Decentralized Security Representative (DSR) Standard

Introduction

Office of Management and Enterprise Services Information Services (OMES IS) utilizes a system of decentralized security representatives (DSR) at each agency, which serves as the agency's approval authority for access to the agency's data and network resources.

Purpose

This document outlines the role of the DSR for the State of Oklahoma.

Definitions

Decentralized security representative (DSR) – an individual designated by a state agency to approve user access; communicate security policies, procedures, guidelines and best practices to agency personnel and report on all deviations to security policies, procedures, guidelines and best practices.

DSR appointing authority – the agency DSRs that have been given the approval to appoint additional DSRs.

Emergency – any event resulting in owning agency loss of services.

Hosting state agency – an agency that has physical and operational control of the hardware, software, communications or databases (files) of the owning agency. The hosting agency can also be an owner.

Information – any data or knowledge collected, processed, stored, managed, transferred or disseminated by any method.

Owner – the state agency responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.

Sensitive data – Oklahoma statute (74 O.S. 3113.1) defines sensitive data to include "personal information", consisting of the first name, or first initial, and last name of an individual in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: a) social security number; b) driver license number; or c) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the financial account of an individual. This statute also specifies that if such information is reasonably believed to have been acquired by an unauthorized person, then disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement (Information Security Policy, Appendix E).

Standard
All information content hosted by a state agency is owned by and is the primary responsibility of the agency responsible for collecting and maintaining the authenticity, integrity and accuracy of information. The objective of the owning state agency is to protect the information from inadvertent or intentional damage as well as unauthorized disclosure or use according to the classification standards and procedural guidelines of the owning state agency. The state agency director whose agency collects and maintains (owns) the information is responsible for interpreting all confidentiality restrictions imposed by laws and statutes as well as establishing information classification and approving information access. The owning agency shall validate user access on an annual basis. Thus, all agencies must designate a security representative whose role shall include granting, on behalf of their agency, user access to system functions and data (Information Security Policy, sections 2.2-2.4).

The commissioner, executive director and employees of the human resources department of the owning state agency are automatically considered a DSR for their agency. Additional employees of the owning state agency may be appointed as DSR by the commissioner or executive director to act on their behalf for their agency. They may also delegate the authority to appoint additional DSRs to specific employees of their agency at their discretion.

DSR appointment occurs by the commissioner, executive director or DSR appointing authority completing the DSR appointment request form via the ticketing system. Such requests are processed by the hosting agency, OMES. OMES maintains the list of appointed DSRs and makes available to owning agencies via the DSR SharePoint site.

Prior to DSR appointment, the appointee must complete the required Decentralized Security Representative 101 training via Workday Learning. Upon DSR appointment, the hosting agency confirms setup to the Agency Appointment Authority (Information Security Policy, section 2.3). DSR renewal training shall be completed by all individuals with DSR authority on an annual basis.

OMES can approve IS staff access to support agencies with the exception of agencies who have sensitive, protected or confidential data which will require approval from that agency DSR. In emergency situations, OMES IS can approve access to return services to an agency. Approval for contractor accounts for IS services is through legal review as agencies authorize support for access in this agreement. Approval for contractor accounts for an agency is approved by the agency DSR.

Compliance
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale
To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- DSR appointment instructions.
- DSR SharePoint site.
- Information Security Policy.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 12/21/2023	**Review cycle:** Annual
Last revised: 03/26/2024	**Last reviewed:** 07/15/2024
Approved by: Joe McIntosh, Chief Information Officer	