Full Enablement Package

Election Information Security Policy

The Election Information Security Policy (EISP) defines the security policies required to protect technology, data, and operations from the cyberattacks threatening elections. The Policy incorporates the Security Best Practices developed by the Texas Secretary of State (SOS) in compliance with HB1421 (2019) legislation adopted to protect elections from cyber threats. It is also aligned to the five core objectives outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). This document is the foundation of the Information Security Program for the County/Elections Department. It designates the governance, standards, and requirements that the other policy documents are built to address.

Continuity of Operations Plan

The purpose of the Continuity of Operations Plan (COOP) is to define a step-by-step process for keeping election functions operational during disruptions such as those caused by cyberattacks or other disaster events. The critical nature of elections makes it imperative that the Election Authority maintains a current version of this plan and that the plan is reviewed and updated on a regular basis. As a crucial element of the Information Security Program, the COOP directs staff on how to ensure an election can be held without delay or disruption even under negative circumstances.

Incident Response Plan

The incident response plan provides clear instructions for handling a cyberattack so employees, community leaders and other stakeholders can block threat activity, minimize the damage and begin the recovery process as quickly as possible. This is the blueprint or outline of steps to be followed when responding to a security incident. Can think of it as a set of guidelines and processes to follow so threats can be identified, eliminated and recovered from.

- The importance of having an Incident response plan is hard to overstate in the current climate. These days it is not a matter of “if” an organization or County will be attacked, but “when” will it happen. Having plans such as the Incident Response Plan in place will ensure rapid response and recovery of critical business operations when an incident occurs. The existing County Emergency Plan, though robust in it’s scope, does not adequately focus on the business of the election and the unique requirements needed to respond to an incident related to this area of critical infrastructure. The Incident Response Plan coupled with the Continuity of Operations plan will both help to not only respond and recover from an incident but enable critical business, such as an ongoing election, can continue while response and recovery occurs.

Election System Security Plan

The Election System Security Plan provides an overview of the functions, components, and cybersecurity requirements for the information systems used to manage elections and enable voting. The plan documents a structured process for planning adequate and required security protections and risk management for core and supporting systems for elections.

Vendor Risk Management Policy

The critical role that technology plays in election operations drives the need to protect the confidentiality, privacy, integrity, and availability of information and communications systems from cyberattack or other disruptive events. By evaluating the key cybersecurity practices implemented by third-party vendors, the County can ensure that security is at the foundation of all operations. The Vendor Risk Management Policy is presented in the form of an assessment survey to provide a way to evaluate vendor cybersecurity practices and technologies. This helps to ensure that risks associated with outsourcing services and utilizing technology provided by third-party suppliers are understood and reduced where possible.