8-210. Information security strategic plan.

Proper risk-based planning is critical to ensure the most appropriate projects are prioritized and funded by the state and its agencies. Information security planning is no exception. Planning for information protection should be given the same level of executive scrutiny at the state as planning for information technology changes. This plan must be updated and published on an annual basis, and should include a 5-year projection of key security business drivers, planned security infrastructure implementation, and forecasted costs. It should include an educated view of emerging threats and protections, and an analysis of the potential impacts to state information assets. This plan is necessary to ensure that information security is viewed as a strategic priority, and is included as part of the overall planning process.

Contents of the information security strategic plan:

(1) Summary of the information security, mission, scope, and guiding principles;

(2) Analysis of the current and planned technology and infrastructure design, and the corresponding changes required for information security to stay aligned with these plans;

(3) Summary of the overall information risks assessments and current risk levels. Detailed descriptions of significant security risks, and plans to mitigate or remediate those risks;

(4) Assessment of the current information security posture related to the future targeted posture, identified gaps, and high-level timeline necessary to close or mitigate those gaps;

(5) Summary of the policies, standards, and procedures for information security, and projected changes necessary to stay current and relevant;

(6) Summary of the information security education and awareness program, progress, and timeline of events;

(7) Summary of disaster recovery and business continuity activity and plans;

(8) Analysis of the regulatory and contractual compliance environment, including potential new regulations or pending contractual requirements that will affect information security;

(9) Proposed five-year timeline of events and key deliverables or milestones; and

(10) Line item cost projections for all information security activity that is itemized by:

(a) Steady state investments: The costs for current care and maintenance of the information security program;

(b) Risk management and mitigation: The line item expenses necessary to mitigate or resolve security risks for the agency in a prioritized order;

(c) Future technology: The line item forecasted expenses and timelines necessary to support emerging or changing technology, and to be ready for new and emerging threats; and

(d) Regulatory: The line item expense necessary to meet all regulatory and contractual compliance requirements.

--

History: Adopted on July 12, 2017.
URL: http://nitc.nebraska.gov/standards/8-210.pdf