Document Title:	**Remote Access Policy and Acceptable Use Agreement**[1] [2]
Document Type:	*Policy / Employee Agreement*
Document Purpose:	This policy provides guidelines for Government and non-Government users of Remote Access (RA), remote access security appliances or routers to the Government network.
Scope of Application:	This policy applies to all Government employees, authorized contractors, consultants, constitutional employees, temporaries, and other workers, including all personnel affiliated with third parties that use Remote Access via Virtual Private Networks (VPNs) or remote access security appliances or routers to enter the Government's network. This policy applies to all methods of remote access, including but not limited to read-only access to network resources, remote access to the desktop, with access via workstation, laptop, or mobile device (i.e., iPad, notebook, iPhone, or smartphone).

1. Policy Details

Authorized Government employees and authorized third parties (visitors, vendors, etc.) may use the benefits of Remote Access, a "user managed" service. "User Managed" means that the user is responsible for selecting a compatible Internet service provider (ISP), coordinating installation of required software, and paying associated fees, etc. The ISP must provide a single IP address for the remote computer for the entire VPN session.

Vendors and other non-Government users may utilize the Government's remote access capability if approved by sponsoring agency directors, immediate supervisors or project managers.

[1] This policy template is based on policies provided by Arlington County as a response to the call, by the Mason - NSF project (No. 1623653), for cybersecurity partnership and information sharing among cities and counties.

[2] As used in this document, (i) "Government" means XXX County/City Government, (ii) "CIO" means Chief Information Office or his/her designee, (iii) "Department of Technology and Information Services" or "DTS" refers to the department that manages the Information Communication Technology, (iv) "CISO" means the Chief Information Security Office or his/her designee, (v) "Communications Office" refers to the department or designee that manages communications and public relations, (vi) "Chief Records Management Officer" or CRO means the officer that manages Government records policies and enforcement.

For Government-owned equipment, the sponsoring agency is responsible for providing Government equipment (i.e., workstation, laptop, router, and IP telephone), additional software and licensing fees (such as Absolute security software, Cisco Call Manager or any software required to conduct Government business). For equipment not owned by the Government, the owner will bear the cost of any software and licensing fees.

If remote network access is required, then users may be required to use VPN client software, which will be provided by DTS, licensing and installation instructions required to enable a secure connection to the Government network. This applies to both Government-owned and non-Government owned equipment.

All users that utilize equipment that is not Government-owned must abide by this policy and maintain current versions of anti-virus software and protection by a firewall. The sponsoring agency will approve a non-Government user's access and provide details of access requirements (such as telnet/ftp access to a specific server).

DTS will provide remote access for Government employees, authorized contractors, consultants, constitutional employees, temporaries, and other workers, including all personnel affiliated with third parties and allow appropriate access to the Government network. To be in compliance with this policy, the user will adhere to the following acceptable use requirements.

(1) It is the responsibility of the user with remote access privileges to ensure that unauthorized users are not allowed access to Government's internal network. This includes the physical security of the machine. If a user suspects unauthorized access or if the user's Government provided equipment is lost or stolen, then the user must immediately contact the Government Help Desk and sponsoring agency.

(2) Remote access is controlled by user name and password. Each user is responsible for securing their user name and password. Any activity performed through the use of an authorized user account will be assumed to have been conducted by that user. The user assumes full responsibility for all actions performed by their account. If a user suspects unauthorized access, then the user must immediately contact the Government Help Desk and the sponsoring agency.

(3) There is no expectation of privacy. All activity while connected to the Government Network via remote access may be monitored, in accordance with Electronic Communications and Internet Services Policy[3].

(4) Only one network connection is allowed. Dual (split) tunneling is not permitted. Split tunneling allows a remote access user to access both a public network (e.g. the Internet) and the Government network at the same time using the same physical network connection.

(5) Gateways will be set up and managed by the Department of Technology Services (DTS).

(6) All computers connected to the Government's internal network via remote access must use the most up-to-date anti-virus software that is the Government standard. In addition, all computers must utilize a firewall, which can be software, hardware or both. This applies to computers owned by vendors or employees.

(7) All Government-owned laptop computers must have an active license for computer theft recovery and data protection software. DTS can load and activate the software on Government laptops upon request.

(8) Remote access users will be automatically disconnected from the Government's network after thirty minutes of inactivity. The user must then log in again to reconnect to the network with their username and password. Pings or other artificial network processes are not to be used to keep the connection open.

(9) Users of computers not issued by Government are responsible for configuring the equipment to comply with Government's remote access policies.

(10) By using remote access with equipment not issued by Government, users acknowledge that this equipment is a de facto extension of Government 's network. As such, users are subject to and must conform to the provisions in Electronic Communications and Internet Services Policy, and all other rules and regulations that apply to Government-owned equipment.

(11) Users who fail to follow any of the policies provided by the Government may forfeit remote access privileges.

2. Remote Access Service Support

[3] Reference to Mason - NSF VA City and County Cybersecurity Partnershing, Leadership and Governance / Document reference Number VA Series-01

DTS will provide support for the remote access service during normal business hours of operation, weekdays 7 AM to 5 PM. Service desk tickets should be issued for all remote access service issues.

DTS does not support non-Government resources such as personal laptops or workstations. This includes Government and non-Government users. Limited support for these devices will include verifying the remote access service is available and validating user name and passwords.

3. Remote Access Service Termination

Any agency sponsoring Remote Access will notify DTS of any account termination requests, ten days prior to the effective termination date.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Contractors, consultants, temporaries, constitutional employees and other workers, including all personnel affiliated with third parties using remote access to access Government's network will be held liable for any damage, leakage, and/or destruction of Government information.

Your signature means that you have read, understand and ***agree to comply*** with the requirements of this policy.

_____ _____

User Signature Date

_____

Contractor / Vendor Name (if applicable)

_____ _____

Authorizing Government Supervisor Date

Department Charge Code (if applicable): _____