Document Title:	**Electronic Communications and Internet Services Policy**[1] [2]
Document Type:	*Policy*
Document Purpose:	This policy provides guidelines on the usage of Government provided services and resources for the purpose of electronic communications and internet use. This policy is designed to protect the Government's computer networks and data assets against unauthorized and malicious use as well as to prevent potential misuse of Government resources.
Scope of Application:	This policy applies to all Government employees, contractors, consultants, constitutional employees, temporaries, and volunteers.

1. Background:

Government provides services and resources to enhance the ability of the user to perform job duties, improve customer service, increase productivity, reduce paperwork and provide opportunities for professional growth. E fficient use of these services and resources may enhance partnership, community involvement and information exchange among citizens, businesses and governments; provide information on Government activities and services both internally and to the public, and improve the quality, productivity and general cost-effectiveness of the Government's work force.

This policy defines access to and the use of these services and resources, and ensures that their use is consistent with Government policies, applicable laws, and the individual user's job responsibilities. It is designed to protect Government's computer networks and data assets against unauthorized and malicious use as well as to prevent potential misuse of Government resources.

[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 Officer or his/her designee, (iii) "Department of Technology and Information Services" or "DTS" refers to the department that manages the Information and Communication Technology, (iv) "CISO" means the Chief Information Security Officer 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.

2. Definitions:

This policy covers Government "networked resources," which for purposes of this policy includes the Government's email system, network, software, applications, databases, internet/intranet access, all computer systems, internally hosted or cloud-based, hardware, temporary or permanent files and any related systems or electronic devices authorized, personally owned or leased by the Government and/or made available to employees or other authorized users in their role as employees or authorized users.

"Internet services" include the following:

(1) Internet access and usage - Internet access is defined as the ability to connect to and access the Internet.
(2) Electronic Messages sent using the Government's domain as well as sent through the Internet - This policy is applicable to e-mail, text messaging, social media posts, messages sent to list services, user groups and other Internet forums.
(3) VPN - Use of Internet resources while connected through a Virtual Private Network.
(4) Installation of Network devices - Appliances such as routers, hubs, switches, wireless access points, or other devices which facilitate authorized access to Government servers, messaging systems or the Internet.
(5) Social Media - This policy supplements the Government's regulations regarding social media use and maintenance of web sites.
(6) Calendaring - The electronic systems provide a scheduling function whereby employees may schedule meetings with each other and non- Government personnel. Calendaring capability also provides for the reservation of resources such as conference rooms and equipment.

3. Roles and Responsibilities:

The Chief Information Officer (CIO) and the various sponsor groups of his/her peers from the Executive Leadership Team and Constitutional Officers have managerial responsibility for the technology initiatives contained in this regulation. The CIO is responsible for reviewing and approving any exceptions to this policy.

Department of Technology and Information Services (DTS) is responsible for providing, administering, and insuring security and records management compliance of messaging services, as well as a secure Internet/Intranet connections.

Government networked resources are intended for Government business purposes only. Therefore, users must adhere to this policy. If in doubt, the burden of responsibility is on the user to inquire as to acceptable and unacceptable uses prior to accessing network resources. Questions concerning whether a particular use is acceptable or unacceptable should be referred to the department director, delegated representative or the DTS Help Desk.

Users are expected to know how to manage records in an electronic messaging system and to comply with Government's records retention policies. Questions related to records retention should be directed to the DTS Help Desk.

4 . **Ownership and Privacy**

All information created, generated, transmitted, and stored by users is the property of the Government. The information is not considered private. The Government reserves the right to set or restrict permissions and accessibility rights to all data resources as it deems necessary. The Chief Information Security Officer (CISO) will authorize access to data stores upon written request.

5. **Access and Monitoring**

There is no expectation of privacy when using Government networked resources whether those resources are locally hosted or cloud-based. The Government reserves the right to monitor and/or log all network activity with or without notice, including messaging and all web communications. The Government will not monitor individual messaging or device tracking without proper approval following established Government processes.

However, in the routine course of technology administration, the Government undertakes construction, repair, operations and maintenance of messaging systems that may occasionally result in accessing random transmitted or stored messages. Government servers also maintain logs of Internet activity, i.e., sites accessed by users and Internet traffic. Government servers also maintain logs reflecting messaging traffic, i.e., to whom messages were sent and received; including external destinations.

Monitoring of a specific activity, or an individual's use, may be performed without consent or knowledge of the individual only under the following circumstances and only when authorized by the Government CISO. By way of example, not limitation, monitoring and/or access may be authorized:

(1) If required by law or in defense of a charge, claim, notice of violation or lawsuit;
(2) When reasonably necessary to investigate a possible violation of a Government Policy, breach of security or in support of a FOIA related request;

(3) When there is reasonable suspicion that a user has committed or is committing a crime;
(4) If there is a suspected violation of this policy, of any administrative regulation and/or to investigate claims made against the Government, the CISO will notify the Office of the Government Attorney;
(5) To comply with the requirements of the Virginia Freedom of Information Act (FOIA)[3] and the Virginia Public Records Act[4];
(6) To comply with any Litigation Hold requirements or legal discovery requests; and/or
(7) To resolve a technical problem.

6. Acceptable Uses

(1) Network resources shall be used:

a. In the pursuit of Government goals, objectives and activities - Official Government business conducted via networked resources and electronic communications shall comply with all statutory requirements;

b. When electronic communications are the most efficient and/or effective means of accomplishing the Government's business;

c. For Government work-related job responsibilities, research, activities and/or information gathering;

d. Using utility and applications software that accomplish tasks and fulfill job functions that are under a license issued to the Government;

e. To facilitate communication and collaboration between staff and/or other appropriate entities or persons; and/or

f. To support the professional activities or projects of users (e.g. electronic scheduling of meetings, electronic calendars, project management software, address books and completion of work related forms electronically) that support the user's official Government responsibilities and job duties.

(2) Incidental and reasonable personal use is permitted so long as it does not interfere with the conduct of a user's work, the effective delivery of services, incur cost to the Government, generate more than incidental traffic or use of networked resources, and/or conflict with Unacceptable Uses (stated in Section 7). This limited personal use of Government networked resources is best accomplished during breaks and lunch time or to address critical personal matters.

[3] https://law.lis.virginia.gov/vacodepopularnames/virginia-freedom-of-information-act/
[4] https://law.lis.virginia.gov/vacodepopularnames/virginia-public-records-act/

(3) When using electronic communications provided by Government, employees are representing the Government and should conduct themselves as Government representatives at all times. Electronic messaging is considered an official communication of Government. In addition:

a. Only signature lines that provide an employee's name, title, physical address and contact information should be appended to any email sent in furtherance of Government business or sent through Government networked resources.

b. "Tag-lines" that are unrelated to the users work functions are not permitted.

(4) Care must be taken when handling confidential information - Confidential information contains Personally Identifiable Information (PII) including financial information, proprietary information, social security numbers, credit card or bank account numbers; health records and personally identifiable health information. Such information should be sent via encrypted messaging and stored encrypted when at rest. If sent internally, such messaging should be limited to a "need to know" basis and sent in accordance with department procedures in effect at the time of transmittal. All such messaging should be marked "confidential" and no Personal Identifiable Information (PII) should be included in the subject line of email or posting in social media applications.

(5) Use of network resources must conform to the Government's anti-harassment and discrimination policies.

7. **Unacceptable Uses**

Unacceptable uses include, but are not limited to, the following:

(1) Interference with the security or operation of Government networked resources including, but not limited to, sabotage of or vandalizing any Government or Internet hardware, software, network or data file;
(2) Deliberate introduction or distribution of computer viruses, malware, or spy ware such as keystroke logging tools;
(3) Use of network resources beyond the uses outlined in Section 8 or copying, sale or distribution of networked resources;
(4) Alteration of Government-provided Internet access configurations in any way except as authorized in writing by the director of DTS;
(5) Unauthorized use of copyright protected works including software, electronic files (including, but not limited to, messages, e-mail, text files, image files, database files, sound files and music files), movies or data or making available copies of such works or files using Government-provided electronic communications services. Permission from

the owner for the use, distribution or copying of such information must be properly documented;

(6) Except as may be necessary for the performance of the user's job, access to, generation, transmission, receipt or storage of information that is abusive, discriminatory, harassing, associated with gambling or has sexually explicit content as set forth in Virginia Code Section 2.2-2827[5];

(7) Unauthorized access to Government data intended for internal operations in support of non-Government activities related to outside employment or personal gain;

(8) Unauthorized access to materials, systems or files that are restricted by law or Government policy;

(9) Release or distribution of confidential information required by law or policy;

(10) Representation of oneself with an anonymous or fictitious name or hosting a personal web site on a Government server;

(11) Transmission of chain messages;

(12) Transmission of global (meaning to all users) or mass (appropriate number of users to be defined by agency head) e-mails, even when the content is related to Government business must be authorized by the Communications Office. Department directors, or designees, may authorize employees to send messages related to Government business to all members of a work or organizational group, or team that exceeds 50 users;

(13) Any activities unrelated to Government business in the pursuit of profit or gain for the user or on behalf of any other individual or organization;

(14) Unauthorized access of Government data intended for internal operations or any use of this data for political activities such as, but not limited to, solicitation of funds, or endorsement or advocacy of any particular candidate or political party;

(15) Storage of Government data on third-party (SaaS or cloud) applications (including, but not limited to, file storage and sharing services such as Dropbox) without prior approval from DTS;

(16) Storage of Government data on personal devices or media, if the device or media does not have Mobile Device Management software installed and activated;

(17) Storage of official Government records in applications that have not been approved by the Chief Records Management Officer, or storage of official Government records on media that is not backed up on a routine basis;

(18) Violating the rights of others by publishing or displaying any information that is defamatory, obscene, known to be false, inaccurate, abusive, profane, sexually oriented, threatening, racially offensive, and considered to be bullying or otherwise biased, discriminatory or illegal or otherwise insensitive forms of humor.;

[5] https://law.lis.virginia.gov/vacode/title2.2/chapter28/section2.2-2827/

(19) E-mail or social media discussions involving any subject that interferes with work or where items are debated at length;
(20) Unreasonable work time surfing the Internet, as determined by the employee's job functions and the task involved;
(21) Misrepresenting one's position in the Government for activities unrelated to official Government business;
(22) Using Government networked resources for private consulting or personal gain.
(23) Uses that violate Government warranties or terms of use for Government-provided devices or software;
(24) Forwarding (bulk or individually) of Government official email accounts to personal email accounts without prior authorization from the CISO;
(25) The use of or installation of routers, hubs, switches, wireless access points, Internet of Things (IoT) devices, etc., without authorization from DTS;
(26) Use of technology to capture and record video and/or audio content where privacy is presumed or where such use has not been authorized.

8. Compliance with Copyright, Licensing and Terms of Use:

Users are required to honor copyright laws of any materials and all site or software terms of use and licensing restrictions. Software piracy is both a crime and a violation of Government policies. Illegally reproducing software may be subject to criminal and civil penalties as well as disciplinary action. In no instance shall any user disassemble, reverse engineer or otherwise reproduce any software or code provided by the Government. Further, all software must be used strictly in accordance with its license agreement, including any restrictions on the number of users.

Please be aware that many copyright and licensing restrictions do not allow a person to store copies of a program on multiple machines, distribute copies to others via disks or Internet or to alter the content of the software unless permission has been granted under the license agreement. Most times, supervisory permission is also required by the Government. If copyrighted material is downloaded, it must be with permission of the owner and its use must be strictly within the agreement as posted by the owner, author or otherwise in accordance with current copyright law.

9. Virus protection

Government's standard anti-virus software must be installed on Government PCs prior to accessing Government networked resources. DTS is responsible for the installation of virus protection software on PCs that departments purchase. In the event updates do not occur successfully, users must contact the DTS HELP DESK to open a trouble ticket so that the updating process can be re-established. Any virus detected must be reported to the DTS HELP DESK.

10. Security

Government users are responsible for their email and social media accounts. To ensure security compliance, users are prohibited from using another person's user ID, password, files, systems, even if that person has neglected to safeguard his/her user ID. Users are specifically prohibited from messaging under another user's name or spoofing another individual's identity.

Employees, contractors, or vendors responsible for connecting outside networks to the Government's network are liable for any damages which may occur as a result of the connection. Safeguards such as Firewall protection, VPN, Data Loss Prevention, Encryption, and other security technologies must be provisioned and authorized by DTS. DTS must be notified prior to any connection between a non-Government and Government-network. Every department that uses the Government's Internet gateway must be authorized and registered through DTS. Every "device" or "host" connecting to the Internet must have a unique identifier assigned by DTS.

Internet security protocols can be compromised. Users should assume that all transmissions over the Internet via e-mail, the Web, or other media, such as file transfer protocol (FTP), are publicly available, and individuals other than the intended recipient(s) can intercept such information (reference Section 13(5).).

When working remotely, users must ensure anti-virus and firewall software operating on their telework device has been updated.

When using wireless routers for telework users must activate password protected access as well as transmission encryption (example WPA2).

When using Mobile Devices (such as iPhones, iPads, etc.), the user must ensure the device has DTS enabled Mobile Device Management (MDM) installed and activated. If any smart device (Government or BYOD), which contains Government information is lost or stolen, the user must notify DTS Help Desk within 24 hours (Reference – *Mobile Device Use and Management Policy*).

Password protection of all electronic devices is required. All users shall be required to change network access passwords in a manner and time as determined by DTS (please see below). Passwords are not to be shared or otherwise distributed by any user except as authorized. Passwords must be changed every 90 days without exception.

Contractors who may have access to Government confidential information shall be required to sign the Government's *Nondisclosure and Data Security Agreement* prior to commencing work under any Government contract.

The provision of new applications must comply with DTS information governance requirements as defined by the CISO and Chief Records Management Officer (CRMO).

11. Access Violations

It is a violation for any user, including the system administrator, security administrator, supervisors and department directors to access any e-mail system, files or communications that do not belong to them except for authorized business purposes or as noted in Section 6. The Government reserves the right to monitor access in order to ascertain whether unauthorized access has been attempted.

12. Failure to Comply

Employees who fail to comply with this policy may be subject to disciplinary action that could result in cancellation of system access, disciplinary action up to and including termination of employment and/or criminal prosecution.

13. Policies Specific to Internet Access and Usage

(1) **Integrity of Information.** When using information from an Internet site for Government business decisions, employees should verify the integrity of that information, i.e., that the site is updated on a regular basis (the lack of revision date might indicate out-of-date information) and that it is a valid provider of the information. Just because it is there does not mean that it is accurate or valid.

The Government has no control or responsibility for content on an external server not managed by DTS.

(2) **Web-based Applications.** The use of free web-based applications must be approved by DTS.

a. Employees are responsible for any Government content stored and must ensure that the information is protected and conforms to all Government policies.

b. Employees are responsible for ensuring that the Government information that is used or posted is authorized to be released to the public and any content created by the user is retained in accordance with the Government's record management policies. Both record retention and information security standards apply to non-Government hosted Web sites.

c. Sensitive or confidential information requires pre-approval before posting or use in an web-based application and includes but is not limited to Personally Identifiable Health information (ePHI), dates of birth, Social Security Numbers (SSN); Critical Infrastructure (CI) information such as drinking water, sewage pipe, fiber, underground power grid routes, internal disaster recovery plans; and also includes but is not limited to information that in any manner that describes, locates or indexes anything about an individual including, but not limited to, his/her (hereinafter "his") real or personal property holdings, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, Social Security Number, tax status or payments, date of birth, address, phone number or that affords a basis of inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual, and the record of his presence, registration, or membership in an organization or activity, or admission to an institution or other sensitive information and should not be content that is associated with free web based applications which often times retain or track the content.

d. Free web tools that help develop presentation materials are not in the control of DTS are not authorized for use by employees.

(3) **Commercial Internet accounts.** All access to the Internet, for Government purposes or on Government equipment, will be provided through the Government's Internet access facilities. Commercial subscription accounts (e.g., COMCAST, AOL, etc.) are not authorized.

(4) **Streaming media.** Certain features of the Internet, such as streaming audio and video, can saturate the Government's Internet connection, and are only to be used for Government business.

(5) **File Transfer Protocol (FTP).** A user should not FTP to any system on which they do not have an account, or that does not allow anonymous FTP services. Downloaded files may contain viruses. Observe the Government's policy with respect to scanning files for viruses. Observe any posted restrictions on the FTP server.

(6) **Telnet.** Users should not Telnet (a program that allows the user to access distant computers via TCP/IP connections) to machines on which they do not have an account, or where there is no guest account. Users should observe any posted restrictions when they Telnet to another machine.

(7) **Remote Access.** Users who are authorized to Telework must use the DTS provided Remote Access (RA) method. Other remote access services are not authorized for use. Services such as "LOGMEIN", "GOTOMYPC", VNC, and Team Viewer, etc., are not under the control of DTS and thus have less than optimal security and are not permitted to be used in conjunction with Government networked resources.

14. <u>Electronic Communications</u>

Employees provided with Government account(s) are to protect their account information by excluding unnecessary exposure of the Government email address (not to be published in public media, newspapers, social media applications, websites, etc.). The account is for Government business, subject to any limitations outlined in this policy. Electronic communications (e-mail, voice mail, social media, texting, etc.) are subject to the provisions of the Virginia Freedom of Information Act and Virginia Public Records Act and the requirements below:

(1) Respond appropriately to messages and follow proper etiquette when fashioning email correspondence;
(2) Be aware of email security best practices;
(3) Ensure the e-communication is sent to the person/s for which it was intended by confirming that you have the correct contact information. Use the "reply all" feature carefully;
(4) Respond appropriately to Freedom of Information Act (FOIA) requests;
(5) Protect e-communications from unauthorized release to third parties;
(6) Sensitive information should be protected through encryption;
(7) Utilize official Government-issued accounts for communications regarding transaction of Government business.

15. Records Management

(1) Management of electronic Records

All public records created, stored, or received on Government information systems are to be retained in accordance with the provisions of these guidelines and as described in the Virginia Public Records Act (§ 42.1-76 et seq.) and the Library of Virginia (LVA) Records Retention & Disposition Schedule[6].

(2) Retention of electronic communication records

By default, records generated in electronic communication systems are retained as "Correspondence", under LVA Records Retention and Disposition Schedule, General Schedule No. GS-19[7] for localities. Electronic Communication systems include, but are not limited to, e-mail and social media applications.

[6] http://www.lva.virginia.gov/agencies/records/retention.asp
[7] http://www.lva.virginia.gov/agencies/records/sched_local/GS-19.pdf

Electronic Communication systems are not designed to be records management systems. Records other than routine "Correspondence" are not to be stored in electronic communications systems. All Government staff members and contractors are responsible for ensuring that records are retained for the appropriate retention period pursuant to LVA requirements. **It is the responsibility of each staff member to determine if records require longer retention** by reviewing the appropriate LVA Records Retention and Disposition Schedule and moving the record into a Government approved records management system.