2016

Department of Social Services

INFORMATION SECURITY POLICY:
PERSONNEL SECURITY

Contents

1. INTRODUCTION 2
1.1 Document Versioning Control 2
1.2 Purpose 2
1.3 Scope 2
1.4 Roles and Responsibilities 2
1.4.1. Management Commitment 3
1.4.2. Coordination among Organizational Entities 3
1.5 Compliance 3
1.6 References 3
1.6.1. External 4
1.6.2. Internal 4
1.7 Maintenance 4
2. INFORMATION SECURITY POLICY 5
2.1 Personnel Security 5
Personnel Security Policy and Procedures [PS-1] 5
Position Risk Designation [PS-2] 6
Personnel Screening [PS-3] 6
Personnel Termination [PS-4] 6
Personnel Transfer [PS-5] 7
Access Agreements [PS-6] 8
Third-Party Personnel Security [PS-7] 9
Personnel Sanctions [PS-8] 10

1. INTRODUCTION

1.1 Document Versioning Control

The history of revisions, modifications, and changes to this document should be documented and reflected in this section.

Last Reviewed:	**Effective Date: 8/22/2016**
Reviewed By: DSS CISO	**Next Review: 08/21/2017**
Date Approved: 8/22/2016	**Authority: DSS CISO**
Approved By: DSS CIO	**Policy Owner:**
Supersedes:	**Policy Number:**

Version	Sections Revised	Description of Revisions	Changed By	Date
1.0	All	Initial Document Creation	Clifford Callender	4/01/16
2.0	All	Revised Document Based on Initial Review Comments from DSS	Clifford Callender	5/25/16
3.0	All	Final Document Based on Final Review Comments from DSS	Clifford Callender	8/19/16

1.2 Purpose

This Personnel Security (PS) policy establishes the requirements to manage the risks related to personnel screening, termination, management and third-party access. This policy, in conjunction with the other information security policies, will be used to construct, implement, and support the information security program across the Department of Social Services (DSS). Section 2 of the Master Governance Policy further defines the purpose of the DSS information security and privacy policies.

1.3 Scope

All DSS employees, contractors, and business partners are responsible for understanding and complying with this policy. This policy applies to all current and future systems and processes handling DSS data. Section 3 of the Master Governance Policy further defines the scope of this policy.

1.4 Roles and Responsibilities

The following roles are responsible for implementing, distributing, enforcing, maintaining, or otherwise supporting this policy.

- D.2, The Agency Risk Management Steering Committee
- D.3, The DSS Chief Information Officer (CIO)
- D.4, The Committee Co-Chair DSS Deputy Commissioner
- D.5, D.8, The Chief Information Security Officer (CISO)
- D.9, The Business Owners and Information Technology (IT) Custodians
- D.10, The System Managers/Application Administrators/Technical Administrators and Managers

While these roles are an integral part of this policy, it is the responsibility of all DSS personnel to promote a strong security posture. For more information regarding the responsibilities, owners, and structure of these roles, please see Section 4 of the Master Governance Policy.

1.4.1. Management Commitment

DSS management is committed to promoting security within the organization through clear direction, demonstrated commitment, explicit assignment, promotion of a strong security culture and awareness, and acknowledgment of information security responsibilities. Section 4.1 of the Master Governance Policy provides more details on the management commitment statement for the DSS information security and privacy policies.

1.4.2. Coordination among Organizational Entities

The following organizational entities have a role in the implementation, distribution, enforcement, maintenance, or support of this policy:

- N.1, The Office of Organizational and Skill Development (OSD)
- N.2, Human Resources
- N.3, Legal Counsel
- N.4, Users
- N.5, DSS Operations
- N.7, DAS-BEST
- N.17, Contracts
- N.22, DAS-BEST Human Resources
- N.23, Guards/Police

While these listed organizational entities are an integral component of this policy, it is the responsibility of all organizations within DSS to support a strong security posture. Section 4.2 of the Master Governance Policy defines the coordination among organizational entities for this policy.

1.5 Compliance

Violations of this policy may lead to revocation of system privileges and/or disciplinary action up to and including termination. Section 6 of the Master Governance Policy further defines the compliance requirements of this policy.

1.6 References

The sections below list the internal and external artifacts that are referenced by this policy.

1.6.1. External

- Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E v. 2.0) – System Security Plan (SSP)
- Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules
- Internal Revenue Service (IRS) Publication 1075 (IRS p1075) (October 2014) – Safeguard Security Report (SSR)
- The United States Social Security Administration (SSA) Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information (SSA EIE) – Security Design Plan (SDP)
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4

1.6.2. Internal

This policy references the following internal policies, procedures, standards, guidelines and methodologies:

- DSS PS Procedures
- DSS Governance Policy
- Legacy: DSS Risk Management Framework Security Planning Approval Process
- Legacy: State of Connecticut Acceptable Use Policy
- Legacy: State of Connecticut HIPAA Security Policy

1.7 Maintenance

This policy and its supporting procedures, standards, and guidelines, will be reviewed annually and updated as needed. A record of the updates can be found in Section 1.1, Document Versioning Control of this policy. Section 8 of the Master Governance Policy further defines the maintenance requirements of this policy.

2. INFORMATION SECURITY POLICY

2.1 Personnel Security

DSS has chosen to adopt the moderate-impact baseline controls established in the NIST SP 800-53 Rev.4 Personnel Security (PS) control family as the framework of this policy. The following subsections outline personnel security control requirements that constitute the DSS PS policy.

Policy	Personnel Security Policy and Procedures [PS-1]
	• [PS-1]: DSS shall develop, document, and disseminate to applicable personnel:
	  o A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
	  o Procedures to facilitate the implementation of the personnel security policy and associated system and services acquisition controls.
	• [PS-1]: DSS shall review and update the current:
	  o Personnel security policy within every 365 days;
	  o Personnel security procedures within every 365 days.
	• [HIPAA – §164.308(a)(3)(ii)(A)]: DSS shall implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
	• Legacy: A Personnel Security process defining position categorization, personnel screening, personnel termination, personnel transfer, access agreements, third-party personnel security and personnel sanctions methodologies, guidelines and procedures will be established, approved, monitored and maintained across the Agency.
	• Legacy: The personnel security baselines will be continuously reviewed and evaluated. Baselines will be updated as required to ensure that IRS, HIPAA and SSA compliant control capabilities will be maintained. Supporting methodologies and procedures will provide specific guidelines and instructions to ensure the effective implementation of required security controls and control enhancements in the NIST SP 800-53 personnel security control family. Methodologies, processes and procedures in support of required NIST 800-53 personnel security control element definitions will be developed, documented, approved and disseminated in accordance with the DSS Risk Management Framework Security Planning Approval Process for all information systems storing, accessing, processing or transmitting State of Connecticut or Federal Government data. Roles, responsibilities and coordination among DSS entities will

	be established in accordance with approved definitions documented within the DSS Risk Management Framework Security Planning Approval process. Processes, methodologies and procedures will include specific references and mappings to required NIST 800-53 control elements required to meet regulatory compliance. Position Risk Designation [PS-2] • [PS-2]: DSS shall assign a criticality/sensitivity risk designation to organizational positions. • [PS-2]: DSS shall establish screening criteria for individuals filling those positions. • [PS-2]: DSS shall review and update position criticality/sensitivity risk designations within every 365 days. • Legacy: Managed by the Department of Administrative Services Personnel Screening [PS-3] • [PS-3]: DSS shall screen individuals prior to authorizing access to the information system. • [PS-3]: DSS shall rescreen individuals periodically, consistent with the criticality/sensitivity risk designation of the position. • [PS-3]: DSS shall require that when an employee moves from one position to another, their role based access will be reviewed and adjusted as necessary. • [MARS-E - §PS-3]: DSS shall perform a criminal history check prior to employment. • [MARS-E - §PS-3]: DSS shall require that employees and contractors requiring access to Affordable Care Act (ACA)-sensitive information meet personnel suitability standards. These suitability standards are based on a valid need-to-know, which cannot be assumed from position or title, and favorable results from a background check. The background check for prospective and existing employees (if not previously completed) should include, at a minimum, contacting references provided by the employee as well as the local law enforcement agency or agencies. • [HIPAA – §164.308(a)(3)(ii)(B)]: DSS shall implement procedures to determine that the access of a workforce member to electronic Protected Health Information is appropriate. • Legacy: Managed by the Department of Administrative Services Personnel Termination [PS-4] • [PS-4]: DSS, upon termination of individual employment, shall: o Disable information system and physical access prior to or during the employee termination process; o Terminate or revoke authenticators and credentials associated with the individual; o Conduct exit interviews that include a discussion of non-

	disclosure of information security and privacy information; o Retrieve security-related DSS information system-related property; o Regain and retain access to DSS information and information systems formerly controlled by the terminated individual; o Notify defined personnel or roles (defined in the applicable SSP) within one (1) business day; o Promptly escort employees terminated for cause out of the organization. • [MARS-E - §PS-4]: DSS shall revoke system and physical access prior to or during the employee termination process. • [MARS-E - §PS-4]: DSS shall suspend access and privileges to systems, networks, and facilities when employees or contractors temporarily separate from the organization (e.g., leave of absence). • [HIPAA – §164.308(a)(3)(ii)(C)]: DSS shall implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in HIPAA §164.308(a)(3)(ii)(B). • Legacy: DSS Information System Owners will ensure that upon termination of individual employment the agency will terminate information system access, conducts exit interviews, retrieve all organizational information system-related property, and provide appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems. Personnel Transfer [PS-5] • [PS-5]: DSS shall review and confirm ongoing operational needs for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the agency. • [PS-5]: DSS shall initiate the following transfer or reassignment actions during the transfer process: o Re-issuing appropriate information system-related property (e.g., keys, identification cards, and building passes); o Notification to security management; o Closing obsolete accounts and establishing new accounts; o When an employee moves to a new position of trust, logical and physical access controls shall be re-evaluated as soon as possible but not to exceed thirty

	(30) days. • [PS-5]: DSS shall modify access authorization as needed to correspond with changes in operational needs due to reassignment or transfer. • [PS-5]: DSS shall notify defined personnel or roles (defined in the applicable SSP) within one (1) business day. • Legacy: As part of the DSS Role Based Access Control system the agency will review information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiate appropriate actions. Access Agreements [PS-6] • [PS-6]: DSS shall develop and document access agreements for agency information systems consistent with the provisions of applicable laws and regulations, defined in Section 1.6.1 of this policy. • [PS-6]: DSS shall review and update the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every three hundred sixty-five (365) days, whichever occurs first. • [PS-6]: DSS shall require that individuals requiring access to agency information and information systems: o Acknowledge and sign appropriate access agreements prior to being granted access; o Re-acknowledge and sign access agreements to maintain access to agency information systems annually or when access agreements have been updated. • [HIPAA – §164.314(a)]: DSS shall require its business associate contracts or other arrangements to provide that the business associate will: o Require that subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the DSS information security policies by entering into a contract or other arrangement that complies with this policy; o Report security incidents to the covered entity, including breaches of unsecured protected health information; o Enforce the same requirements (listed in the sub-bullets above) on the contracts or other arrangements between the business associate and a subcontractor. • [SSA EIE – §5.11]: DSS shall require that contractors and agents who will process, handle, or transmit information provided to DSS by SSA will include language in their signed agreement that obligates the contractor to follow the terms of the agency's data exchange agreement with SSA.

	• Legacy: Managed by the Department of Administrative services through the State of Connecticut Acceptable Use policy Third-Party Personnel Security [PS-7] • [PS-7]: DSS shall establish personnel security requirements including security roles and responsibilities for third-party providers. • [PS-7]: DSS shall require third-party providers to comply with personnel security policies and procedures established by the organization. • [PS-7]: DSS shall document personnel security requirements. • [PS-7]: DSS shall require third-party providers to notify contracting officers or contracting officer's representatives (via the roster of contractor personnel) of personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days. • [PS-7]: DSS shall monitor third-party provider compliance. • [MARS-E - §PS-7]: DSS shall regulate the access provided to contractors and define security requirements for contractors. The contractors shall be provided with minimal system and physical access, and shall agree to and promote the information security requirements. • [MARS-E - §PS-7]: DSS shall assess the contractor's ability to adhere to and promote information security policies and standards as a part of the contractor selection process. • [SSA EIE – §5.11]: DSS shall provide proof of the contractual agreement with all contractors and agents who encounter SSA-provided information as part of its duties. • [HIPAA – §164.308(b)(1)]: DSS shall permit a business associate to create, receive, maintain, or transmit electronic protected health information on its behalf only if DSS obtains sufficient assurances that the business associate will appropriately safeguard the information. DSS is not required to obtain such sufficient assurances from a business associate that is a subcontractor. • [HIPAA – §164.308(b)(2)]: DSS shall require that its business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains sufficient assurances, that the subcontractor will appropriately safeguard the information. • [HIPAA – §164.308(b)(3)]: DSS shall document the sufficient assurances required through a written contract or other arrangement with the business associate. • Legacy: Through HIPAA Business Associate Agreements (see State of Connecticut HIPAA Security Policy), Memorandums of

	Understanding with other governmental agencies and appropriate contractual clauses for suppliers and contractors the agency will establish personnel security requirements including security roles and responsibilities for third-party providers and monitor provider compliance. Personnel Sanctions [PS-8] • [PS-8]: DSS shall employ a formal sanctions process for individuals failing to comply with established information security policies and procedures. • [PS-8]: DSS shall notify defined personnel or roles (defined by DSS Human Resources) within defined time period (defined by DSS Human Resources) when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. • [HIPAA – §164.308(a)(1)(ii)(C)]: DSS shall apply appropriate sanctions against workforce members who fail to comply with DSS' security policies and procedures or their business associates. • [SSA EIE – §5.10]: DSS shall certify that each employee, contractor, and agent who views SSA-provided information has certified that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure. • Legacy: Included in State of Connecticut HIPAA Security Policies