NIST
Election Security Series

Data Integrity and Recovery

OVERVIEW

Ransomware and other destructive attacks can paralyze an election office, disrupting the vital data records and systems relied upon to conduct elections. To ensure the integrity and availability of our election systems, it is essential to protect data assets and restore compromised data quickly after an event. This guide provides an overview of how to identify, protect against, and recover from potentially destructive events to maintain operations and integrity of data critical to the election infrastructure.

WHAT IS DATA INTEGRITY AND RECOVERY?

Data integrity and recovery refers to the capabilities, processes, and procedures used to defend against unauthorized data corruption, modification, and destruction. It includes:

- Identifying critical data assets and any vulnerabilities that may facilitate attacks
- Protecting these assets using access control, secure storage, and vulnerability management
- Detecting and recovering from attacks using integrity monitoring, backups, contingency planning, and incident response

HOW TO IMPLEMENT DATA INTEGRITY AND RECOVERY

Inventory critical assets – Identify devices, data, and applications that may become targets of attack. Prioritize these assets based on their criticality to election activities.

Safeguard critical data—Limit access to critical assets using multi-factor authentication. Keep critical data in secure storage. Identify and remediate system vulnerabilities.

Monitor and log – Monitor, log, and report access and changes to critical data. Detect and report data corruption. Analyze logs to detect anomalies. Enable file integrity protection for logs and audit data.

Backup data – Create backups on a regular basis. Store backups encrypted and in secure locations. Test the backup and restoration processes periodically.

Contingency planning and incident response – Develop plans for responding to and recovering from data integrity events. Test, validate, and update contingency plans regularly.

HOW DATA INTEGRITY AND RECOVERY SUPPORTS CYBERSECURITY OBJECTIVES

The recommendations in this guide can help address the risks to the integrity of a voting system identified in the **Voluntary Voting System Guidelines 2.0.** The recommendations also help achieve **NIST Cybersecurity Framework** outcomes supporting data integrity.

IMPORTANT RESOURCES

- Voluntary Voting System Guidelines 2.0
- NIST Cybersecurity Framework
- NIST Special Publication (SP) 1800-25, Data Integrity Identifying and Protecting Assets Against Ransomware and Other Destructive Events (NIST Cybersecurity Framework)
- NIST SP 1800-11, Data Integrity Recovering from Ransomware and Other Destructive Events

For more information on this Data Integrity and Recovery guide and to view other guides in this series, visit: vote.nist.gov

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE