1002 Secure Employee Workstation and Identification Policy

I. Applicability

These rules apply to all Department of Human Services (DHS) employees, contractors, workforce members, and anyone with access to confidential DHS client information or DHS information systems.

II. Definitions

(A) Confidential Information: information that is protected from disclosure by federal law (such as the Health Insurance Portability and Accountability Act [HIPAA], Protected Health Information [PHI], Criminal Justice Information Services [CJIS], Health Information Technology for Economic and Clinical Health [HITECH], Social Security Administration [SSA], and Federal Tax Information [FTI]), state law, regulation, or information that identifies a foster child, foster or adoptive parents, or Medicaid recipients. See DHS Policy 4002 for more detailed information on confidential information.

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

III. Policy

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

(B) Employees must restrict the visibility of confidential information by:

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

(2) Ensuring that visitors are not left unattended;

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

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

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

(6) Not storing passwords near computers.

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

(D) 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).

(E) Immediately remove documents containing confidential information from printers, copiers, and fax machines.

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

(G) All confidential information 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 facilities and must wear their badge at all times while in a DHS facility. Report violations to the Office of Security and Compliance (OSC) and then report it as a security incident using the Incident Reporting System on DHS Share.

(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 at all times.

(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 on the Incident Reporting System (on DHS Share) as soon as possible after the loss or theft is discovered.

V. Visitors to DHS Facilities

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

(B) Visitors must comply with ID badge requirements pertaining to the specific DHS location being visited.

(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."