

MEMORANDUM

To: BOS IT Committee
From: Scott Varner, IT Director
Subject: BOS IT Committee Agenda and Supporting Information
Date: 4/24/2020

The BOS IT Committee meeting will be held in the First Floor Conference Room at 107 N Kent Street on Wednesday, April 29, 2020, at 8:30 a.m.

Information and Discussion

1. Broadband Expansion
 - a. Establish public Wi-Fi at Fire Stations and Sunnyside Plaza during COVID-19 crisis – **Attachment A**
 - b. Timeline of Actions to Date – **Attachment B**
 - c. Coverage comparison – 2013 vs 2019 – **Attachment C**
 - d. Virginia Telecommunication Initiative Grant (VATI)
 - a) Matrix of Successful Grant Applications (2020) – **Attachment D**
 - b) Strategies for 2021 Grant Process
 - e. Broadband Expansion Next Steps
 - a) Broadband Committee
 1. Makeup of Committee
 - b) RFP for Unserved/Underserved Areas
 - c) Other Broadband Expansion Options
 1. Forming a Broadband Authority
 2. Options for other Franchise Agreements
 3. Allow the market to work it out
 - d) Timeline for Next Steps
2. Information Technology Acceptable Use Policy Revisions – **Attachment E**
 - a. Combining Acceptable Use and Internet Use Policies

b. Sections Added

- a) Email Signatures
- b) Cybersecurity Training
- c) Remote Worker Policy
 - 1. Standard Laptop Kit for members of the Board of Supervisors

Action Items

1. Requesting IT Committee approval for monthly funding of public Wi-Fi during the COVID-19 crisis.
2. Requesting IT Committee approval for staff to create an RFP for soliciting providers to expand broadband in the underserved/unserved areas of Frederick County. The RFP will be used to pursue the 2021 Virginia Telecommunication Initiative (VATI) Grant.
3. Requesting IT Committee approval to form a Broadband Committee to pursue further options for broadband expansion.
4. Requesting IT Committee approval for updates to the Frederick County Information Technology Acceptable Use Policy.

Sincerely,

Scott Varner

Scott Varner
County of Frederick
Director of IT

Attachment A



COUNTY OF FREDERICK

Information Technologies

Scott Varner, Director of Information Technology

svarner@fcva.us

Voice 540.722.8261

MEMO

To: Kris Tierney, County Administrator
From: Scott Varner, Director of Information Technology
Subject: Request for funding public Wi-Fi at Fire Stations and Sunnyside Plaza
Date: April 13, 2020

The Information Technology Department is requesting \$18,804 to cover costs associated with providing public Wi-Fi in the parking lots of County fire stations and the property at Sunnyside Plaza. The funding would cover hardware, installation, and the monthly access fee for data service. The breakdown of costs along with the fire stations that are proposed to be served are below.

During this time of COVID-19 and stay-in-place orders, students and parents are struggling in several parts of our County to provide necessary access for schoolwork and for some parents, their telecommuting needs. Although providing this service does not solve our long-term broadband issues, in my professional opinion this would provide some relief for those individuals that need access, but don't have it or the bandwidth at their home is so low it is not effective.

Deputy Chief Majchrzak spoke to the Fire Chiefs about this project and the only fire station to opt out is Stephens City. Please let me know if you have any questions.

Fire Stations to be Served

- Reynolds Store
- Clear Brook
- Round Hill
- Greenwood
- Star Tannery
- Gainesboro
- North Mountain
- Millwood Station
- Middletown
- Gore

Additional Sites

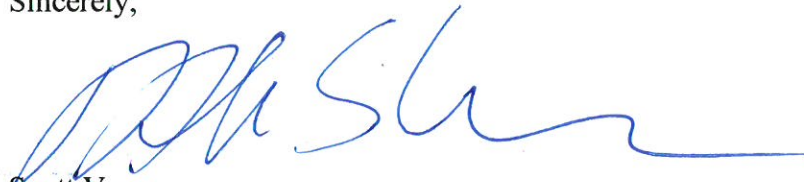
Sunnyside Plaza

Costs

- One-time costs for installation and hardware - \$15,504
- Monthly data costs for all sites - \$3,300

Total - \$18,804

Sincerely,

A handwritten signature in blue ink, appearing to read 'S. Varner', with a long horizontal flourish extending to the right.

Scott Varner
County of Frederick
Director of Information Technology

Attachment B

Frederick County Broadband Timeline



- June 2012 - "Let's Get Connected" Public Meeting
- March 2013 - CIT Project Kick Off
- March/April 2013 - "Kick Off Meeting"
- June 2013 - "Needs Assessment" Public Meeting
- July 2013 - Jan 2014 – VIBEVOIP product demo "Clearbrook Park public Wifi enable"
- Nov 2013 - CIT Project Delivery
- Nov 2013 - "Final Presentation" Public Meeting
- Nov/Dec 2013 – County Website has page added providing info on broadband providers in our area.
- Dec 2013 - Memo to BOS with Executive Summary of Broadband Study
- 2013/2014 - Stoneymeade Dr – Comcast Expansion
- 2015 - VATI Grant - No Providers willing to Participate
- 2015/2016 - Shawneeland – Comcast Expansion
- 2016 – Round Hill/National Lutheran Blvd Expansion
- 2018 - VATI Grant – No Providers willing to Participate
- 2019 - VATI Grant — Partnered with Comcast, was not awarded grant
- On average 10 – 15 Citizen request per year for help primarily with Comcast. Anything from a service request to billing issues.

Attachment C



Frederick County Broadband Gaps

As Identified by CIT in the 2013 Frederick County, VA Broadband Study.





Map Features

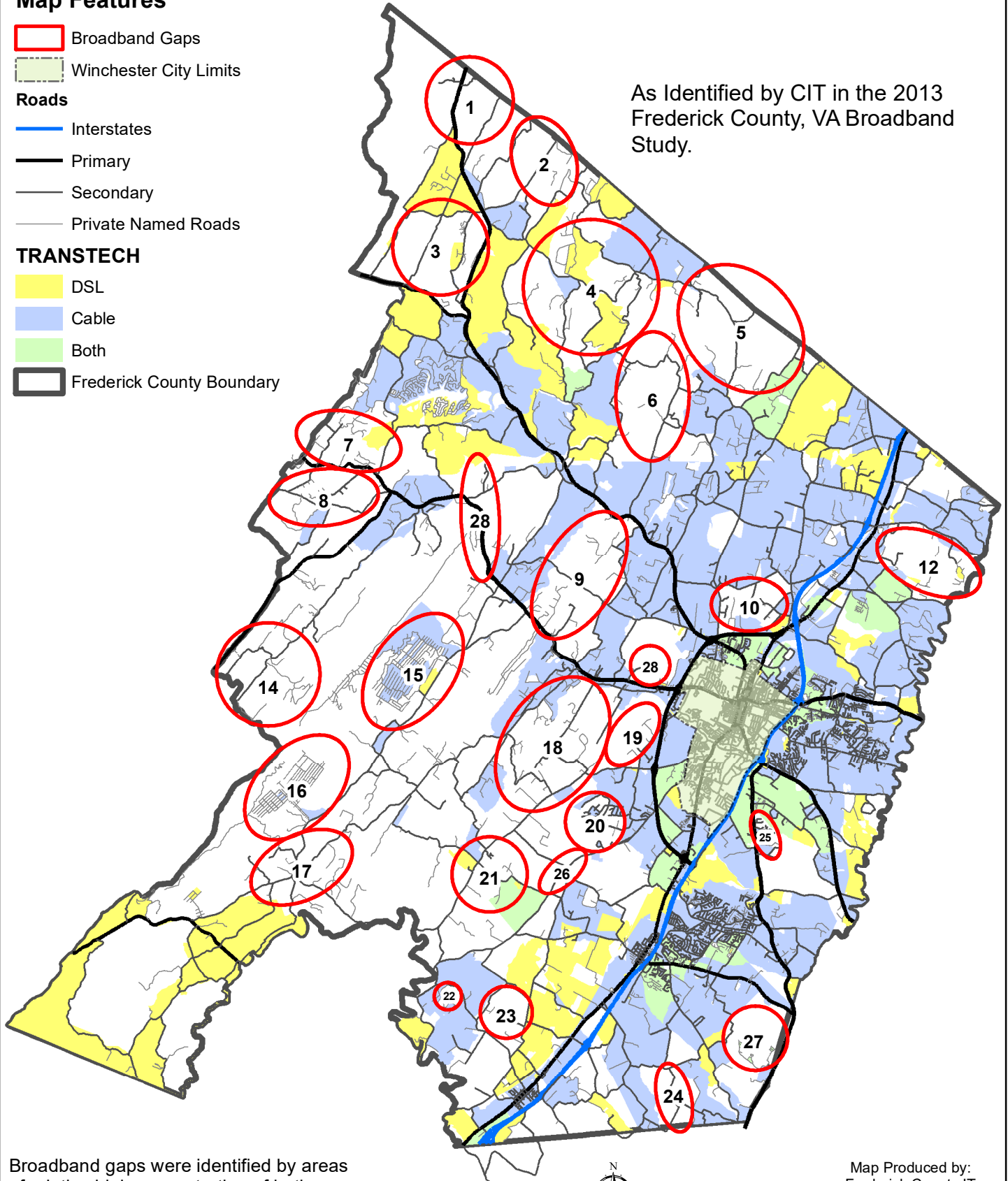
-  Broadband Gaps
-  Winchester City Limits

Roads

-  Interstates
-  Primary
-  Secondary
-  Private Named Roads

TRANSTECH

-  DSL
-  Cable
-  Both
-  Frederick County Boundary








Broadband gaps were identified by areas of relative high concentration of both residential and commercial structures in areas with little to no DSL or Cable coverage as identified by VITA.

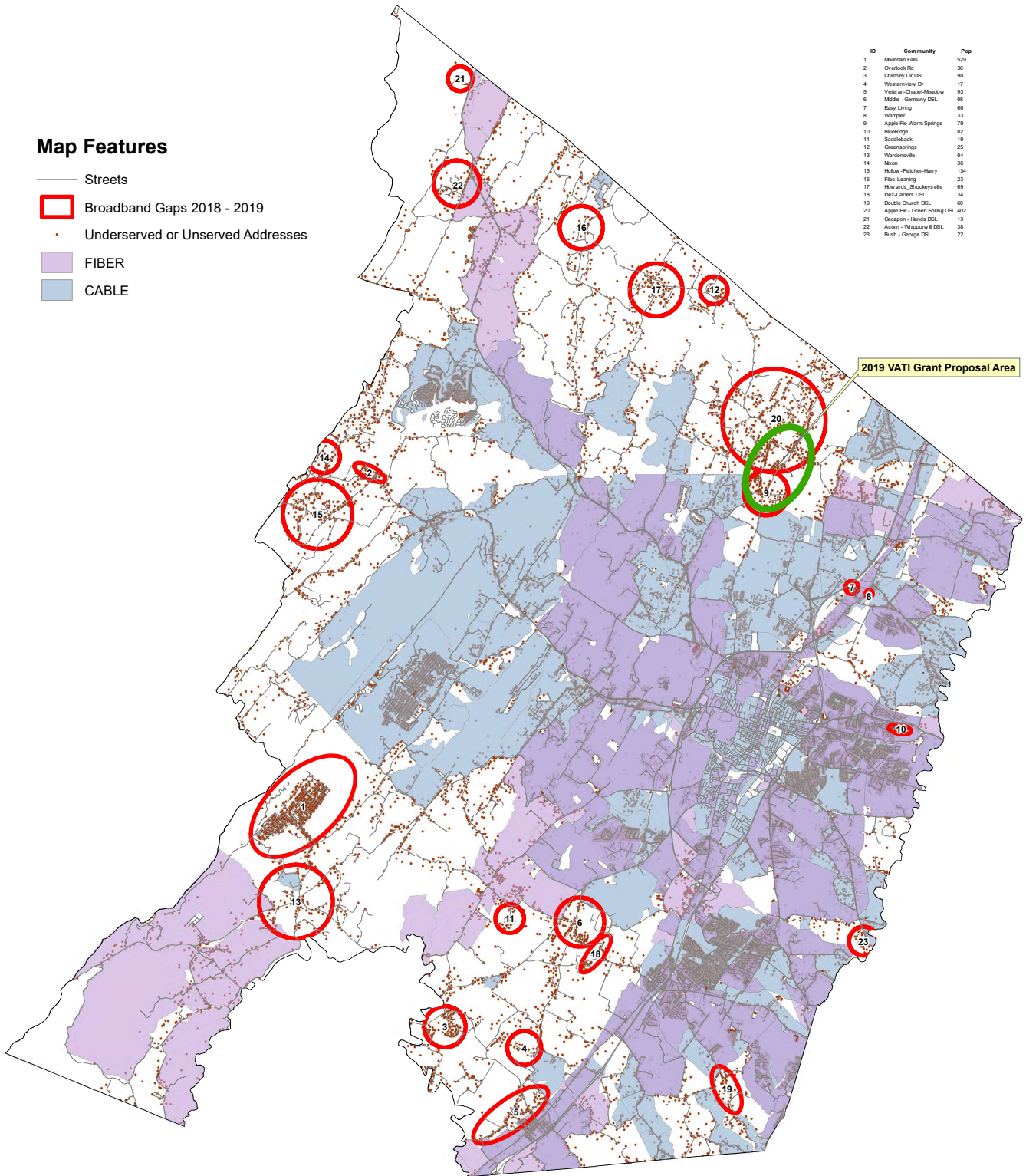
Map Produced by:
Frederick County IT
GIS Division
107 N Kent St
Winchester, VA 22601
Drafted 9/5/2013

Frederick County, VA Broadband Study Map

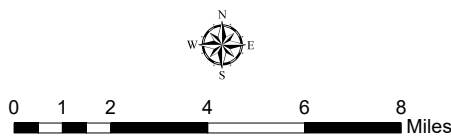
Map Features

-  Streets
-  Broadband Gaps 2018 - 2019
-  Underserved or Unserved Addresses
-  FIBER
-  CABLE

ID	Community	Pop
1	Mountain Falls	529
2	Overlook Rd	36
3	Chimney Cr DSL	90
4	Westernview Dr	17
5	Veteran-Chapel-Meadow	93
6	Midvale - Germany DSL	98
7	Easy Living	66
8	Wangler	33
9	Apple Pie-Warm Springs	79
10	BlueRidge	82
11	Stablesback	19
12	Greensprings	23
13	Wardensville	94
14	Nearm	35
15	Hollow-Fletcher-Harry	134
16	Fires-Leaning	23
17	Howards-Stockleysville	69
18	Hez-Carters DSL	34
19	Double Church DSL	80
20	Apple Pie - Green Spring DSL	422
21	Cacapon - Hands DSL	13
22	Acorn - Whispore B DSL	38
23	Bush - George DSL	22



Broadband gaps for 2018 Telecommunications grant were identified as areas of relatively high populations in rural Frederick County, VA that show little or no broadband coverage based on Virginia Broadband Maps produced by VITA.



Map Produced By:
Frederick County Dept.
of Information Technology
GIS Division.
Drafted 12/03/2018

Attachment D

Virginia VATI Grant 2020 - Breakdown

Locality	Private Provider/Partner	Funding requested	Leverage/Match	Total Project Cost	Grant funds as a % of overall Cost	Local funds as a % of overall cost	Population per Grant Area
Albemarle Broadband Authority	Century Link	\$291,300.00	\$1,650,700.00	\$1,942,000.00	15%	85%	837
Augusta County	MGW Networks	\$722,746.00	\$389,172.00	\$1,111,918.00	65%	35%	
Botetourt County	Lumos	\$2,008,938.56	\$1,106,626.13	\$3,115,564.69	64%	36%	
Brunswick County	Mecklenburg Electric	\$444,259.00	\$366,206.00	\$810,465.00	55%	45%	
Central Shenandoah PDC - Rockbrige/Bath	BARC	\$2,202,000.00	\$15,633,969.00	\$17,835,969.00	12%	88%	1085
Central Shenandoah PDC - Bath/Highland	MGW Networks	\$460,560.00	\$115,140.00	\$575,700.00	80%	20%	
Charles City County	Comcast	\$3,966,012.00	\$1,322,004.00	\$5,288,016.00	75%	25%	2350
City of Chesapeake	Cox	\$532,632.00	\$146,054.00	\$678,686.00	78%	22%	
City of Suffolk	Open Broadband	\$661,610.00	\$634,720.00	\$1,296,330.00	51%	49%	
Franklin County	BRISCNET	\$2,383,039.00	\$2,216,038.00	\$4,599,077.00	52%	48%	600
Frederick County	Comcast	\$997,171.00	\$332,390.00	\$1,329,561.00	75%	25%	313
Louisa County	Acela Net/SCS Broadband	\$104,730.00	\$52,500.00	\$157,230.00	67%	33%	
Culpeper County - DOT COM	Virginia Broadband	\$1,046,246.00	\$282,629.00	\$1,328,875.00	79%	21%	
Cumberland PDC - Davenport	Point Broadband	\$226,560.00	\$528,643.00	\$755,203.00	30%	70%	1026
Cumberland PDC - Bear Pen	Point Broadband	\$785,236.00	\$523,491.00	\$1,308,727.00	60%	40%	
Gloucester County - Wired	Cox	\$369,181.00	\$194,416.00	\$563,597.00	66%	34%	

Gloucester County - Wireless	Open Broadband	\$1,082,217.00	\$1,005,141.00	\$2,087,358.00	52%	48%	
Grayson County	Gigabeam	\$2,087,015.00	\$5,792,698.00	\$7,879,713.00	26%	74%	2648
Greene County	Century Link	\$142,500.00	\$332,500.00	\$475,000.00	30%	70%	
Halifax County	Mecklenburg Electric	\$1,033,398.00	\$2,918,620.00	\$3,952,018.00	26%	74%	866
Hanover County	Comcast	\$1,081,533.00	\$360,511.00	\$1,442,044.00	75%	25%	
IDA of Russell County	iGo	\$1,028,213.00	\$1,955,680.00	\$2,983,893.00	34%	66%	
King and Queen County	Riverstreet	\$6,043,905.00	\$11,217,787.00	\$17,261,692.00	35%	65%	3832
King George County	KGI	\$460,314.00	\$142,046.00	\$602,360.00	76%	24%	
LENIWISCO PDC	Scott County Telephone	\$790,464.00	\$526,976.00	\$1,317,440.00	60%	40%	387
Mecklenburg County	Mecklenburg Electric	\$56,200.00	\$116,061.00	\$172,261.00	33%	67%	
New Kent County	Cox	\$290,386.00	\$103,755.00	\$394,141.00	74%	26%	
Northern Neck PDC	Atlantic Broadband	\$675,114.53	\$648,440.34	\$1,323,554.87	51%	49%	
Orange County - Barboursville	Madison Gigabit	\$1,452,385.00	\$558,434.00	\$2,010,819.00	72%	28%	
Orange County - BLM	Hosted Backbone	\$1,896,140.00	\$770,001.00	\$2,666,141.00	71%	29%	
Page County - PageCo	Century Link	\$952,600.00	\$779,400.00	\$1,732,000.00	55%	45%	
Page County - Overlook	Comcast	\$333,428.00	\$111,143.00	\$444,571.00	75%	25%	
Patrick County	Riverstreet	\$798,283.00	\$540,450.00	\$1,338,733.00	60%	40%	1950
Prince George County	Prince George Electric	\$560,000.00	\$560,000.00	\$1,120,000.00	50%	50%	
Pulaski County	All Points	\$612,475.00	\$410,000.00	\$1,022,475.00	60%	40%	
Spotsylvania County	Data Stream	\$387,222.00	\$245,700.00	\$632,922.00	61%	39%	
Stafford County	KGI	\$874,478.00	\$405,177.52	\$1,279,655.52	68%	32%	727

Surry County	Prince George Electric	\$2,225,000.00	\$2,225,000.00	\$4,450,000.00	50%	50%	1253
Washington County	Point Broadband	\$1,574,139.00	\$1,093,893.00	\$2,668,032.00	59%	41%	

	Awarded Grant
	Not Awarded

Attachment E

Document Title: **Electronic Communications and Internet Services Policy**

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. Efficient 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 the Government’s computer networks and data assets against unauthorized and malicious use as well as to prevent potential misuse of Government resources.

¹ As used in this document, (i) “Government” means County of Frederick, Virginia,, (ii) “Director” means Director of Information Technology or his/her designee, (iii) “Department of Information Technology” or “DIT” refers to the department that manages the Information and Communication Technology, (iv) “CDFIS” means the Chief Deputy for Security 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 Director of Information Technology has managerial responsibility for the technology initiatives contained in this regulation. The Director is responsible for reviewing and approving any exceptions to this policy.

The Department of Information Technology (DIT) is responsible for providing, administering, and ensuring 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 DIT 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 County Records Retention Officer.

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 Deputy for Security (CDFS) 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 CDFS. 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 CDFS 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 Act⁴;
- (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 the Government, employees are representing the Government and should always conduct themselves as Government representatives. 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 DIT;
- (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 2.2-2827⁵;
 - (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 DIT;
 - (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 CDFS;
- (25) The use of or installation of routers, hubs, switches, wireless access points, Internet of Things (IoT) devices, etc., without authorization from DIT;
- (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. DIT is responsible for the installation of virus protection software on County owned PCs. In the event updates do not occur successfully, users must contact the DIT HELP DESK to open a trouble ticket so that the updating process can be re-established. Any virus detected must be reported to the DIT 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 DIT. DIT 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 DIT. Every "device" or "host" connecting to the Internet must have a unique identifier assigned by DIT.

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 DIT 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 DIT 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 DIT (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 DIT information governance requirements as defined by the CDFS 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 DIT.

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

- 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 DIT 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 FTPserver.
- (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 DIT 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 DIT and thus have less than optimal security and are not permitted to be used in conjunction with Government networked resources.

14. Electronic Communications

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 Schedule⁶.

- (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-19⁷ 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.

Document Title:	Remote Access Policy and Acceptable Use Agreement ¹
Document Type:	<u>Policy / Employee Agreement</u>
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:	<p>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.</p> <p>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).</p>

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 As used in this document, (i) “Government” means County of Frederick, Virginia,, (ii) “Director” means Director of Information Technology or his/her designee, (iii) “Department of Information Technology” or “DIT” refers to the department that manages the Information and Communication Technology, (iv) “CDFIS” means the Chief Deputy for Security 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, Frederick County is responsible for providing Government equipment (i.e., workstation, laptop, router, and IP telephone), additional software and licensing fees (such as Cisco AnyConnect, Cisco Jabber 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, users are required to use VPN client software, which will be provided by DIT, 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).

DIT 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.
- (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 Information Technology(DIT).
- (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. DIT 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

DIT 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.

DIT 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 DIT 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): _____

Document Title: **Mobile Device Acceptable Use and Management Policy^{1 2}**

Document Type: Policy

Document Purpose: This document establishes the Government technology policy for the use of Government-issued or personal Mobile Devices that access Government servers, data resources, email systems, software and technology infrastructure (“Government systems”) or to process or store Government data and information when conducting Government business (“government data”). All users of the Government’s technology will ensure the confidentiality, integrity and availability of data provided to, and generated by, Government agencies. This policy exists to prevent data from being deliberately or inadvertently stored or accessed on a mobile device without appropriate security measures; transported over network where the Government data it is at risk and to govern Government issued or owned mobile devices (defined below).

Scope of Application: This policy applies to all Government Mobile Device users, including employees, authorized contractors, consultants, constitutional employees and temporary employees (“Users”).

1. Definition(s)

“Mobile Device” or “Mobile Devices” in this policy refers to all Government-issued mobile devices and personal mobile devices used for Government business. Examples of Mobile Devices include, but are not limited to, smartphones, tablets, notebooks, laptops, Air Cards, netbooks, iPhones and iPads.

¹ As used in this document, (i) “Government” means County of Frederick, Virginia,, (ii) “Director” means Director of Information Technology or his/her designee, (iii) “Department of Information Technology” or “DIT” refers to the department that manages the Information and Communication Technology, (iv) “CDFFS” means the Chief Deputy for Security 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. Issuance and Ownership

- (1) A Government-issued Mobile Device may be provided to Users based upon business need and as approved by the department director where the User is assigned.
- (2) The purchase and provision of Mobile Devices, accessories and/or services are handled through a Government-wide contract and otherwise must follow Government procurement processes, including prior approval by the appropriate Government personnel. Any exceptions to the Government's standard service and device offerings must be pre-approved in writing by the Chief Information Officer or designee.
- (3) Each member of the Frederick County Board of Supervisors will be issued a laptop to conduct Government related business and as such will be subject to all applicable electronic policies. The Department of Information Technology will be responsible for securing, updating, and providing technical assistance for the County issued laptops.
- (4) Based upon business need, and with department director approval, Users may use personally owned Mobile Devices to access Government systems, to sync email, calendar and contacts etc. Employees using personal devices for Government business are subject to the same usage, security and records management requirements as employees using Government-issued devices.
- (5) All Users provided a Government-issued Mobile Device or who use a personal Mobile Device for Government business must comply with the requirements set forth in this policy as well as other related regulations, i.e. *Electronic Communications and Internet Services*³.
- (6) Government-issued Mobile Devices are the property of the Government. All government data stored on a Mobile Device remains the property of the Government and must be handled appropriately.
- (7) The physical integrity and security of the Mobile Device is the responsibility of the User to whom the Mobile Device has been assigned or in the owner of a personal Mobile Device.
 - a. All Mobile Devices used for Government business must be registered with DIT Help Desk support.
 - b. Mobile Devices should be kept in the User's physical presence whenever possible and shall be stored in a secure location at all times (car seats or unlocked glove compartments are not secure storage areas) and away from environment hazards such as heat, water, and chemicals.
 - c. The Mobile Device must be protected from unauthorized access and have encryption features activated.
 - d. Installation of Mobile Device Management (MDM) software will be required on Government-issued and personal Mobile Devices before access to Government systems will be permitted.
 - e. GPS feature full-time activation is required to assist in locating lost or stolen Mobile Devices.
- (8) If a Mobile Device is lost or stolen, the incident must be reported to the Help Desk call center as soon as possible, but no later than 24 hours after the loss or theft is discovered. Mobile

Device access to Government systems will then be denied and the government data stored in the Mobile Device will be deleted (via remote wipe) within 24 hours after the incident is reported.

- (9) Users should understand that there is no expectation of privacy in the use or content stored on a Government-issued Mobile Device or any reports generated by the use of a Government-issued Mobile Device, such as a billing statement or charge back statement issued to a department. Such information or data may be collected or reviewed following appropriate Government procedures and may be subject to the provisions of the Virginia Freedom of Information Act (FOIA)⁴. Users of personal Mobile Devices do so at their own risk.

3. Mobile Device Use Requirements and Support

All Users of authorized Mobile Devices agree to the terms and conditions of this use policy each time they gain access to Government systems at login or use a Government-issued Mobile Device. DIT Help Desk Support staff will assist employees authorized to sync a Mobile Device, with initial set-up of the sync feature. DIT will ensure encryption is activated on the Mobile device. Additionally, DIT will, at a minimum, apply the following criteria to the Mobile Device:

- (1) Enabled password protection
- (2) Retention of e-mails will be set for a maximum of 15 days
- (3) Device lock-out after 10 failed login attempts
- (4) Auto log-out after 5 minutes of inactivity
- (5) GPS activation for lost and stolen recovery purposes.

4. User Responsibilities

All Users must adhere to the following requirements:

- (1) Set a password to access the Mobile Device. Do not share the password except with authorized Government personnel;
- (2) Immediately report a lost or stolen Mobile Device, or compromised password, to the DIT Help Desk;
- (3) Provide full cooperation and support to DIT Help Desk personnel if a remote-wipe of a Mobile Device's content is required;
- (4) Take proper care of a Government-issued Mobile Device to protect it against damage, loss and voiding of any applicable warranties;
- (5) Comply with the Government's Acceptable Use and Driver Safety policies when conducting Government business while using a Mobile Device;
- (6) Compliance with any Litigation Hold for any government data stored on the Mobile Device

⁴ <https://law.lis.virginia.gov/vacodepopularnames/virginia-freedom-of-information-act/>

- (7) All Government-issued Mobile Devices must be promptly surrendered when requested by appropriate Government personnel and/or upon separation, resignation or retirement from Government service;
- (8) All government data must be removed from a personal Mobile Device, with the assistance of DIT, upon separation, resignation or retirement from Government service or completion of a Government contract, as applicable;
- (9) As appropriate, refrain from storing confidential or protected government data on the device and comply with any applicable confidentiality or privacy rules related to government data;
- (10) Failure to comply with any of the requirements of this policy or the preventable loss or destruction of a Mobile Device may result in disciplinary action;

Users are also prohibited from:

- (11) Downloading, fee-based 'service' that will be charged to the Government without prior department authorization. Services include, but are not limited to Internet, ringtones, music, videos and premium texting;
- (12) Downloading any application or service, or modifying the operating system of a Mobile Device which would bypass Government-installed or required security measures;
- (13) Downloading any application or service, or modifying the operating system of a Mobile Device in a manner that bypasses or circumvents the Government records retention requirements pursuant to the Virginia Public Records Act, Library of Virginia records retention schedules and guidelines⁵;
- (14) Violating the Government's Acceptable Use policy and other department policies or Government administrative regulations;
- (15) Using the camera feature on a Government-issued Mobile Device in any restroom, locker room, Government medical facility or other area considered by the general public to be private;
- (16) Non-exempt employees are prohibited from accessing Government systems outside of their assigned work hours unless pre-approved in writing by authorized department personnel.

5. Departmental Responsibilities

Users must be approved prior to enrollment - Each user is limited to a maximum of 'two' mobile devices. The department director may increase the number of managed devices on a case by case basis. The On-Base Wireless Provisioning process will support enrollment of devices. BYOD devices that are damaged, lost or stolen will not be replaced by the Government.

⁵ <http://www.lva.virginia.gov/agencies/records/retention.asp>

Costs associated with initial purchase and monthly charges for a Government-issued Mobile Device are the responsibility of each individual department and subject to a Government-wide contract. Departments are responsible for employee accounts where spending for-fee-based services (e.g. 411, International Calls and texting in excess of employee’s monthly plan) are determined to be excessive.

The department will notify DIT at least 30 days in advance that a Mobile Device is being re-assigned to another employee. If the notification is not received or received after 30 days, the service for the Mobile Device may be terminated.

Each department may adopt department specific policies to supplement this policy and/or to ensure enforcement of this policy. Managers and supervisors are responsible for ensuring that Users of Mobile Devices are aware of and comply with this policy.

In the event a Mobile Device/s or service was previously purchased outside of the Government-wide contract, departments are responsible for promptly transitioning those Mobile Device/s and service contract(s) to the Government-wide contract and notifying the Help Desk to register the Mobile Device/s.