using ODRC or DAS OIT resources are the property of ODRC and DAS OIT except for those IT items whose ownership is protected by law, contract, license agreement, copyright or other agreement. System assets are subject to review, investigation and inspection and, depending upon its content, may be subject to public records laws and/or eDiscovery. As a result, authorized users of system assets have no expectation of privacy.

- B. ODRC and DAS OIT can access and monitor the use of all system assets and generate and retain logs, reports and other documentation pertaining to the use of the system assets. ODRC and DAS OIT shall disclose usage logs and other documentation when deemed appropriate for purposes of litigation, audits and investigations. Any suspected misuse of any system assets shall be reported to the ODRC Office of the Chief Inspector who may, in turn, report the suspected misuse to the appropriate law enforcement agency for further investigation and action.
- C. ODRC reserves the right to limit and restrict access to all system assets. In order to protect the security of said system assets, all access requests from ODRC authorized users shall be documented via submission of a System Access Request (DRC3424) and shall be reviewed and approved by one or more management levels as follows:
1. For regular system access, the immediate supervisor of an ODRC authorized user, or appropriate supervisor if a non-ODRC authorized user, shall review and approve the request.
 2. For specialized system access, the immediate supervisor of an ODRC authorized user, or appropriate supervisor if a non-ODRC authorized user, and the managing officer/designee shall review and approve the request.
 3. For highly secure system access, the immediate supervisor of an ODRC authorized user, or appropriate supervisor if a non-ODRC authorized user, and the managing officer/designee shall review and approve the request. In addition, the appropriate Operation Support Center (OSC) administrator representing the data owner shall review and approve the request.
- D. Approved System Access Requests (DRC3424) shall be submitted by the final approving supervisor/manager/administrator to the ODRC Information Service Center at OSC at DRC.InfoServCtr@odrc.state.oh.us via a ticket in ServiceNow, pursuant to ODRC Policy 05-OIT-25, Standardized Procedures to Report DRC IT Incidents, Problems and Issues and Request IT Products and Services. Upon receipt of the ticket and attached, completed System Access Request (DRC3424), ODRC Help Desk staff shall create the appropriate user account.
- E. In order to obtain access to non-ODRC or non-DAS OIT IT systems, networks or data, such as the Law Enforcement Automated Data System (LEADS), the Ohio Courts Network (OCN) or the Ohio Law Enforcement Gateway (OHLEG), authorized users shall follow all access request, policies and procedures of the external agency that owns, manages or hosts the IT systems, networks or data.
- F. The authorized user shall complete the appropriate access form from the external agency and submit the form to the immediate supervisor, if an ODRC authorized user, or appropriate supervisor if a non-ODRC authorized user for review and approval. Upon approving the request, the immediate/appropriate supervisor shall submit the form to the authorized external agency point of contact, pursuant to the external agency's system access request process for creation of the account.

1. Upon obtaining an account, the authorized user is responsible for following all IT systems, networks or data access and usage requirements stipulated by the external agency. Failure to follow these requirements may lead to termination of the account.
 2. Suspected misuse of an external agency's systems, networks or data may be reported by the external agency to the ODRC Office of the Chief Inspector who may, in turn, report the suspected misuse to the appropriate law enforcement agency for further investigation and action.
- G. The system access request/approval process outlined in this policy for regular, specialized, and highly secure ODRC system asset user groups and non-ODRC user groups and the language contained within a System Access Request (DRC3424) shall be revised only with the approval of the ODRC ITGG. When any language contained within a System Access Request (DRC3424) is revised, the BITS chief/designee shall notify all ODRC authorized users of the revision and all ODRC authorized users shall review the revisions upon receipt of the notification.
- H. Authorized users who receive access to any system assets shall follow all ODRC and DAS-OIT security requirements:
1. All system assets, including, but not limited to, all computing devices, the internet, electronic mail and the other tools in Office 365, all on-line services and resources, all telecommunications devices and services, all unified communications services, all digital devices and virtual privacy network (VPN) access shall be used by authorized users for State of Ohio business purposes only.
 2. Authorized users assigned any system asset shall not:
 - a. Allow or permit any inmate/offender to use/access any system asset or view any content displayed on a system asset.
 - b. Use any system assets to violate local, state or federal law or encourage the violation of local, state or federal law.
 - c. Use any system asset to download, duplicate, disseminate, print or otherwise use copyrighted materials (i.e., software, texts, music, graphics or other content) in violation of copyright laws.
 - d. Use any system asset to operate a business, directly or indirectly, for personal gain or attach a signature on any electronic communications that contains information (i.e., name, title and contact information) that is not related to State of Ohio business.
 - e. Use any system asset to access or participate in any type of personals advertisements or services, such as or similar to dating services, matchmaking services, companion finding services, pen pal services, escort services or other personals advertisements.
 - f. Use any system asset to download, display, transmit, duplicate, store or print any material that is sexually explicit, obscene, offensive, threatening or harassing,

including disparaging or derogatory statements about others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs.

- g. Use any system asset to download, display, transmit, duplicate, store or print any communications, including images, that contain incendiary statements which might incite violence or describe or promote the use of weapons or other devices associated with illegal activities.
- h. Use any system asset to download, display, transmit, duplicate, store or print or otherwise organize any data or other materials, including images, used to wager on or participate in any type of gambling event or gambling game of chance or used for recreational purposes (i.e., playing computer games).
- i. Use any system asset to solicit money or support on behalf of any religion or political cause.
- j. Use any system asset to solicit money or support for any ODRC approved effort without the proper authorization.
- k. Use a state business e-mail account for personal communications in internet forums.
- l. Impede the State of Ohio's ability to access, inspect and/or monitor any system assets including, but not limited to, inappropriately encrypting or concealing the contents of files or other electronic communications, inappropriately setting or manipulating system asset accounts or account passwords, physically concealing any device or tampering with, removing or circumventing any security control put in place by ODRC or DAS OIT to protect system assets.
- m. Engage in any IT-related activities or actions that are unauthorized or outside one's job duties that could result in any IT security incident, as defined in ODRC Policy 05-OIT-14, Information Technology Security Incident Response, to include, but not limited to, unauthorized access to any system asset; denial of service (DoS) for any system asset; installation of malicious code on any system asset; improper usage or improper access to any system asset; scans, probes and attempted access of any system asset; information spillage for any system asset; loss or theft of any State of Ohio computing device or media and the compromise, in any way, of any confidential, non-public and personally identifiable information (PII).
- n. Conceal or misrepresent one's name, affiliation, duties, roles, responsibilities or assignments in any electronic communications in order to obtain access to any system asset user account or in order to mask any unauthorized, illegal, fraudulent, irresponsible or offensive behavior.
- o. Access, download, display, transmit, duplicate, store or otherwise disseminate any state sensitive data, confidential data or PII without the proper authorization.

- p. Use a state business e-mail account or any non-state information system account for non-business purposes to access personal information, confidential information or PII about an individual.
- q. Disclose or share any System Asset passwords to/with any other individual, which includes posting or attaching passwords in writing anywhere in the work location, including on computing devices, where they can be viewed by others.
- r. Use another authorized user's system asset account or signature line without proper authorization.
- s. Use a "save password" option on any system asset.
- t. Use the same password for any system asset privilege user accounts and any other system asset user accounts.
- u. Set, manipulate, deactivate or disable any authorized user's system asset password or user account to impede access to the system asset, without proper authorization.
- v. Use any system asset to engage in peer-to-peer (P2P) file sharing with an external, non-business computer system or network.
- w. Use any system asset account to order, download, display, transmit, duplicate or store any non-ODRC or non-DAS OIT authorized software, software service packs, or software updates for use with/on any system asset.
- x. Convey any non-ODRC desktop computing device, portable computing device, other IT hardware or equipment, software or any portable computing media into an ODRC facility or office without proper authorization from the BITS chief/designee or install, attach or connect any non-ODRC desktop computing device, portable computing device, other IT hardware or equipment or any portable computing media to any state business information system or network without proper authorization from the BITS chief/designee.
- y. Use a system asset to send unsolicited e-mail or facsimile communications in bulk or forward electronic chain letters in bulk to recipients inside or outside the State of Ohio business environment.
- z. Use a state Office 365 e-mail "global distribution list" without the proper authorization.
- aa. Download, install and/or use a personal, privately-owned or consumer-grade e-mail or unified communications account on any system assets to conduct State business.
- bb. Physically relocate or replace any non-mobile state computing hardware/equipment assigned to end users (i.e., PCs or network printers) without the approval of the authorized user at a technical level at the ODRC facility/office who is responsible for administering and supporting/maintaining the facility/office's State computing IT

systems and telecommunications technology systems. Requests to relocate or replace non-mobile state computing hardware shall be submitted to the ODRC Information Service Center at OSC at DRC.InfoServCtr@odrc.state.oh.us via a ticket in ServiceNow, pursuant to ODRC Policy 05-OIT-25, Standardized Procedures to Report ODRC IT Incidents, Problems and Issues and Request IT Products and Services. Upon receipt of the ticket, the appropriate authorized user at the technical level at the facility/office will contact the requestor to review the required work and, if approved, schedule the required work to fulfill the request.

cc. Physically relocate or replace or reconfigure any state computing infrastructure hardware/equipment (i.e., servers, switches, routers, etc.) without the approval of the OSC authorized user at the technical level who is responsible for administering and supporting/maintaining computing infrastructure hardware/equipment throughout the ODRC enterprise. Requests to relocate or replace or reconfigure State computing infrastructure hardware/equipment shall be submitted to the ODRC Information Service Center at OSC at DRC.InfoServCtr@odrc.state.oh.us via a ticket in ServiceNow, pursuant to ODRC Policy 05-OIT-25, Standardized Procedures to Report DRC IT Incidents, Problems and Issues and Request IT Products and Services. Upon receipt of the ticket, the appropriate authorized user at the technical level at OSC will contact the requestor to review the required work and, if approved, schedule the required work to fulfill the request.

3. Authorized Users shall adhere to the following social media use requirements:
 - a. Authorized users shall use system assets to access YouTube only for the designated quota time, which they shall acknowledge before accessing YouTube.
 - b. Authorized users with a business-related need to use system assets to access social media sites other than YouTube shall:
 - i. Submit a written e-mail access request to the immediate supervisor, if an ODRC authorized user, or to the appropriate non-ODRC supervisor if a non-ODRC authorized user. The e-mail request shall contain the specific social media site requested and the business justification for accessing the site.
 - ii. If the request is approved, the immediate/appropriate supervisor shall forward the approved request and business justification, via e-mail, to the chief of BITS or designated BITS manager, who shall give the authorized user access to the site.
 - c. ODRC employee, contractor, temporary employee or other agent of the State shall not:
 - i. Design a personal social media site or channel or use a personal social media account to speak on behalf of, speak for, or otherwise represent the State or ODRC without the express authorization of the appropriate ODRC managing director.

- ii. Use a social media account approved for a business-related need and accessed through system assets or a personal social media account to access, download, display, transmit, duplicate, store or otherwise disseminate any State data or information that is not classified as public information.
 - d. Authorized users shall not include pointers or references to any personal social media account in any system asset account (i.e., including a social media account reference or pointer in a State e-mail account signature line).
 - e. Authorized users of system assets shall use only the Cloud File Sharing Solutions approved by ODRC or DAS OIT to store or share State data or synchronize State data between multiple computing devices. Authorized users shall not use approved Cloud File Sharing Solutions to:
 - i. Store or share personal data or information or any other personal content;
 - ii. Store or share PII, sensitive or confidential State data, information or other content without the approval of the appropriate managing director.
4. When any authorized user assigned a desktop or laptop computer leaves the physical proximity of their work area, the authorized user shall secure the computer to prevent unauthorized access to the device or its data/information, using one or more of the following methods:
 - a. Log off all accounts, including the computer and/or network account;
 - b. Lock the computer by using an approved password protected screensaver;
 - c. Lock the computer by using operating system level workstation locking;
 - d. Shut the computer down.
5. When an authorized user has reason to believe any system asset or the password integrity of any system asset has been compromised in any way, the authorized user shall complete an Incident Report (DRC1000) pursuant to ODRC Policy 01-COM-08, Incident Reporting and Notification, and shall ensure a copy of the report is distributed to the chief of BITS.

Related Department Forms:

Incident Report	DRC1000
Systems Access Request Form	DRC3424