Network Access Policy

Approved Date – 02/22/2021
Published Date – 02/22/2021
Review Date – 03/29/2024

1. Purpose

Establish the policy for safeguarding District information technology (IT) and communications ecosystems, data assets, District workforce members, District constituents, and other stakeholders. Due to ever increasing risks, threats, and vulnerabilities, the District must respond with the availability and continued modernization of security policies and technology which provide for information confidentiality, integrity, and availability.

2. Authority

DC Official Code § 1-1401 et seq., provides the Office of the Chief Technology Officer (OCTO) with the authority to provide information technology (IT) services, write and enforce IT policies, and secure the network and IT systems for the District government. This document can be found at: *https://code.dccouncil.us/dc/council/code/sections/1-1402*.

3. Applicability

This policy applies to all District workforce members (including contractors, vendors, consultants, temporary staff, interns, and volunteers) performing official functions on behalf of the District, and/or any District agency or entity (e.g. subordinate and independent agencies, Council of the District of Columbia, D.C. Charter Schools, etc.) who receive enterprise services from OCTO. In addition, this policy applies to any provider or third-party entity with access to District information, networks, and applications.

4. Policy

District agencies and departments must develop or adhere to a strategy which demonstrates compliance with this policy and its related standards. The following outlines the requirements for this policy. The District's agencies must develop and review or update annually and after changes to the policy, a procedure in support of this policy with the following requirements.

4.1. On Network:

4.1.1. Only DC Agency authorized endpoints shall be used to access DC networks.
4.1.2. DC Workforce Members that access DC networks must be granted the most restrictive set of privileges required to perform authorized tasks.
4.1.3. DC Workforce Members that access DC networks must be connected using enterprise active directory credentials.
4.1.4. DC Workforce Members that need to perform IT administrator tasks on DC networks must use a separate privileged account to perform authorized tasks.
4.1.5. DC Agency authorized endpoints must implement an OCTO authorized Operating System image. The following OCTO security and management tools must not be

disabled or removed: an endpoint management agent), Anti-Virus Software), and Full Disk Encryption (for laptops). These requirements are further described in the "OCTO Endpoint Device Standards." Remote administration by any DC Agency must only be performed using the OCTO-approved tools.

4.1.6. Remote Administrative access to enterprise resources within DC Data Centers must use a privilege access management solution (e.g., Direct administrative access from an endpoint to enterprise resources in DC Data Centers is strictly prohibited.

4.1.7. All non-DC agencies must sign a Memorandum of Understanding (MOU), Interconnection Security Agreement (ISA), and/or external rules of behavior document to gain access to DC information and communication technology resources.

4.1.8. All inter-agency network communication must be authorized; DC agencies are prohibited from accessing other DC agency non-public resources without an MOU.

4.2. Off-Network/Virtual Private Network (VPN) Access

For specific VPN guidance, refer to the OCTO Virtual Private Network (VPN) Policy.

4.2.1. Government endpoints (laptop/desktop):

- DC Agency-approved endpoints must follow the same requirements for On Network endpoints
- DC Agency-approved endpoints must only use an OCTO authorized VPN

4.2.2. Government mobile devices (phone, tablets, etc):

- DC Agency approved mobile devices must follow the same requirements as on premises network devices
- DC Agency approved mobile devices must be registered within the OCTO approved Mobile Device Management Solution (MDM)

4.2.3. Non-Government endpoints (e.g., BYOD):

- Non-government endpoints are is permitted only if the use is authorized by the Agency Director or their designee, and if the device is registered within the OCTO approved (MDM)
- Agency helpdesks are not required to provide help desk support for these devices
- Non-government endpoints must use an OCTO authorized Layer-4 VPN connection to authorized network resources

4.3. Access Not Conforming to Standards

Access to the network not conforming to the above standards is expressly prohibited.

5. Exemption

Exceptions to this policy shall be requested in writing to the Agency's CIO and the request will be escalated to the Chief Information Security Officer (CISO) for approval.

6. Definitions

The definition of the terms used in this document can be found on the *Policy Definitions website*.