NORTH Dakota | Information Technology
Be Legendary.

Created: 03/10/2025
Revised: 07/15/2025
Reviewed: 07/15/2025

Prohibited Technologies Policy

1.0 PURPOSE

The purpose of the Prohibited Technologies Policy is to minimize risks in protecting data and systems. The policy prevents the use of applications, software or hardware that pose a critical cybersecurity risk to the confidentiality, integrity, availability, or privacy of data and systems.

2.0 STATEMENT OF MANAGEMENT COMMITMENT

The North Dakota Chief Information Officer (CIO) directs that Information Technology (IT) Policy be created, as defined within the North Dakota Century Code (Chapter 54-59-09). The Governance Review Team is responsible for reviewing and updating this policy. Reviews and updates to the policy and procedures will be a coordinated effort and be done annually or as immediate changes are required.

North Dakota's Chief Information Security Officer (CISO) directs that this policy is created to provide appropriate security and privacy safeguards and countermeasures against the threats and vulnerabilities that may impact the confidentiality, integrity, and/or availability of information and information systems.

3.0 SCOPE

This policy applies to all executive branch state agencies.

4.0 DEFINITIONS

STAGEnet – The statewide network, known as the North Dakota Statewide Technology Access for Government and Education network (STAGEnet), was created by the 1999 legislative session. STAGEnet provides broadband connectivity, Internet access, video conferencing and other networking services for North Dakota state entities.

State-Owned Device – Laptop and desktop computers, cell phones, tablets, and other internet capable devices.

Prohibited Technologies – Any technologies listed within the Policy section of this document for prohibited software or hardware. This includes, but is not limited to, certain applications, software, hardware, companies, telecommunications devices, and equipment.

5.0 POLICY

5.1 State-Owned Devices

The use or installation of prohibited technologies is prohibited on all state-owned devices and STAGEnet. NDIT will identify and track NDIT-managed devices to prevent the installation of or access to Prohibited Technologies or remove Prohibited Technologies on state-owned devices.

All state-owned devices will be managed using an approved mobile device management solution.

NDIT-managed devices shall implement security controls as defined in NDIT policies, Enterprise Architecture standards, and any Executive Orders on similar bans. NDIT can remotely uninstall unauthorized software from NDIT-managed devices. Other agencies shall use a mobile device management solution that incorporates similar controls.

5.2 Network Restrictions

NDIT will implement STAGEnet restrictions by:

- Configuring firewalls to block access to Prohibited Technologies on STAGEnet. STAGEnet controls for this policy apply to VPN connections, devices physically connected to STAGEnet, or connected to STAGEnet-Member wireless.
- Personally-owned devices with Prohibited Technologies are ONLY allowed to connect to STAGEnet-Guest wireless network.

5.3 Ongoing and Emerging Technology Threats

NDIT may add other applications, software and hardware products with security concerns to this policy. Applications, software, or hardware may be immediately banned if security concerns put data and systems at critical risk with detrimental impacts. NDIT will remove and prevent installation and use of Prohibited Technologies on state-owned devices as technologies are added to the Prohibited Technologies list, identified below in section 5.4 or specified by proclamation from the governor.

5.4 Prohibited Technologies

Prohibited technologies from use on a state-owned device and STAGEnet is documented in the Prohibited Technologies List.

6.0 GOVERNANCE AND COMPLIANCE

Violations of this policy will be handled in accordance with applicable State of ND policies, procedures, laws, executive orders, directives, regulations, standards, and guidelines. Team

members may report non-compliance with this policy to the NDIT Security Governance, Risk, and Compliance team for initial review. The Report for Non-Compliance is completed through NDIT's ServiceNow platform. NDIT will address submissions with Entity leadership.

This policy shall take effect upon publication. Compliance is expected with all State policies, procedures, and standards. Policies, procedures, and standards may be amended at any time.

If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support business function, entities shall request an exception through NDIT's exception process. Exceptions to this policy shall be requested though the Policy Exceptions request.

7.0 RESOURCES

December 13, 2022	Gov. Burgum Signs Executive Order to Ban TikTok for Executive Branch Team Members
March 10, 2025	DeepSeek Blocked on State Devices

8.0 REVISION HISTORY

Date	Authored/Reviewed by	Approved by	Version	Description of Change
03/10/2025	NDIT Governance, Risk, and Compliance Team	Governance Review Team	0.1	Policy draft created
03/26/2025	NDIT Governance, Risk, and Compliance Team	Governance Review Team	0.2	Draft completed
04/04/2025	NDIT Executive Leadership Team	Governance Review Team	1.0	Review completed
05/13/2025	Attorney General's Office	Attorney General's Office	1.1	Review and approval of language; modified Ongoing and Emerging Threats section to reference Prohibited Technologies List
06/17/2025	NDIT Governance, Risk, and Compliance Team	Governance Review Team	1.2	Link to Prohibited Technologies List provided

Date	Authored/Reviewed by	Approved by	Version	Description of Change
07/15/2025	NDIT Governance, Risk, and Compliance Team	Governance Review Team	1.3	Updated Section 5.1 to include devices not managed by NDIT