State of North Carolina

Use of High-Risk Applications

Version 1.0

January 26, 2023

INTRODUCTION

AUTHORITY AND PURPOSE

The North Carolina Department of Information Technology ("DIT") is responsible for adopting, establishing, and enforcing information technology security standards 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 standard 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 DIT and the State CIO to develop a policy standard to restrict the use of these technologies.

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

OWNER

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

SCOPE

This policy standard 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 standard 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This policy shall be effective January 26, 2023, and shall remain in effect until otherwise repealed. DIT may amend this policy based on the evolving cybersecurity landscape, or changes to state or federal law, in consultation with the Governor's Office.

Not later than sixty (60) days 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 DIT to ensure compliance with this policy.

SECTION 2. DEFINITIONS

1. "State Network" is defined as any connectivity managed by DIT 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 Application may include those applications where DIT 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.

Applications currently identified by DIT to be High-Risk Technologies include the following applications:
TikTok
WeChat.

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

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

SECTION 3. 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 and WeChat 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 DIT.

SECTION 4. EXCEPTIONS

Exceptions to this policy must submitted to ESRMO and be approved in writing by the State CIO. Agencies must use the Department of Information Technology (DIT) 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 5. VIOLATIONS

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