

<p style="text-align: center;">STATE OF VERMONT AGENCY OF HUMAN SERVICES DEPARTMENT OF CORRECTIONS</p>	<p style="text-align: center;">Systems User Security</p>		<p style="text-align: center;">Page 1 of 4</p>						
<p style="text-align: center;">CHAPTER: MANAGEMENT INFORMATION SYSTEMS</p>	<p style="text-align: center;">#257</p>	<p>Supersedes: #254.06, dated 01/02/2016; and #257.01, dated 01/02/2013</p>							
<p>Local Procedure(s) Required: No Applicability: All staff (including contractors, grantees, and others) Security Level: “B” – Anyone may have access to this document.</p>									
<p>Approved:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 33%; border: none;"><u>SIGNED</u></td> <td style="width: 33%; border: none;"><u>10/16/2024</u></td> <td style="width: 33%; border: none;"><u>10/30/2024</u></td> </tr> <tr> <td style="border: none;">Nicholas J. Deml, Commissioner</td> <td style="border: none;">Date Signed</td> <td style="border: none;">Date Effective</td> </tr> </table>				<u>SIGNED</u>	<u>10/16/2024</u>	<u>10/30/2024</u>	Nicholas J. Deml, Commissioner	Date Signed	Date Effective
<u>SIGNED</u>	<u>10/16/2024</u>	<u>10/30/2024</u>							
Nicholas J. Deml, Commissioner	Date Signed	Date Effective							

PURPOSE

This policy establishes limitations of staff, contractors, grantees, and others who are given equipment or access to the Department of Corrections’ (DOC’s) hardware, software, or systems. Such access shall only be used when directly related to the individual’s current job duties or contract deliverables unless otherwise permitted by State personnel rules.

AUTHORITY

3 V.S.A. § 3052(b)(3); 28 V.S.A. § 102(c)(1)

POLICY

The DOC’s policy is to protect the confidentiality, safety, and security of its records and information. It is the DOC’s responsibility to ensure that staff, contractors, grantees, and others do not misuse their access or equipment, which includes use of generative artificial intelligence (AI) and large-language models

(LLMs). LLMs (e.g., ChatGPT, Bard, Copilot, and LLaMA) have demonstrated biases which can negatively impact groups or individuals and do not align with the DOC's vision, mission, and values. If an LLM, or other generative AI, are used for official DOC business, all resultant work product shall be reviewed to ensure it reflects DOC's vision, mission and values and does not negatively impact groups or individuals.

GENERAL PROCEDURES

A. Access to DOC's Hardware, Software, and Systems

1. DOC shall provide staff, contractors, grantees, and others with access to the equipment and databases or systems required by their position in accordance with the policy on hiring and onboarding.
2. If the individual needs additional access or equipment, they shall submit a request to their supervisor or contract manager.
3. If the access or equipment is approved, the supervisor shall:
 - a. Order the equipment; or
 - b. Request the site user access requestor (UAR) submit the request and include their supervisory approval.

B. Use of Hardware, Software, and Systems

1. All written or recorded information produced or acquired by staff, contractors, grantees, and others in the course of DOC business, including emails, is a public record, and may be subject to public inspection and copying.
2. State-issued work devices remain the property of the State.
3. Records and information stored on a work device may become public.
4. Staff, contractors, grantees, and others:
 - a. Shall use State-issued hardware, software, or systems to produce work product that is directly related to their current job duties or contract deliverables;
 - b. Shall not use the internet for use that is not authorized in accordance with the Department of Human Resources personnel policies (e.g., social media, streaming services, online shopping);
 - c. Shall not provide access to, or display information from, computer or mobile applications to individuals under the custody or supervision of the DOC or other unauthorized individuals that is not directly

- related to their current work duties or contract deliverables, or that could create a risk to safety and security; and
- d. Shall not use their access for the personal or financial gain of themselves or other persons.

C. Password Security Protection

1. Staff, contractors, grantees, and others shall ensure:
 - a. They are logged out of their work devices when they are not actively in use;
 - b. Their passwords are not shared with anyone or accessible to others; and
 - c. They only log in under their own credentials when accessing any DOC software or systems.

D. Generative Artificial Intelligence (AI) and Large Language Models (LLMs)

1. Staff shall receive approval from their supervisor before using generative AI or an LLM for official State business. Supervisors may consult with their ADS IT Lead to help them decide whether a use is acceptable.
2. Contractors, grantees, and others shall seek approval from DOC to use generative AI or an LLM for official DOC business.
3. If staff, contractors, grantees, or others are approved to use an LLM, they must use the LLM in accordance with all other applicable State policies and guidance. Staff, contractors, grantees, or others using an LLM for official DOC business shall:
 - a. Create an account using their State email address. Official business shall not be conducted using an account established with a personal email address;
 - b. Not use a State account utilizing generative AI or an LLM for personal use; and
 - c. Not purchase any generative AI or LLM.
4. Staff, contractors, grantees, and others shall not input non-public information into LLMs. All information put into an LLM becomes public. The following is a non-exhaustive list of information that shall not be entered into LLMs:
 - a. Confidential or privileged information or communications;
 - b. All information generated, collected, and maintained by the DOC for individuals under the custody or supervision of the DOC;

- c. Victim/survivor information;
 - d. Personally identifying information (PII);
 - e. Protected health information (PHI);
 - f. Code containing passwords/secrets; or
 - g. Information that has the potential to erode trust in the DOC.
5. Staff, contractors, grantees, and others shall review all content produced with generative AI or an LLM for accuracy, completeness, and alignment with DOC's vision, mission, and values.
 6. Staff, contractors, grantees, and others using LLMs are responsible for their work product, regardless of whether a portion of it is produced by an LLM.

E. Systems Monitoring

1. The DOC monitors user activity by maintaining audit trails in its software and systems.
2. Staff, contractors, grantees, and others who access or provide access in a manner that violates this policy may be subject to disciplinary action or contract termination.