New Mexico Judicial Branch

NEW MEXICO JUDICIAL BRANCH
INFORMATION TECHNOLOGY POLICY
EXCEPTION REQUEST POLICY

Revision: **0.6.2**	Document Owner: **CIO**
Last Change Date: **3/8/18**	

Cover Page

Table of Contents

1   Purpose

The purpose of this policy is to establish a formalized approach to requesting exceptions to information security-related policies.

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

- CIO – Chief Information Officer
- Compensating Control – Alternate controls designed to accomplish the intent of the original controls as closely as possible, when the originally designed controls cannot be used due to limitations of the environment.
- 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 (as defined above) or a computerized system which stores, transmits, and/or processes information. Some examples include; endpoints (desktop PCs, laptops, tablets, and smartphones), servers (physical or virtual), 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.
- JIFFY – Judicial Information Systems Council
- Risk – A qualitative measurement that depicts the potential of which a vulnerability will be exploited by a threat, and cause negative impact to an individual or NMJ. This resulting calculus takes into account, existing controls, mitigating factors, and organizational mission.
- 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 Roles and Responsibilities

Role	Responsibilities
CIO	● Review and determine the viability of all policy exception requests. ● Determine what risks the exception will pose to NMJB and what potential compensating controls are necessary. ● Approve or Deny policy exception requests.
Strategic Risk Committee (SRC)	● Review and determine the viability of all appealed policy exception requests that are approved or denied by the CIO. ● Determine what risks the exception will pose to NMJB and potential compensating controls are necessary. ● Approve or Deny appealed policy exception requests. ● Review all granted policy exception requests on at least an annual basis.
JIFFY	● Review and determine the viability of all appealed policy exception requests that are approved or denied by the SRC. ● Determine what risks the exception will pose to NMJB and potential compensating controls are necessary. ● Approve or Deny appealed policy exception requests.
Chief Justice of the Supreme Court	● Review and determine the viability of all appealed policy exception requests that are approved or denied by JIFFY. ● Approve or Deny appealed policy exception requests.

5 Policy

All NMJB Information Technology policies are intended to communicate the expectations of senior management and will be followed as prescribed. In select instances, an exception to an established information security policy or related requirement may be requested. All exception requests must be submitted to the CIO for review. The request will provide detailed information on what risks the request poses to NMJB information assets, and what compensating controls, if any, will be implemented to mitigate risks. The requestor will not perform any actions prohibited by NMJB policies until express authorization is granted. Once approved, all policy exceptions will be reviewed on an annual basis. Should the exception request be denied by the CIO, the decision may be appealed to the SRC. Should the exception request be denied by the SRC, the decision may be appealed to JIFFY. Should the exception request be denied by JIFFY, the decision may be appealed to the Chief Justice of the Supreme Court.

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 CIO no less than once every 12 months, or within 60 days after the official release of any update to applicable Information Technology security standards, regulations, or related NMJB policies.

8 Exception Handling

All exception requests will be made in accordance to the 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:

- All NMJB Information Security-Related Policies

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	Replaced "policy owner" with specific title. Updated appeal process to include JIFFY and Supreme Court.	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	Changed Supreme Court to Chief Justice	Wesley T. Reynolds	3/8/18

11 Approval

Name (print)	Signature

Title	Date