Mission Area Directive

MRP 3515.2 **08/18/2022**

MRP Cybersecurity Clean Desk Policy

TABLE OF CONTENTS

1. PURPOSE

The purpose of the Clean Desk Policy is to ensure that all Personally Identifiable Information (PII), Controlled Unclassified Information (CUI), sensitive, and/or confidential information is removed from a user's workspace and locked away when not in use, when the user leaves his or her workstation, or disposed of if no longer needed. This policy is intended to reduce the risk of security breaches and the loss of, or damage to information during and outside of normal business hours.

2. SPECIAL INSTRUCTIONS AND REPLACEMENT HIGHLIGHTS

a. This Directive is effective immediately as of the publication date.

b. This Directive is in force until canceled or superseded.

3. AUTHORITIES AND REFERENCES

This Directive must be applied in conjunction with:

a. 44 United States Code (U.S.C) Chapter 35, Subchapter II: Information Security, §3551 (December 2014)

b. The Privacy Act of 1974, 5 U.S.C. 552a

c. Computer Matching and Privacy Protection Act of 1988 , P.L. 100-503 (October 1988)

d. Federal Information Security Modernization Act of 2014 (FISMA), Public Law No: 113-283 (December 2014)

e. National Information Infrastructure Protection Act of 1996, Public Law (P.L.) 104-294

f. Executive Order (E.O.) 13231, Critical Infrastructure Protection in the Information Age, October 2001

g. E.O. 13556, Controlled Unclassified Information, November 2010

h. Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, revised July 15, 2016

i. OMB A-123, Appendix A, Management of Reporting and Data Integrity Risk, to OMB Circular A-123 (revised June 6, 2018)

j. OMB Circular A-130 , Managing Information as a Strategic Resource, revised July 28, 2016

k. Homeland Security Presidential Directive (HSPD)7 Critical Infrastructure Identification, Prioritization and Protection, December 17, 2003

l. National Institute of Standards and Technology (NIST) Special Publications (SP) 800-61 rev. 2: Computer Security Incident Handling Guide, August 2012

m. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010

n. USDA Department Regulation (DR) 3080-001, Records Management, August 16, 2016

o. DR 3140-001, USDA Information Systems Security Policy, May 15, 1996

p. DR 3180-001, Information Technology Standards, January 5, 2021

q. DR 3300-001, Telecommunications & Internet Services and Use, March 18, 2016

r. DR 3300-001-A, Procuring and Managing Telecommunications Devices and Services, August 2020

s. DR 3440-001, USDA Classified National Security Information Program Regulation, June 09, 2016

t. DR 3440-002, Control, and Protection of "Sensitive Security Information", January 30, 2003

u. DR 3440-003, Controlled Unclassified Information (CUI) Program, September 13, 2021

v. DR 3505-005, Cybersecurity Incident Management, November 30, 2018

w. DR 3545-001, Information Security Awareness and Training Policy, October 22, 2013

x. DR 4070-735-001, Employee Responsibilities and Conduct, October 04, 2007

y. DR 4080-811-002 Telework and Remote Work Programs, November 22, 2021

4. DEFINITIONS

a. Access. Ability to make use of the information system (IS) resource.

b. Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for any other than authorized purpose.

c. Confidential. Information about a person or an entity that, if disclosed, could reasonably be expected to place the person or the entity at risk of criminal or civil liability, or to be damaging to financial standing, employment eligibility, reputation, or other interests.

d. Controlled Unclassified Information. Unclassified information that requires safeguarding and dissemination controls pursuant to law, regulation, or Government-wide policy, as listed in the CUI Registry NARA.

e. Data. Information suitable for use in a computer, in a format that allows it to be stored or transmitted.

f. Information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

g. Information Security. The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

h. Information System. A discrete set of information resources organized for the collection processing, maintenance, use, sharing, dissemination, or disposition of information.

i. Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data of information by the executive agency. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

j. Linkable Information. Information about or related to an individual for which there is a possibility of logical association with other information about the individual.

k. Linked Information. Information about or related to an individual that is logically associated with other information about the individual.

l. Network. Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

m. Personally Identifiable Information. Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

n. Portable Storage Device. Portable device that can be connected to an information system, computer, or network to provide data storage. An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video discs, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

o. Records. All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

p. Sensitive Information. Information where the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

q. System of Records. A group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying information assigned to the individual.

5. SCOPE

This policy applies to all MRP employees, contractors, partners, affiliates, and volunteers (including student interns) working on behalf of MRP who handle, control, access documents, records, or information technology (IT) to include any papers, removable storage media, and computing devices that store or transmit PII and/or CUI. This policy applies to both government office and telework/remote settings as well as partner/vendor locations processing MRP data. The parties are responsible for properly handling, processing, and safeguarding PII, in accordance with the Privacy Act and USDA Policy.

6. POLICY

It is MRP policy to safeguard an individual's privacy in a manner consistent with the Privacy Act, E-Government Act, and other federal directives concerning privacy.

a. Employees shall ensure that all PII, CUI and sensitive/confidential information in hardcopy or electronic form is properly secured in a secure unit or location accessible to only authorized personnel. PII, sensitive/confidential information must be removed from the desk and locked in a locked drawer whenever employees are away from their desk and/or the end of the workday. Employees will work with their individual supervisor to identify secure storage needs.

b. Computer workstations and/or laptops screens should be locked when the workspace is unoccupied and/or the end of the day.

c. File cabinets containing PII, CUI, sensitive and/or confidential information shall be kept closed and locked when not in use or when unattended.

d. Keys used for access to PII, CUI, sensitive and/or confidential information shall not be left at an unattended desk. Keys shall be handled by authorized personnel.

e. Passwords will not be written down at any time (e.g., on sticky notes posted on or under a computer) and will only be recorded within an approved password manager (KeePass).

f. Portable media such as thumb drives or compact discs with PII, sensitive and/or confidential information should immediately have that data removed from those devices and moved to the appropriate System of Record or destroyed. Employees must coordinate with Agency Records Officer to ensure proper disposal of portable media files.

g. All printers and fax machines shall be cleared of papers as soon as they are printed, and personnel shall not leave the printing area while printing information that contains PII. This helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up. Any documents no longer needed should be properly disposed of in accordance with Agency Records Management policies. Employees shall consult with Agency Records Officer for guidance.

h. Whiteboards, if used, containing PII, CUI, sensitive, and/or restricted information should be immediately erased.

i. All actual or suspected PII breaches shall be reported to the Information Security Center (ISC) within 1 hour of discovery.

7. ROLES AND RESPONSIBILITIES

The implementation of the policy and procedures as established by this Directive requires the responsibilities of the following individuals and/or groups:

a. Assistant Chief Information Officer (ACIO) will:

(1) Have the overall responsibility and accountability for ensuring the Agency's implementation of information privacy protections, including the Agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.

(2) Communicate changes and/or new policies and procedures to Agency senior managers, as appropriate.

(3) Approve Agency level privacy policies, procedures, standards, and guidelines.

(4) Ensure the availability of sample cascading goals and objectives for inclusion in performance agreements of employees with privacy responsibilities.

b. Chief Privacy Officer (CPO) will:

(1) Develop Agency-level privacy policies, procedures, standards, and guidelines as needed.

(2) Provide overall privacy management and policy guidance.

(3) Provide guidance to the staff on privacy-related matters including the Clean Desk Policy.

(4) Provide assistance to the supervisory staff and/or employees with barriers to compliance with the Clean Desk Policy.

(5) Develop, coordinate and implement privacy related activities and response procedures to be followed in the event of a breach of PII.

(6) Ensure the Agency takes appropriate steps to remedy identified privacy compliance issues.

(7) Coordinate with the USDA Privacy Office to ensure that all policies, procedures, and guidance are consistent with respect to securing PII.

c. Assistant Chief Information Security Officer (ACISO) will:

(1) Investigate possible violations of the Clean Desk Policy and initiates corrective action and/or referring to appropriate official/supervisor for corrective action.

(2) Work with the CPO to develop, coordinate, and implement privacy related activities and response procedures to be followed in the event of a breach of PII.

d. Agency Incident Response Team (IRT) will:

(1) Assist the ACISO in investigating possible information security related violations of the Clean Desk Policy and initiating corrective action and/or referring to appropriate official/supervisor for corrective action.

(2) Work with the ISC on all reported incidents for the Mission Area.

(3) Provide assistance to supervisory staff and/or employees with barriers to compliance with the Clean Desk Policy.

e. Information System Security Program Manager (ISSPM) will:

(1) Ensure proper application and monitoring of the Clean Desk Policy as it relates to information security, PII and sensitive information.

(2) Provide assistance to supervisory staff and/or employees with barriers to compliance with the Clean Desk Policy.

(3) Ensure timely reporting of all actual and/or suspected breaches of PII to ISC.

f. Directors, Managers and Supervisors will:

(1) Assure employees are educated regarding the Clean Desk Policy.

(2) Assist employees with barriers in implementing the Clean Desk Policy.

(3) Monitor areas under their supervision for compliance with the Clean Desk Policy.

(4) Report actual and/or suspected breaches of PII to the ISC within 1 hour of discovery.

(5) Assist employees in identifying the need for secure storage and obtaining identified storage as required to carry out duties related to handling sensitive data.

(6) Ensure employees properly dispose of documents that are no longer required in accordance with Agency Records Management policies and procedures.

g. Employees, Contractors, Partners, Affiliates and Volunteers will:

(1) Protect all PII and CUI utilized in their daily activities, by complying with all Federal laws and USDA policies and procedures.

(2) Ensure compliance with the Clean Desk Policy and/or identifying specific barriers to compliance.

(3) Inform the supervisor, CPO, and/or ISSM as appropriate of barriers to compliance with the Clean Desk Policy.

(4) Ensure the security and privacy of the data utilized in their daily activities; and the data to which the employee has access.

(5) Properly dispose of documents that are no longer required in accordance with Agency Records Management policies and procedures

(6) Report all actual or suspected breaches of PII to the employee's supervisor and ISC within 1 hour of discovery.

(a) To report an incident, contact the ISC at Cyber.Incidents@usda.gov or 1-866-905-6890 within 1 hour of discovery, with the following information

1. Date/Time of the incident
2. Individuals involved in the incident
3. Location of the incident
4. Description of the incident
5. PII Elements (name, address, SSN, etc.)
6. Type of incident

a. A Loss/Stolen/Website/System defacement/exposure
b. Paper Documents, Electronic /Portable Media (Laptop, USB Drives, CDs)

8. RECORDS MANAGEMENT

Federal records created by this Directive must be maintained in accordance with the established General Records Schedule (GRS) and/or the AMS /APHIS records schedules. You can consult with your records liaison for details on disposition of certain records. If employees are named in an active litigation hold, Freedom of Information Act (FOIA) request, and/or other action, those records, regardless of media, must be preserved and maintained in their native format until otherwise notified by your Agency Records Officer and/or the Office of General Counsel.

9. INQUIRIES AND ADDITIONAL INFORMATION

a. General inquiries concerning this Directive may be directed to the Cyber Security Services Directorate via email to sm.mrp.cyber@usda.gov.

b. Records management inquiries should be directed to the Program Records Management Liaison for AMS or APHIS.

c. Additional information and materials can be found on the Cyber Security Awareness Site.

d. Persons with disabilities who require alternative means for communication of this policy (Braille, large print, audiotape, etc.), should contact the United States Department of Agriculture's TARGET Center at (202) 720-2600 (voice and TDD) for assistance.

e. This Directive can be accessed online via the AMS/APHIS Issuance Web page(s).

/s/
Sergio McKenzie
MRP Assistant Chief Information Officer