New Mexico Judicial Branch

NEW MEXICO JUDICIAL BRANCH
INFORMATION TECHNOLOGY SECURITY POLICY

Revision: **0.6.2**	Document Owner: **JIFFY**
Last Change Date: **2/1/18**	

Table of Contents

1 Purpose

The purpose of this policy is to establish the constructs for the NMJB information security program. This policy and all supporting program components are designed to manage information security risks to acceptable levels, while supporting the objectives of NMJB.

2 Scope and Applicability

This policy applies to all justice, judges, employees, contractors, consultants, and other workers at NMJB, including all personnel affiliated with third parties. This policy also applies to all NMJB information assets.

3 Definitions

- Access Control – A regulation of access to the NMJB's information assets. It regulates who or what can view or have access to the NMJB's information assets.
- Business Recovery – A result of exposure or loss or damage to the NMJB's ability to conduct day-to-day operations. Analysis of business recovery risk involves categorizing threats according to their short, medium, and long-term impact.
- Change Management – Structured approach for ensuring that changes are thoroughly vetted prior to implementation, and that the lasting benefits of change are achieved.
- Configuration Management – Process to reduce attack surfaces by proactively and routinely hardening system configuration through the authorization, management, and control of system changes.
- Encryption – Method in which to protect the confidentiality, integrity, and availability of information that is stored, transmitted, or processed.
- Enterprise Architecture – Practice for conducting enterprise analysis, design, planning, and implementation, using a holistic approach to successful development and execution of strategy. Enterprise architecture applies architecture principles and practices to guide organizations through the business, information, process, and technology changes necessary to execute their strategies. These practices utilize the various aspects of an enterprise to identify, motivate, and achieve these changes.
- Human Resource Security – Integrating security into Human Resource (HR) processes, from pre-employment, during employment, and through termination, to ensure that policies and procedures are in place to address security issues.
- Information – NMJB data stored electronically or physically that must be protected, based on its sensitivity, from disclosure or release to, or use by unauthorized personnel or third parties. Some examples include; strategic information, business plans, financial information, intellectual property, computer programs, passwords etc.
- Information Asset – Information or a computerized system which stores, transmits, and/or processes Information. Some examples include; endpoints (desktop PCs, laptops, tablets, and smartphones), servers, network infrastructure (routers, switches, etc.), databases,

software, operating systems, storage media (such as hard drives, USB flash drives, and writable CDs), etc. This term may also be used for a collection of such systems performing a common function.

- Information Management – Managing information throughout its lifecycle through various sub-processes, such as data classification, labeling, handling, retention and destruction. A well-planned information management system makes essential data easy to find, retrieve, and protect. This can be of particular importance for risk management, legal discovery, and compliance.
- Information Security – Preservation of the confidentiality, integrity, and availability of data.
- IT Asset Management – Management of information assets throughout their lifecycle phases, including acquisition, tracking, and disposal. This includes a detailed account of what information assets are within the environment, where they exist, and who is using them.
- JIFFY – Judicial Information Systems Council
- Physical IT Security – Protection of hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to the organization.
- IT Security Risk Management – Managing information security risks at a level commensurate with the risk appetite of the Judiciary.
- Secure Systems Development – Managing information security risks within the development environment and throughout the systems development life cycle.
- Security Awareness – The knowledge NMJB employees possess regarding the protection of the physical and information assets of the organization.
- Security Incident Handler — Individual notified immediately of a potential incident. Security Incident Handler will conduct the initial investigation of the incident. The Security Incident Handler may involve other internal groups or individuals in its investigation to ascertain the scope, nature and magnitude of the incident.
- Security Incident Response – Organized approach to responding to and managing the aftermath of a security breach or attack. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.
- Security Management – Ability to effectively manage the NMJB information security requirements using the resources available.
- Security Operations – The administration of tactical security controls used to protect NMJB.
- Software Development Life Cycle (SDLC) – A framework defining tasks performed at each step in the software development process. SDLC is a structure followed by a development team within the software organization. It consists of a detailed plan describing how to develop, maintain and replace specific software.
- Strategic Risk Committee (SRC) – Senior management committee responsible for the governance of certain information security functions, including, but not limited to security incident response and risk management.

4 Policy

The NMJB shall use all practical and appropriate security measures to protect information assets in accordance with the concept of least privilege, separation of duties, regulatory, contractual, best practices, and other NMJB policies. NMJB shall protect the following aspects of information:

- Confidentiality – Unauthorized disclosure throughout its lifecycle
- Integrity – Protection of the accuracy and completeness of information
- Availability – Protection of the accessibility of information when required

4.1 Strategic Risk Committee (SRC)

The purpose of the SRC is to provide oversight of the NMJB information technology risk management function, including the strategies, policies, processes, and systems established by JIFFY to identify, measure, monitor, and manage the major risks facing the Judiciary, which risks include information and cyber security risks.

- The SRC is comprised of:
    - The Chief Information Officer (CIO)
    - A Court Executive Officer (CEO)
    - A district court judge
    - A magistrate court clerk or manager
    - A Second Judicial District Court IT staff member
    - A Bernalillo County Metropolitan Court administration staff member
    - The Judiciary IT Security Officer
    - A non-NMJB JIFFY member
- The SRC will carry out the following responsibilities:
    - Provide ongoing oversight of the overall information technology risk management framework with the goal of incorporating relevant best practices.
    - Ensure that JIFFY understands and takes responsibility for identifying, assessing and managing material information technology risks.
    - Monitor information technology risk management practices, including completion of an annual Judiciary wide information technology risk assessment.
    - Determine which information technology risks are most significant and approve resource allocation for risk monitoring and mitigating activities.
    - Assign risk owners and approve mitigation plans.
    - Periodically review and monitor risk mitigation progress.
    - Serve as an escalation point for security incidents.
    - Receive reports on the results of internally or externally performed information technology risk management reviews and assessments.
    - Report monthly to JIFFY and annually to the Supreme Court.

4.2 Incident Response Team (IRT)

The NMJB shall establish a centralized tactical group of individuals responsible for executing the assessment, containment, eradication, and recovery activities of security incidents, utilizing the Security Incident Response Plan. This team has authority to make decisions related to an information technology security incident and notify appropriate parties. IRT membership shall include the Security Incident Handler and select operational members of the following groups:

- Information Technology
- Information Security
- Physical Security
- Human Resources
- Legal

4.3 Information Security Team

The Information Security Team is authorized to develop and direct the NMJB information security program. The Information Security Team shall use all practical and appropriate security measures to protect information assets in accordance with federal and state laws, regulatory and contractual obligations, and NMJB rules and policies. The Information Security Team will provide reports, metrics, and other information to appropriate stakeholders and review security policy exceptions when appropriate. The Information Security Team is responsible for ensuring appropriate security controls are implemented as required by the Judiciary's business and legal compliance commitments. The Information Security Team shall conduct ongoing reviews of cyber security risks to NMJB's information assets and report findings to senior management.

4.4 Information Technology Risk Management

The NMJB shall develop a formal information technology risk management program to identify and manage organizational informational technology risks, including cyber security risks. All information technology risk analysis activities performed across the organization must align with the information technology risk management program and risk findings must be aligned to risk formats defined in the information technology risk management program.

4.5 Information Security Program

Role	Responsibilities
NMJB Technology Information Users	● Adhere to all NMJB information security policies and standards.
Judiciary Chief Information Officer	Information Technology ● Security Operations ● Change Management ● Asset Management ● Configuration Management ● Access Control Information Security ● Risk Analysis ● Security Awareness (content) ● Security Operations Security Review Application Development ● Secure SDLC Architecture ● Secure Architecture ● Enterprise Architecture
Judicial Entity Human Resources Officer	● Assist with the the information technology security awareness training program, and ensure all employees complete applicable training. ● Oversee the HR security for a Judicial Entity, including background screening, maintaining up-to-date position descriptions, and user termination processes.
Incident Response Team	● Execute and maintain the NMJB information technology security incident response process.
General Counsel or designee	● Establish and maintain the Judiciary's data classification scheme and associated data handling, retention, and disposal requirements. ● Coordinate with the Judicial Entities regarding data handling.
Physical Security Officer	● Manage and coordinate physical security controls to secure NMJB's physical information assets.
Information Technology Risk Management Officer	● Evaluate and improve the effectiveness of information technology risk management and the controls and governance processes around information/cyber security. ● Manage and coordinate enterprise risk by developing standards, and collecting appropriate requirements.

5 Monitoring and Enforcement

The NMJB reserves and may exercise the right, at any time and without prior notice of permission, to intercept, monitor, access, search, retrieve, record, copy, inspect, review, block, delete and/or disclose any material created, stored in, received or sent for the purpose of protecting the system. Violation of this policy may lead to disciplinary or corrective action as appropriate, which for employees could include termination.

Employees shall be held responsible for the security and integrity, to the degree that their job requires, for the use of all computer applications. Fulfillment of these responsibilities shall be mandatory, and violation of security requirements or other provision of this policy may be cause for disciplinary action.

6 Review and Revision

This policy shall be reviewed in its entirety, including all appendices, by the policy owner no less than once every 12 months, or within 60 days after the official release of any update to applicable security standards, regulations, or NMJ policies.

7 Exception Handling

All exception requests will be made in accordance to the Information Technology Exception Request Policy.

8 Authoritative Standards and Guidelines

This policy has been implemented as mandated by and/or in support of the following policies and/or standards:

- ISO 27001:2013
    - A.5.1.1 – Policies for information security
    - A.5.1.2 – Review of the policies for information security
    - A.6.1.1 – Information security roles and responsibilities
    - A.18.2.2 – Compliance and security policies and standard

9 Revision History

Version	Change(s)	Change(s) Made By	Date of Change
0.1.0	Document created		
0.5.0	Updated with all suggestions and changes	Wesley T. Reynolds	12/12/17
0.6.0	Added definition, updated SRC responsibilities, cleaned up formatting	Wesley T. Reynolds	1/29/18
0.6.1	Added seal, updated index, updated revision numbering	Wesley T. Reynolds	1/30/18
0.6.2	Added SRC membership, removed sentence from Monitoring and Enforcement	Wesley T. Reynolds	2/1/18

10 Approval

Name (print) Signature

Title Date