NORTH Dakota | Information Technology
Be Legendary.

Created: 03/26/2025
Revised: 05/19/2025
Reviewed: 05/19/2025

Prohibited Technologies List

1.0 OVERVIEW

The Prohibited Technologies List provides a full list of prohibited technologies in response to the Prohibited Technologies Policy. The Prohibited Technologies Policy was created in March 2025 for applications, software, or hardware that pose a critical cybersecurity risk to the confidentiality, integrity, availability or privacy of state data and systems. North Dakota Century Code (Chapter 54-59-05) requires North Dakota Information Technology Department (NDIT) to secure the state network (STAGEnet) by implementing security controls to safeguard data and systems.

2.0 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.

3.0 GOVERNANCE AND COMPLIANCE

Violations of the Prohibited Technologies 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.

If compliance with the policy is not feasible or technically possible, or if deviation from this policy is necessary in using a prohibited technology 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.

4.0 Prohibited Technologies

The following lists are technologies prohibited from use on state-owned devices and networks.

Prohibited Applications, Software, Developers (as of April 2, 2025):

- ByteDance Ltd.
  - Risk Assessment Date: 7/20/2022
  - Effective Date: 12/13/2022
- DeepSeek
  - Risk Assessment Date: 02/05/2025
  - Effective Date: 3/10/25
- Kaspersky
  - Risk Assessment Date: N/A Banned by Federal Government
  - Effective Date: 9/29/2024
- RedNote
  - Risk Assessment Date: 01/14/2025
  - Effective Date: PENDING
- TikTok
  - Risk Assessment Date: 7/20/2022
  - Effective Date: 12/13/2022
- Perplexity AI
  - Risk Assessment Date: 03/24/2025
  - Effective Date: PENDING
- Manus AI
  - Risk Assessment Date: 04/02/2025
  - Effective Date: PENDING
- 4KDownloader
  - Risk Assessment Date: 11/30/2023
  - Effective Date: PENDING
- AE Juice/AI VoiceOver
  - Risk Assessment Date: 01/22/2025
  - Effective Date: PENDING
- CamScanner
  - Risk Assessment Date: 05/19/2025
  - Effective Date: PENDING
- MooMoo
  - Risk Assessment Date: 05/23/2025
  - Effective Date: PENDING
- Tiger Brokers

    - Risk Assessment Date: 05/19/2025
    - Effective Date: PENDING
- WPS Office
    - Risk Assessment Date: 05/19/2025
    - Effective Date: PENDING
- Alipay
    - Risk Assessment Date: 05/19/2025
    - Effective Date: PENDING
- Lemon8
    - Risk Assessment Date: 05/19/2025
    - Effective Date: PENDING
- Tencent Holdings LTD (QQ Wallet, WeChat, and WeChat Pay)
    - Risk Assessment Date: 05/19/2025
    - Effective Date: PENDING
- SHAREit
    - Risk Assessment Date: 04/16/2025
    - Effective Date: PENDING
- Any subsidiary or affiliate of an entity listed above.

Prohibited Hardware, Equipment, Manufacturers (as of March 18, 2025):

- Federally Prohibited Manufacturers: United States General Services Administration (GSA)
    - Kaspersky Lab
    - Huawei Technologies Company
    - ZTE Corporation
    - Hytera Communications Corporation
    - Hangzhou Hikvision Digital Technology Company
    - Dahua Technology Company
    - Any subsidiary or affiliate of an entity listed above

5.0 QUESTIONS

For questions regarding prohibited technologies, please contact the NDIT Service Desk at (701) 328-4470 or submit an online incident.

6.0 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	List Draft Created
03/26/2025	NDIT Governance, Risk, and Compliance Team	Governance Review Team	1.0	Draft Completed
04/02/2025	NDIT Governance, Risk, and Compliance Team	Governance Review Team	1.1	Added technologies to the list
05/19/2025	NDIT Governance, Risk, and Compliance Team	Governance Review Team	1.2	Added to the technologies list