8-211. System security plan.

The state and agency system security plan (SSP) provides an overview of the security requirements of the information system including all in-house or commercially developed and maintained systems and installations and to all external business partner systems and installations operated by, or on behalf of the state. The SSP describes the controls in place or planned for meeting those requirements and delineates responsibilities and expected behavior of all individuals who access the system. The SSP will address all control areas identified in the NIST SP 800-53 control framework, and will describe the current controls in place to protect information at a level commensurate with the sensitivity level of the system.

The state information security officer will work with each agency information security officer to maintain an SSP incorporating each identified system managing information or used to process agency business.

The agency information security officer and the state information security officer are required to develop or update the SSP in response to each of the following events: new system; major system modification; increase in security risks/exposure; increase of overall system security level; serious security violation(s); or every three years (minimum) for an operational system.

Contents of the system security plan:

(1) System name and title, description and scope of system including each all in-house or commercially developed system and installations included in the SSP;

(2) Responsible organization: Name and contact information for business area responsible for the systems defined in the SSP. Decision authority for business functionality and business risks;

(3) Key contacts: Name and contact information for personnel who can address system characteristics and operation. IT maintenance personnel for the system, applications, and infrastructure;

(4) System operation status and description of the business process, including a description of the function and purpose of the systems included in the SSP;

(5) System information and inventory, including a description or diagram of system inputs, processing, and outputs. Describe information flow and how information is handled. Include the information classification for all information processed, accessed, or exposed. Include a system network and workflow diagram;

(6) A detailed diagram showing the flow of sensitive information, including CONFIDENTIAL and RESTRICED information. Describe details where this data is stored, accessed, or processed and include details of the security mechanisms applicable to this type of data;

(7) Detailed information security descriptions, procedures, protocols, and implemented controls for all NIST SP 800-53 control areas within the scope of the system. Identify compensating controls or compliance gaps within this section of the SSP;

(8) System interconnection or information sharing: Describe all interfacing or connections between two or more systems or business partners;

(9) Applicable laws, regulations, or compliance requirements: List any laws, regulations, or specific standards, guidelines that specify requirements for the confidentiality, integrity, or availability of information in the system;

(10) Review of security controls and assessment results that have been conducted within the past three years; and

(11) Information security risk assessment which includes identification of potential threat/vulnerabilities in the information system, analysis of planned or actual security controls, and potential impacts on operations, assets, or individuals.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-211.pdf