In accordance with the Office of Management and Budget (OMB) M-25-04 Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements[1], and to protect the confidentiality, integrity and availability of the U.S. Office of Personnel Management's (OPM's) USALearning system, rules of behavior on the safe handling of data must be followed when accessing Personally Identifiable Information[2] (PII) in USALearning. The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information.

- I acknowledge that my access to the USALearning system is for official government purposes only in support of authorized training, education, and workforce development.
- I will not use the Learning Management System (LMS) for any personal, commercial, or unauthorized purposes.
- I acknowledge that I am responsible for protecting my login credentials, including my PIV/CAC card.
- I will not share my login credentials or allow others to access the LMS using my account.
- I will log out of my session or lock my device when leaving my computer unattended.
- I acknowledge that I may have access to sensitive or PII and will handle such information in accordance with applicable privacy laws, regulations, and agency policies.
- I will not download, store, or transmit PII or sensitive data outside of authorized and secure environments.
- I will ensure that any downloaded training data is erased/removed from my system within 90 days unless its official use is still required.
- I acknowledge that I will use the system and its content only for official government-related learning and development purposes.
- I will not upload, post, or transmit any malicious or offensive content.
- I will not upload, post, or transmit any copyrighted content without authorization.
- I will comply with all federal copyright, accessibility, and content usage policies.
- I acknowledge that all activity on this system may be monitored, recorded, and audited by authorized personnel.
- I understand that I have no reasonable expectation of privacy while using this government system.
- I acknowledge my responsibility to promptly report any suspected or actual:
    - Unauthorized access or account misuse
    - Security breach or data loss
    - System anomalies or malicious behavior
- I will immediately report incidents in accordance with my Agency specific incident reporting procedures and shall immediately notify the OPM Cyber Integration Center at CyberSolutions@opm.gov.
- I acknowledge that training records, completions, and certifications generated through the LMS are considered official government records.
- I will not falsify, manipulate, or misrepresent training data.
- I understand that any changes in my employment status or changes in my job responsibilities may require my access to be modified or terminated.
- I will notify USALearning@opm.gov if my position, role, or agency affiliation changes, so access can be appropriately updated.

- I acknowledge that when accessing the LMS from remote locations, I will use government approved secure connections and devices.
- I will comply with my agency specific guidance on utilization of public or untrusted networks when accessing the LMS.
- I acknowledge that I must complete required cybersecurity and privacy training before gaining or to maintain access to this system.
- I will review and reaffirm these Rules of Behavior annually or as required by my agency.
- I understand that violation of these Rules of Behavior may result in:
    - Suspension or revocation of LMS access
    - Disciplinary or administrative action by my employing agency
    - Civil or criminal penalties, depending on the severity of the violation

In addition to the responsibilities outlined in this document, I acknowledge that the following longstanding restrictions remain in effect and are enforceable under federal law, regulation, and agency policy. These restrictions are not superseded by any other terms or conditions and are aligned with established security, privacy, and acceptable use requirements.

- 5 U.S.C. § 7211 (governing disclosures to Congress)
- 5 U.S.C. § 2302(b)(8), as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats)
- 50 U.S.C. §§ 421-426 (governing disclosures that could expose confidential Government agents), and
- Executive Order 12356
- Statutes which protect against disclosure that may compromise the national security, including:
    - 18 U.S.C. §§ 641, 793, 794, 798 and 952
    - 50 U.S.C. § 783(b)

References

1 https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/M-25-05-Phase-2-Implementation-of-the-Foundations-for-Evidence-Based-Policymaking-Act-of-2018-Open-Government-Data-Access-and-Management-Guidance.pdf

2 https://csrc.nist.gov/glossary/term/pii

3 https://csrc.nist.gov/glossary/term/sensitive_information

4 https://csrc.nist.gov/glossary/term/encrypt