

STATE OF OHIO



DEPARTMENT OF REHABILITATION
AND CORRECTION

SUBJECT: DRC Sensitive Data Security Requirements	PAGE <u>1</u> OF <u>9</u>
	NUMBER: 05-OIT-23
RULE/CODE REFERENCE:	SUPERSEDES: 05-OIT-23 dated 02/0714
RELATED ACA STANDARDS:	EFFECTIVE DATE: February 2, 2015
	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 define the process for identifying Ohio Department of Rehabilitation and Correction (DRC) sensitive data and the security requirements for the access, use, storage and release of DRC sensitive data.

III. APPLICABILITY

This policy applies to all DRC employees, contractors, volunteers, interns and other agents of the state.

IV. DEFINITIONS

Alternate Workplace – Generally would be a work site in an employee’s home, but could also be a work center, mobile work site or customer site close to the employee’s home that has been approved by the agency.

Annual DRC Sensitive Data Security Plan – The fiscal year plan completed by the DRC Chief of BITS that identifies the actions that must be taken in the upcoming fiscal year to ensure that DRC sensitive data remains secure pursuant to the standards promulgated by the Ohio Department of Administrative Services, Office of Information Technology (DAS OIT).

Annual DRC Sensitive Data Security Survey – The annual survey (DRC1677) distributed by the DRC Chief of the Bureau of Information Technology Services (BITS) to DRC data owners for the purpose of identifying and reporting the types of sensitive data from their respective areas.

Authorized User - A DRC employee, contractor, intern, volunteer or other agent of the State who is authorized at a high technical level to administer and support / maintain state computing information technology systems and telecommunications technology systems or is authorized at an end user level, to

have access to and use State computing information technology systems and telecommunications technology systems for business purposes on behalf of the State of Ohio.

Data Owners – DRC executive staff members or designees responsible for identifying overall data requirements for their respective areas, identifying and reporting types of sensitive data from their respective areas and authorizing or denying access to the data for their respective areas.

Data Privacy Point of Contact (DPPOC) – The DRC Chief of the Bureau of Information Technology Services (BITS) who is responsible for overseeing data privacy issues for the DRC enterprise.

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 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.

Memorandum of Understanding (MOU) - A document describing a bilateral or multilateral agreement between two or more parties. A MOU executed by all parties is required for non-DRC entities to receive DRC sensitive data in an electronic form.

Non-DRC Entity – An organization external to DRC or one or more individuals representing an organization external to DRC that are not authorized DRC users who request DRC sensitive data.

Record - Any item that is kept by the Department that: (1) is stored on a fixed medium, including and electronic or digital medium (2) is created, received, or sent under the jurisdiction of the Department and (3) documents the organization, functions, policies, decisions, procedures, operations, or other activities of the Department.

Sensitive Data – Records, information or data considered private, confidential or non-public, as prescribed by law, administrative rule or other legally binding authority that are restricted to a limited number of authorized DRC users for specialized business purposes and available only to non-DRC entities pursuant to a formal request, review and approval process, such as a MOU. Personal identification data, including an individual's last name, first name or first initial, in combination with any of the following data elements, shall always constitute sensitive data: social security number, driver's license number, state identification card number, financial account number, credit card number or debit card number. Sensitive data must be protected with a high level of security from unauthorized access, use, storage or release.

V. POLICY

It is the policy of the Ohio Department of Rehabilitation and Correction to identify sensitive data on an annual basis and take the required steps to protect and secure the access, use, storage and release of the data on an ongoing basis pursuant to the requirements promulgated by DAS OIT.

VI. PROCEDURES

- A. A significant amount of DRC sensitive data is contained in the various DRC online database systems, which are organized automated repositories of information storage, retrieval and review

that are part of an overall research and decision-making capacity relating to both offender and operational needs. As a result, all DRC database systems shall be maintained in a current and accurate status and the correct data shall be entered into the various databases by authorized users as soon as practical. Data shall not be knowingly entered into any DRC database system when it is false, inaccurate or misleading. In order to identify DRC sensitive data and the security requirements for the access, use, storage and release of the data a DRC Sensitive Data Security Survey shall be conducted annually and a Sensitive Data Security Plan shall be completed annually.

1. Every year in the last quarter of the fiscal year, the DRC Chief of BITS shall distribute an Annual DRC Sensitive Data Security Survey (DRC1677) and instructions for completing the survey to DRC data owners.
 2. DRC data owners shall complete the survey, identifying the types of sensitive data from their respective areas, and return the survey results within 60 calendar days to the DRC Chief of BITS.
 3. The DRC Chief of BITS shall compile the survey results, share the results with the appropriate DRC technical staff and other appropriate staff and complete an Annual DRC Sensitive Data Security Plan, which will identify the actions that must be taken in the upcoming Fiscal Year to ensure that the access, use, storage and release of DRC sensitive data remains secure. The plan shall include the action steps necessary, pursuant to the requirements promulgated by DAS OIT, to address the initiating or maintaining of enterprise level controls, such as physical security controls; state-approved strong encryption controls; data transmission controls and restrictions; data storage access and backup controls; portable computing device and media controls and restrictions; non-state computing device controls; data access, use and disclosure controls at the user level and user data account management controls. The annual plan shall also include a summary of revisions to the incident response procedures that must be taken when the security of DRC sensitive data is breached or otherwise compromised.
 4. The DRC Chief of BITS shall distribute the Annual DRC Sensitive Data Security Plan to the ITGG and to all DRC data owners.
 5. The DRC Chief of BITS shall task the appropriate BITS technical staff, in consultation with the appropriate DRC data owners, to take the appropriate actions to meet the requirements of the Annual DRC Sensitive Data Security Plan.
 6. The DRC Chief of BITS shall report on the progress of the DRC Sensitive Data Security Plan and any necessary revisions to the plan to the ITGG on a regular basis.
- B. DRC employees, contractors, volunteers, interns and other agents of the State who are not authorized DRC users shall not access, use or store DRC sensitive data on any electronic computing device, nor shall they release DRC sensitive data in any form to any individual or any organization.

- C. Sensitive Data Security Requirements For All Authorized Users Including DRC Data Owners
1. DRC personal identification data shall be accessed, used, stored or released only by authorized DRC employees, contractors, volunteers, interns and other agents of the State and only for official lawful purposes.
 2. DRC sensitive data in paper form shall not be accessed, used, stored or released without the approval of the appropriate DRC data owner:
 - a. Written justification and documentation must be submitted by the appropriate DRC requesting party to the appropriate DRC data owner prior to approval being granted to access, use, store or release DRC sensitive data in paper form.
 - b. Access requests from non-DRC entities for DRC sensitive data in paper form shall be submitted by the non-DRC entity in writing with the necessary justification to the appropriate DRC data owner who shall review and approve or deny the request. If the request is approved, the data owner shall process the request pursuant to all applicable laws and DRC policies. The data owner may require a MOU or other written agreement to release or otherwise facilitate access to the data.
 3. DRC sensitive data in electronic form shall not be accessed, used, stored or released without the approval of the DRC Chief of BITS, in consultation with the appropriate DRC data owner
 - a. Access requests from DRC authorized users for DRC sensitive data in electronic form shall be requested, reviewed and approved or denied pursuant to Department Policy 05-OIT-10, Internet, Electronic Mail and On-Line Services Use.
 - b. Access requests from non-DRC entities for sensitive DRC data in electronic form shall be submitted in writing with the necessary justification to the appropriate DRC data owner who shall review and approve or deny the request. If the request is approved, the data owner shall forward the request to the DRC Chief of BITS who, in turn, shall provide the data requestor with information regarding DRC's data sharing MOU requirements. Non-DRC entities shall not receive approval to access, use, store or release DRC sensitive data in electronic form until a MOU is fully executed.
 4. DRC sensitive data must be stored in server files on secured servers supported and maintained by DAS OIT, DRC BITS, or higher level technical authorized users approved by the DRC Chief of BITS.
 5. DRC sensitive data shall be secured, placed, used, stored and transported on DRC portable computing devices and DRC portable computing media pursuant to the requirements of Department Policy 05-OIT-15, Portable Computing.
 6. DRC sensitive data shall be accessed only through the DRC authorized user's DRC virtual private network (VPN) account when the authorized DRC user is performing job

duties in an alternate workplace approved pursuant to Department Policy 35-PAY-09, Telecommuting Procedure.

7. DRC sensitive data shall not be stored on an authorized user's non-DRC computing device, except for personal smartphones approved for use in conducting state business pursuant to the requirements of Department Policy 05-OIT-16, Using Personal Smartphones to Conduct State Business.
 8. DRC sensitive data shall not be transmitted by an authorized user through any non-DRC email account, web site or web service not approved by the DRC Chief of BITS.
 9. DRC sensitive data shall not be transmitted by an authorized user through an unknown or untrusted channel or to an unknown or untrusted site. Requests for DRC sensitive data that requires transmission of the data through an unknown or untrusted channel or to an unknown or untrusted site shall be reported immediately to the appropriate DRC data owner.
 10. DRC sensitive data shall not be stored by an authorized user on an on-demand, paid service or free service cloud storage Internet site.
 11. DRC employees, contractors, interns, volunteers or other agents of the state shall immediately:
 - a. Report any known or any suspected unauthorized access, use, storage or release of DRC sensitive data in any form or any suspicious attempts to otherwise obtain DRC sensitive data in any form to their immediate DRC supervisor who shall, in turn, document the incident pursuant to Department Policy 01-COM-08, Incident Reporting and Notification.
 - b. Advise the appropriate DRC supervisor upon receiving any DRC sensitive from a non-DRC entity. The DRC supervisor shall, in turn, immediately advise the appropriate DRC data owner, and the data owner shall take the appropriate action, which may include contacting the non-DRC entity to resolve to matter or completing an incident report pursuant to Department Policy 01-COM-08, Incident Reporting and Notification.
 12. An exemption from these procedures may be requested by submitting a written justification to the DRC Chief of the BITS, who serves as the DRC Data Privacy Point of Contact (DPPOC). The DRC Chief of the BITS shall assess the request, approve or disapprove the request and inform the data owner of the decision. Exemptions shall be reviewed annually during completion of the Annual DRC Sensitive Data Security Plan.
- D. Sensitive Data Security Requirements For High Level Technical Authorized Users Including DRC BITS Staff
1. DRC shall use only state-approved strong encryption and a cryptographic key management plan approved by the DRC Chief of BITS that conforms to DAS OIT Standards to secure sensitive DRC data.

2. DRC sensitive data shall be encrypted via state-approved strong encryption, or secured via equivalent compensating controls, when transmitted by an authorized user via:
 - a. Email;
 - b. State-controlled web sites;
 - c. Instant messaging;
 - d. Remote printing;
 - e. Data transfers;
 - f. Wireless transmission.
3. DRC shall secure all physical computing devices and physical computing facilities and locations, such as standalone personal computers, standalone servers, computer training laboratories and computer data centers, in order to restrict physical access to sensitive DRC data.
 - a. Enhanced security approved by the DRC Chief of BITS shall be provided for physical computing devices and physical computing facilities that contain unencrypted DRC sensitive data.
 - b. DRC shall permit only authorized DRC users approved by the DRC Chief of BITS, or vendors approved by the DRC Chief of BITS, to have access to physical computing devices and physical computing facilities and locations that contain or access DRC sensitive data.
4. Pursuant to Department Policy 05-OIT-21, Inventory, Donation, Transfer and Disposal of DRC IT Hardware and Software, DRC computing devices shall be properly sanitized to ensure the removal of DRC sensitive data when the device is transferred or taken out of service and disposed of or donated.
5. DRC protocol for DRC sensitive data backups and DRC sensitive data restorations shall include the following:
 - a. Site-to-site transmission of DRC sensitive data must be secured using state-approved strong encryption.
 - b. State-approved strong encryption must be consistently applied to both backup media and active data containing DRC sensitive data.
6. DRC sensitive data backups and restorations shall be physically stored in a secure state-owned or state-approved site approved by the DRC Chief of BITS and shall be under the control of authorized users approved by the DRC Chief of BITS. When it is necessary to physically transport backup or restoration media containing DRC sensitive data:
 - a. Only authorized users approved by the DRC Chief of BITS shall conduct the transport.

- b. The transport shall be made only in a state-owned or personal motor vehicle that has the appropriate means to secure the backup or restoration media, preferably a motor vehicle that contains a lockable trunk.
 - c. The backup or restoration media shall be secured in the vehicle during the course of the transport, preferably in a locked trunk. If the transport is made in a vehicle that does not contain a locked trunk, the vehicle shall not be left unattended during the course of the transport.
7. Backup and restoration media containing DRC sensitive data may be reused; however, the media shall be properly sanitized prior to reuse pursuant to procedures detailed in Department Policy 05-OIT-21, Inventory, Donation, Transfer and Disposal of DRC IT Hardware and Software.
8. When backup or restoration media containing DRC sensitive data is no longer serviceable or necessary, the media will be sanitized and disposed of pursuant to procedures detailed in Department Policy 05-OIT-21, Inventory, Donation, Transfer and Disposal of DRC IT Hardware and Software.
9. When it is necessary to physically transport one or more DRC servers or personal computer workstations containing DRC sensitive data:
 - a. Only authorized users approved by the DRC Chief of BITS shall conduct the transport.
 - b. The transport shall be made only in a state-owned or personal motor vehicle that has the appropriate means to secure the equipment, preferably a motor vehicle that contains a lockable truck.
 - c. The equipment shall be secured in the vehicle during the course of the transport, preferably in a locked trunk. If the transport is made in a vehicle that does not contain a locked trunk, the vehicle shall not be left unattended during the course of the transport.
10. All DRC information technology systems and telecommunications technology systems, including portable computing devices, and applications that reside on those systems shall contain:
 - a. A session lock for all accounts, including remote access accounts requiring re-authentication after 30 consecutive minutes of inactivity.
 - b. A mandatory logout at the end of a defined allowable period established by the DRC Chief of BITS.

11. Authorized DRC sensitive data user accounts shall be:
 - a. Deactivated when the user is no longer using the account pursuant to the requirements of Department 05-OIT-17, Information Technology Systems Passwords and Account Security.
 - b. Audited and validated by DRC BITS staff pursuant to the protocol promulgated by the DRC Chief of BITS in the Annual DRC Sensitive Data Security Plan.
 12. Only DAS OIT can grant an exception to the encryption requirements mandated by DAS OIT to secure the access, use, storage and release of DRC sensitive data. The exception request must be submitted to DAS OIT by the DRC Chief of BITS and, at a minimum, must include:
 - a. A justification that demonstrates that DRC has performed a risk assessment identifying the potential threats and impact of such threats to the DRC sensitive data.
 - b. The list of alternate security technology and procedures and their respective purchase and implementation costs that will be used by DRC, in lieu of the encryption requirements mandated by DAS OIT, to provide an equivalent level of security for the DRC sensitive data.
 - c. A justification that demonstrates how the purchase and implementation costs for the alternate security technology and procedures outweigh the benefits of the encryption requirements mandated by DAS OIT.
- E. Incident Response Procedures When DRC Sensitive Data is Breached or Compromised
1. The DRC Chief of BITS, in consultation with the DRC Chief Inspector, shall establish the incident response procedures that must be taken when the security of DRC sensitive data is breached or otherwise compromised. At a minimum, the plan shall contain the actions necessary to:
 - a. Report the breach or compromise pursuant to Department Policy 01-COM-08, Incident Reporting and Notification.
 - b. Identify, isolate and mitigate the breach or compromise.
 - c. Notify and respond to the DRC data owners impacted by the incident.
 - d. Notify and respond to the appropriate administrative and law enforcement authorities tasked with investigating the breach or compromise.
 - e. Identify additional controls that must be implemented to ensure that a similar breach or compromise does not occur again.

2. The DRC Chief of BITS, in consultation with the DRC Chief Inspector, shall review the incident response procedures on an annual basis, revise them as necessary and include a summary of the revisions in the Annual DRC Sensitive Data Security Plan.

Related Department Forms

Annual DRC Sensitive Data Security Survey DRC1677