1002 Secure Employee Workstation and Identification Policy

I. Applicability

This policy applies to all Department of Human Services (DHS) employees, Business Associates, contractors, subcontractors, workforce members, and anyone with access to Personally Identifiable Information (PII) or DHS information systems. These requirements apply to all DHS offices and facilities.

II. Definitions

(A) Business Associate: a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. It includes a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. As defined by HIPAA Definitions (45 C.F.R. §§160.103, 164.103).

(B) Confidential Information: information that must be protected from disclosure by federal or state law, rule, or regulation, including without limitation Protected Health Information (PHI) and Personal Identifying Information (PII).

(C) Computing devices: include, but are not limited to, laptops, notebooks, smart phones, tablets, and computers.

(D) Personally Identifiable Information (PII) information that is protected from disclosure by federal or state law or regulations. This includes, but is not limited to, the following:

a. Protected Health Information (PHI) in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH);
b. Criminal History Report Information (CHRI) in accordance with the Criminal Justice Information Services (CJIS) Security Policy;
c. Social Security Information (SSI) in accordance with the Social Security Act (SSA)
d. Federal Tax Information (FTI) in accordance with IRS Publication 1075;
e. Education Records in accordance with the Family Educational Rights and Privacy Act (FERPA); and
f. Information that identifies a foster child, foster family, adoptee or adoptive family, or benefit recipients as required by applicable state statutes and federal regulations

See DHS Policy 4002 “Privacy and Security Sanctions” for more detailed information on PII.

III. Policy

(A) All DHS employees and contractors are required to protect PII.

(B) DHS employees and contractors are not allowed to let individuals tailgate, sometimes called piggyback, into restricted locations. Tailgating, or piggybacking, is when an unauthorized person follows an authorized person into a secure location. Employees and contractors must take reasonable measures to prevent unauthorized physical access to buildings. The Office of Security and Compliance must be notified of any tailgate/piggyback attempts.

(C) Employees must restrict the visibility of PII by:

(1) Ensuring that workstations are positioned away from public viewing;

(2) Ensuring that visitors are not left unattended;

(3) Ensuring that all PII is erased from whiteboards/chalkboards, and flip charts are covered;

(4) Ensuring that PII is kept in a locked location when not in use;

(5) Ensuring that keys, access cards, and smart cards used to access PII are not left unattended; and

(6) Ensuring passwords are not visible or accessible to anyone.

(D) All DHS employees and contractors are required to lock computer terminals when leaving their workstations, if even for a brief period.

(E) Authorized DHS wireless device users should keep devices under users control and in a secure location when not in use and be passcode locked (also follow DHS Policy 1074 "DHS Wireless Communications Device").

(F) Immediately remove documents containing PII from printers, copiers, and fax machines.

(G) Use only the locked shred bins for documents containing PII when they are no longer needed. Do not use the recycling bins to dispose of documents that contain PII. All documents containing PII must be destroyed in compliance with the "IT Data Destruction and End of Life Procedures" (APM 129).

(H) All PII must be destroyed in compliance with the "IT Data Destruction and End of Life Procedures" (APM 129).

IV. Identification Badges and Proximity Cards

(A) DHS employees must present a valid ID badge to obtain access to DHS offices and facilities and must wear their badge at all times while in a DHS office or facility. Report violations to the Office of Security and Compliance (OSC) and then report it as a physical security incident using the Incident Reporting

System.

(B) All new employees must obtain a badge as soon as possible but no later than one (1) week after the date of hire. It is the supervisor's responsibility to ensure a new employee gets an ID badge.

(C) Employees can only change their profile picture through the DHS Office of Information Technology (OIT). The photographs used for DHS badges also serve as the DHS internet profile photograph used for DHS security. The photograph on the badge is the individual's official DHS photo and should match the profile photograph

(D) ID badges and proximity cards are the property of DHS. Employees are responsible for protecting badges against unauthorized use and must return them in good condition.

(E) Lost or stolen badges or proximity cards must be reported as a physical security incident using the Incident Reporting System as soon as possible after the loss or theft is discovered.

V. Visitors to DHS Facilities

(A) All visitors to DHS facilities must be logged in/out and accompanied by an employee at all times in areas where PII or DHS information systems are present.

(B) Visitors must comply with ID badge requirements pertaining to the specific DHS location being visited. Badges must be clearly visible at all times.

(C) Visitor badges are issued only for a specific event, meeting, or day.

(D) Division Directors, Office Chiefs, or their designees may specify areas where business visitors may work unaccompanied.

VI. Failure to Comply

Failure to comply with this policy can result in restriction or suspension of all network access to DHS Information Systems, deactivation of network attached devices, civil and criminal penalties, and contractual penalties. In addition, DHS employees are subject to disciplinary action outlined in DHS Policy 4002, "Privacy and Security Sanctions" and DHS Policy 1084, "Employee Discipline."