Security and Privacy Awareness Training

Purpose

This policy describes the responsibilities of all Judicial Branch members to use Judicial Branch technology and information in a secure manner. A workforce trained in security and privacy awareness results in fewer security and privacy incidents, thereby avoiding damage to Judicial Branch computer systems and unauthorized access to information in the custody of the Judicial Branch. Security and privacy awareness training shall follow NIST 800-53, r4 or later as an information security framework and provisions described in the Judicial Branch's Acceptable Use Policy.

Applicability

This policy applies to all Judicial Branch officials, employees, temporary personnel, volunteers, and contractors. Users of Judicial Branch computer systems must attend security and privacy awareness training to ensure the integrity of computer systems, electronic data, court records, and other electronic information on an annual basis.

Authority

The Chief Justice of the Supreme Court is the establishing authority for this policy with the advice and guidance of the Chief Technology Officer.

Employee Responsibility

All Judicial Branch officials, employees, temporary personnel, volunteers, and contractors shall attend appropriate security and privacy awareness training on an annual basis.

- Current employees have ninety (90) days from the date of notification to complete the required training.
- New employees shall complete the required training within forty-five (45) days from the date of employment.

Curriculum

Security and privacy awareness training shall include content that addresses the importance of:

- information security and privacy throughout the Judicial Branch;
- being familiar with and complying with applicable information security and privacy requirements and obligations;
- basic knowledge regarding procedures involving security and privacy (e.g., incident reporting, phishing, password security, etc.); and
- personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information in the custody of the Judicial Branch.

Security and Privacy Awareness Training, continued

Curriculum Continued	Personnel paid through the Integrated HR-Payroll System will have courses assigned and completion monitored in the Learning Management System (LMS). Contractors, interns, and those not paid through the Integrated HR-Payroll System will have courses assigned by the Judicial Branch hiring authority to whose work unit they are assigned.
Policy Violations	Policy violations, such as failure to complete the required security and privacy training modules, may result in suspension or restriction of access to Judicial Branch computer systems. The NCAOC may conduct periodic reviews to ensure policy compliance. Misuse or abuse of Judicial Branch networks, computer systems, applications, or data may result in disciplinary action up to and including termination.
Reporting Security or Privacy Incidents	Any breach or suspected breach of the security of Judicial Branch networks, computer systems, applications, or data must be immediately reported to the Technology Services Division by contacting the NCAOC Help Desk at (919) 890-2407.
DEFINITIONS	See the NCAOC Security and Privacy Awareness and Training Policy.
NIST 800-53 r5	The National Institute of Standards and Technology (NIST) SP 800-53 provides a list of controls that are the operational, technical, and management standards and guidelines government agencies use to maintain the confidentiality, integrity, and availability of their information systems and information. NIST Special Publication 800-53, revision 4 or later, has been adopted as the security and privacy standard for the Judicial Branch and its information technology resources.