Minnesota Judicial Branch Policy

Policy Source: Minnesota Judicial Council
Policy Number: 1000
Category: Cyber Security
Title: Cyber Security Policy
Effective Date: March 1, 2018
Revision Date(s):
Supersedes:

Cyber Security Policy

I. POLICY STATEMENT

It is the policy of the Minnesota Judicial Branch to establish uniform cyber security requirements to protect the integrity, confidentiality, and security of all Judicial Branch networks, information systems and data.

This Policy applies to all employees, judicial officers, contractors, third parties, vendors, and state government agencies that access or use Judicial Branch data, electronic or voice communications systems, and/or equipment.

II. DEFINITIONS

A. Device – An object or piece of equipment capable of accessing Judicial Branch information systems or data, e.g. desktop, laptop, cell phone, handheld tablet.

B. End Point Protection - Software that protect a user's computer from viruses, spyware, and other software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the internet.

C. Judicial Branch Data – Facts and statistics created, stored or derived from the collection, filtering, and processing of information within the Judicial Branch.

D. Judicial Branch Information Systems - Interconnected networks of hardware and software used by the Judicial Branch to collect, filter, process, create, store and distribute data.

E. Managed Device – A device owned by the Judicial Branch or a device owned by a Judicial Branch employee or judicial officer that accesses Judicial Branch information or data.

F. Media Protection - A safeguard to protect electronic media containing Minnesota Judicial Branch information. Electronic media includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

III. CYBER SECURITY REQUIRMENTS

A. Identity and Access Management

The Judicial Branch shall establish uniform standards to ensure identification and authentication of users accessing Judicial Branch information systems or data. Access to Judicial Branch information systems or data shall be through authorized secure means. Authorized access shall provide for privileges to enable access to systems or data essential to the performance of the business function of the user. The Judicial Branch shall establish uniform standards for the deactivation or removal of access to Judicial Branch information systems or data.

B. Logging and Monitoring

The Judicial Branch shall monitor Judicial Branch information systems and devices accessing Judicial Branch information systems for threats, vulnerabilities and computer security incidents. The Judicial Branch shall monitor, log, review and respond to data loss on managed devices and email. The Judicial Branch shall create logs for systems that store, process or transmit non-public data.

C. Vulnerability Management

The Judicial Branch shall regularly schedule and conduct vulnerability scans for all Judicial Branch information systems. The Judicial Branch shall categorize all identified vulnerabilities by risk level and timely remediate all vulnerabilities.

D. Data Handling

Judicial Branch data shall be stored on managed centralized storage devices. All storage and transmission of Judicial Branch data shall use applications, methods of transfer or third party provided hosting solutions approved by the Judicial Branch. The Judicial Branch shall establish media protection and destruction requirements for data disposal and backup requirements for backup and recovery.

E. Network Security

The Judicial Branch shall securely configure all Judicial Branch information systems to protect the confidentiality, availability and integrity of Judicial Branch data. The Judicial Branch may restrict network connections to those necessary to the performance of the business function of the user. The Judicial Branch shall maintain current network diagrams that identify all connections (including wireless) to the Judicial Branch network.

F. Information Technology (IT) Systems

The Judicial Branch shall restrict physical access to routers, firewalls, switches, wireless access points, gateways, and other networking equipment. Judicial Branch information systems shall use a standardized, secure configuration and follow media protection and destruction requirements during decommission, reuse or recycling.

G. Software and Hardware

The Judicial Branch shall maintain and document a list of all approved hardware and software along with any usage restrictions. All application software on Managed Devices is subject to security vulnerability testing and vulnerability management.

H. Cyber Security Risk Assessment

The Judicial Branch shall establish a cyber security risk assessment process. New technologies are subject to a cyber security risk assessment before deployment. New third party partnerships related to information technology systems are subject to a cyber security risk assessment prior to contract signing. Changes to existing information technology systems are subject to a cyber security risk assessment prior to implementation.

I. Security Incident Management

The Judicial Branch shall log, track, prioritize and resolve all cyber security incidents. The Judicial Branch shall adhere to a cyber security incident management process for all known security-related incidents. Users of Judicial Branch information systems or data shall promptly report all suspicious activity and information security concerns pursuant to an established protocol.

J. Security Awareness

All Judicial Branch employees and judicial officers shall complete and attest to the completion of biennial cyber security training. Contractors, third parties, vendors, and state agencies may be asked to show proof of attending cyber security training within the last year, if necessary, for the execution of a contract or agreement.

IV. IMPLEMENTATION AUTHORITY

Implementation of this policy shall be the responsibility of the State Court Administrator acting as the Judicial Council's agent, in consultation with the Cyber Security Steering Committee.

V. EXECUTIVE LIMITATIONS

Not applicable.