New Mexico Judicial Branch

NEW MEXICO JUDICIAL BRANCH
INFORMATION TECHNOLOGY SECURITY OPERATIONS POLICY

Revision: **0.6.1**	Document Owner: **Strategic Risk Committee**
Last Change Date :**1/30/18**	

Table of Contents

1 Purpose

The purpose of this policy is to establish a formalized and consistent approach to securely administering information assets at NMJB to secure protected and other critical information. Establishing and maintaining secure administration and access reduces risk by protecting the confidentiality, integrity, and availability of NMJB's information assets.

2 Scope and Applicability

This policy applies to all justices, 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

- Accountable – The individual that must ensure those that are responsible complete their tasks.
- Checksums – A small-sized datum derived from a block of digital data for the purpose of detecting errors which may have been introduced during its transmission or storage.
- Data Encryption – The process of encoding information in such a way that only authorized parties can access.
- Demilitarized zone (DMZ) – A DMZ (sometimes referred to as a perimeter network) is a physical or logical sub-network that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet.
- Domain Name System (DNS) – DNS is a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network.
- Firewall – A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.
- Gateway Routing Tables – A data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes.
- Information – Company 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.
- 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 Security – Preservation of the confidentiality, integrity, and availability of information.
- Intrusion Detection System – IDS is software, appliance, or systems configured to detect inappropriate, incorrect, or anomalous activity either on a specific host or network.
- Intrusion Prevention System – IPS is software, appliance, or systems configured to actively drop data packets or disconnect from connections that contain unauthorized or anomalous data.

- JIFFY – Judicial Information Systems Council
- Key Management Personnel – Those individuals responsible to provide accountability for the secure administration of information assets as designated by JIFFY
- Malware Appliance – A network appliance containing anti-malware software that is often placed at the perimeter. This may work in conjunction or separately from other anti-malware controls at the endpoints.
- Network Packet and Flow Monitoring – The collection of network traffic statistics as it enters or exits an interface.
- Network Segmentation – The splitting of a computer network into subnetworks, each being a network segment, for increasing performance and improving security.
- Origin Authentication – A means to ensure that a network message has not been modified while in transit, and allows the recipient to verify the source of the message.
- Privileged Access – The right to access and/or modify some or all administrative aspects of an Information Asset.
- Responsible – The individual assigned tasks based on their roles for which they must perform.
- Router Packet Filtering – The process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols.
- Secure Network Segment – The separation or isolation of a network segment, typically using one or more firewalls, to isolate from other internal networks and/or the internet to provide enhanced security and additional protection.
- Security Infrastructure Appliances – Hardware or software used to provide IT security services such as firewalls, IDS, IPS, etc.
- 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.
- Stateful – Tracks the operating state and characteristics of connections.
- VLAN – A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution.

4 Roles and Responsibilities

Role	Responsibilities
Information Security Team	● Review privileged access to all critical information assets ● Review the implementation of security infrastructure appliances ● Advise in the development and implementation of processes and procedures to ensure systems and applications are administered in a secure manner
Strategic Risk Committee	● Accountable for securing the organization's information assets
Key Management Personnel	● Provide accountability for the secure administration of information assets
Technical Custodian	● Establish administrative and device management standards for all information assets, including management access, configuration maintenance, documentation requirements, and other administrative controls

	● Document all access and configuration changes of security appliances and applications ● Possess necessary skills through experience and training in the handling of information assets

5 Policy

5.1 Boundary Defense

Information Technology approved and managed stateful firewalls shall be positioned at all connections between the corporate networks, demilitarized zones (DMZs) and untrusted networks. Traffic from untrusted networks shall be controlled, monitored, and logged to only traffic necessary for business functions to operate. Detected or known malicious IP addresses or network traffic will be blocked by NMJB's firewalls. All security rules within the boundary shall be reviewed at least quarterly.

NMJB shall maintain intrusion detection and intrusion prevention sensors between the corporate network and the Internet. These sensors will be used to block harmful traffic and provide alerting capabilities from NMJB's Internet boundaries. In addition, the NMJB will also utilize network packet and flow monitoring at all network boundaries in order to identify potentially harmful traffic and assist with the incident management process.

All emails entering and leaving the NMJB network will be scanned for malicious code. When malicious code is detected, the email gateway will automatically delete or quarantine the email. Unauthorized email attachments will be blocked at the organization's email gateway.

Other security techniques should be selectively applied to communications over the Internet including data encryption, origin authentication, checksums, gateway routing tables and router packet filtering.

5.2 Network Security

The NMJB shall maintain a list of approved network ports, protocols, and services accompanied by business need and associated business owners. Additionally, network devices will be configured with rules that deny ports, protocols, and services that are not explicitly allowed as defined in the approved list of network ports, protocols, and services. When an Information Owner determines that a business application and its associated network ports, protocols, and services are no longer required, the application and all associated ports, protocols and services will be decommissioned. This list of ports, protocols, and services will be reviewed at least semi-annually.

All administrative activities performed on network devices will be performed from dedicated administrative sessions located on a management network that is completely separate from the organization's primary business network. This will either be enforced via a separate cable plant or dedicated VLANs with access control lists on network devices. All network engineering and administrative tasks shall be conducted from a secured system.

The NMJB shall conduct periodic scans of the corporate network and its required subnets and any other networks associated with the DMZ(s) to discover all unauthorized networks including personal routers, dual-homed computers, modems, dial-up networks, unauthorized VPN connections as well as back channel connections. Information Technology will be alerted to the presence of unauthorized networks and will remediate and report in accordance with NMJB's Security Monitoring and Event Management Policy.

5.3 Wireless Security

NMJB may implement wireless networks for its users, external parties, and guests. Guest wireless networks shall be segmented from internal NMJB networks. A separate guest wireless network shall be maintained for NMJB visitors. Devices not under the control and management of the organization's management systems shall only be authorized to utilize the guest network. The NMJB information assets must not connect to these untrusted guest networks.

All wireless devices connected to an NMJB internal wireless network must be configured securely in accordance with this document and NMJB's Configuration Management Policy and Standards. All wireless devices that connect to a generally accessible NMJB wireless network must:

- Be installed, supported, and maintained by NMJB Information Technology
- Use NMJB approved authentication protocols and infrastructure
- Use NMJB approved encryption protocols
- Not interfere with wireless access deployments maintained by other organizations.

Wireless users are prohibited from sending protected information over untrusted wireless networks. NMJB expressly prohibits the use of ad-hoc or peer-to-peer wireless networks on any of its information assets.

5.4 Network Segmentation

Networks will be segmented and labeled based on their respective trust level, and deemed either trusted or untrusted. Network segmentation will be implemented based on business risk, which is the impact resulting from the exploitation of a vulnerability. This resulting calculus takes into account existing controls, mitigating factors, data classification, application tier, compliance requirements, and organizational mission.

Segmentation principles will be applied regardless of information asset location, region, system type (production, development, QA, etc.), or Technical Owner, e.g. deny all network communications traffic, permit by exception. This means that all NMJB networks, whether located on premise or hosted data centers, are subject to segmentation. Hosted service provider environments to which network segmentation cannot be directly applied must demonstrate equivalent compensating controls (technical and contractual) to achieve a commensurate level of risk reduction to the NMJB.

5.5 System Security

The NMJB will deploy enterprise anti-malware administration tools that inspect traffic from Internet sources for executables and malware. Scanning methods must include a signature-based detection engine and may include behavioral-based engines. NMJB will maintain enterprise anti-malware management consoles and all anti-malware software agents will automatically report to these centralized consoles.

The NMJB will deploy software inventory tools to each of the NMJB's information systems. Each system shall run the latest tested, approved and updated system software for both the server's operating system and all applications installed on the system in accordance with this organization's Configuration Management Policy.

All critical services such as Domain Naming Services, email and other business critical services will be installed and maintained on separate physical or logical hosts. These systems will have enhanced monitoring and security, including yearly security review of those systems.

Backups of each system shall be performed on a regular basis. Backups shall be performed of each server's operating system, application code, system and application configurations, and business information.

5.6 Encryption & Key Management

The NMJB shall utilize hashing, symmetric and asymmetric key algorithms to encrypt authentication information and other critical information. All symmetric, asymmetric keys and hashing functions shall possess a default key length of 256-bits and possess a block size of 128-bits. NMJB shall take a lifecycle approach to key management, utilizing the concepts of least privilege and separation of duties for personnel.

6 Monitoring and Enforcement

Violations of this policy may lead to disciplinary or corrective action as appropriate, which for employees could include up-to and including termination.

7 Review and Revision

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

8 Exception Handling

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

9 Authoritative Standards and Guidelines

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

- NMJ Information Security Policy
- ISO 27001:2013
    - A.12.1.1 – Documented operating procedures
    - A.12.2.1 – Controls against malware
    - A.12.6.2 – Restrictions on software installation
    - A.13.1.1 – Network controls
    - A.13.1.2 – Security of network services
    - A.13.1.3 – Segregation in networks
    - A.18.2.3 – Technical compliance review

10 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	Corrected formatting errors, replaced “policy owner” with specific title	Wesley T. Reynolds	1/29/18
0.6.1	Added seal, updated index, updated list numbering, updated revision numbering	Wesley T. Reynolds	1/30/18

11 Approval

Name (print) Signature

Title Date