NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

State of North Carolina

Use of High-Risk Applications Policy

Statewide Security Policy

Version 1.1

February 6, 2025

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
Jan 26, 2023	1.0	New	Policy Creation	ESRMO
Feb 5, 2025	1.1	Revised	Updated to new format. Added DeepSeek to high-risk applications	Chris Brittingham

Document Details

Department Name	Enterprise Security and Risk Management Office
Owner	State Chief Risk Officer
Title	Use of High-Risk Applications Policy
Publication Date	January 26, 2023
Last Update	February 6, 2025
Document Type	PDF
Document Number	1
Version	1.1

Table of Contents

Purpose

The N.C. Department of Information Technology (NCDIT) is responsible for adopting, establishing and enforcing information technology security policies for state agencies (N.C.G.S. 143B-1321(a)).

The state chief information officer (State CIO) is responsible for the security of all state data and state networks and for adopting and establishing a statewide policy for information technology security and privacy to maximize the security of the state's distributed information technology assets (N.C.G.S. 143B-1376(a)).

In addition, the Statewide Information and Security Manual requires state agencies to ensure third parties and providers of external system services comply with statewide security and privacy requirements, as outlined in the System and Services Acquisition Policy (SA-9, External System Services).

Certain applications, websites and other technologies present a significant and increasing risk to the security and privacy of state data and the state infrastructure. To best protect the safety, security and privacy of North Carolinians, Executive Order No. 276 directs NCDIT and the State CIO to develop a policy to restrict the use of these technologies.

Therefore, NCDIT and the State CIO adopt this policy for information technology.

Owner

State Chief Risk Officer, Enterprise Security and Risk Management Office (ESRMO)

Scope

This policy applies to all employees of state agencies (as defined below) and covers those devices owned or issued by state agencies including but not limited to mobile devices, smartphones, tablet computers, televisions or displays, laptop or desktop computer and any other state-owned or state-issued device that may be utilized to access the internet via a cellular, Wi-Fi, fixed wireless or any internet service provider.

This policy also applies to any access to high-risk applications or affiliated websites via the state network.

This policy applies to personal devices only to the extent that a personal device is connected to the state network.

Policy

Section 1. Implementation

This policy shall be effective February 6, 2025, and shall remain in effect until otherwise repealed. NCDIT may amend this policy based on the evolving cybersecurity landscape, or changes to state or federal law, in consultation with the Governor's Office. No later than twenty-four (24) hours after the effective date of this policy, state agency and state agency employees must comply with the requirements of this policy. All state agencies subject to this policy shall work with NCDIT to ensure compliance with this policy.

Section 2. Definitions

1. "State Network" is defined as any connectivity managed by NCDIT designed for the purpose of providing internet protocol transport of information for state agencies (N.C.G.S. 143B-1370(a)(5)(g)). For purposes of this policy, the state network does not include any fully segmented "guest networks," which are intended for the public's use and are maintained by the

state or a state agency.

2. "High-Risk Application" means any application, website or other product that poses an unacceptable level of cybersecurity risk to state data. High-risk applications may include those applications where NCDIT has a reasonable belief that the vendor or manufacturer may participate in activities such as surveillance by government entities, cyber-espionage or inappropriate collection of the personal information of state agency employees.

3. For purposes of this policy, "state agency" shall have the same meaning provided in N.C.G.S. 143B-1320(a)(17).

Section 3. High-Risk Applications

Applications currently identified by NCDIT to be high-risk technologies include the following applications:

- **TikTok**
- **WeChat**
- **DeepSeek**

NCDIT may modify this list to remove or include additional high-risk technologies, in consultation with the Governor's Office.

Section 4. Requirements

1. State agency employees may not install or otherwise utilize the identified high-risk applications on state issued devices and must remove any existing instances of the TikTok, WeChat and DeepSeek applications from state-issued devices within the time specified in the policy.

2. State agency employees may not access any high-risk technology website on a state-issued device.

3. The state network may not be used to access high-risk technology on any personally owned device.

4. State agencies and their employees may obtain an exception from the prohibition on the installation and use of high-risk applications for law enforcement or other legitimate purposes under conditions specified by NCDIT.

Section 5. Exceptions

Exceptions to this policy must be submitted to ESRMO and be approved in writing by the State CIO. Agencies must use the N.C. Department of Information Technology (NCDIT) Exception Request Process and Form (Form C: Security) to request any exception(s) to this policy and shall include a plan for risk mitigation.

Section 6. Violations

Violation of this policy could result in disciplinary action up to, and including, termination.

Regulations and Applicable Laws

The following reference sections in the N.C. General Statutes provide additional information with respect to compliance with state law.

- N.C.G.S. 143B-1320(a)(17)
- N.C.G.S. 143B-1321(a)
- N.C.G.S. 143B-1370(a)(5)(g)
- N.C.G.S. 143B-1376(a)
- Executive Order No. 276