Bedford County Tennessee

Acceptable Use Policy for Electronic Equipment & Media

Date: 12.05.11

Ver. 3.30 (9/3/14)

Draft by: Chris White

Policy Number: __________
1.0 Overview

Bedford County Government’s intentions for publishing an Acceptable Use Policy For Electronic Equipment & Media is not to impose restrictions that are contrary to Bedford County’s established culture of openness, trust and integrity. Instead, Bedford County Government is committed to protecting our employees and our citizens from illegal or damaging actions by individuals, either knowingly or unknowingly.

To remain efficient, better serve the citizens of Bedford County and provide our employees with the best tools to do their jobs, Bedford County Government makes available to our workforce access to one or more forms of electronic media and services, including computers, e-mail, telephones, cellular telephones, voicemail, fax machines, external electronic bulletin boards, video-conferencing/telephony equipment, wire services, online services, intranet, Internet and the World Wide Web.

Bedford County Government encourages the use of these media and associated services. They can make communication, record keeping, and problem solving more efficient and effective because they are the conduit for valuable sources of information about vendors, property, law, policies, technologies, and new products and services. All employees and everyone connected with the organization should remember that electronic equipment, media and services provided by Bedford County Government are government property and their purpose is to facilitate and support official government business. All computer users have the responsibility to use these resources in a professional, ethical and lawful manner.

Effective security is a team effort involving the participation and support of every Bedford County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer or electronic equipment user to know these guidelines and to conduct their activities accordingly.

Internet/Intranet/Extranet-related systems, including, but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing and FTP, are the property of Bedford County Government. These systems are to be used for the business of county government in serving the interests of the citizens of Bedford County, customers of Bedford County Government services and private business vendors that provide services to Bedford County Government in the course of normal operations. To ensure that all employees are responsible, the following guidelines have been established for using e-mail, the Internet and other electronic devices provided to employees as a necessary work tool. No policy can lay down rules to cover every possible situation. Instead, it is designed to express Bedford County Governments’ philosophy and set forth general principles when using electronic media and services.
The following policies are considered to be a minimum standard for all departments. Any department head who chooses to increase these standards in any way, especially involving the maintenance of sensitive or private records or involved in critical infrastructure, is welcome to do so by providing the Mayor’s office with copies of the adopted provisions.

2.0 Purpose

Inappropriate use of these systems unnecessarily exposes Bedford County Government to certain risks including virus attacks, a compromise of network systems and services, legal issues and economic losses. This policy will serve to mitigate those risks.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries and other workers in Bedford County Government. These rules are in place to protect the employee and Bedford County Government. Inappropriate computer use exposes Bedford County Government to risks including virus attacks, a compromise of network systems and services and legal issues. Departments not using Voice or Data service provided by the Bedford County IT Department should have their own policies, procedures and equipment necessary to protect their network, equipment, information and data (i.e. Network Firewall).
4.0 Policy

4.1 GENERAL USE AND OWNERSHIP

While Bedford County's network administration (IT Dept.) desires to provide a reasonable level of privacy, users should understand that the data they create on the county network remains the property of Bedford County Government. Because of the need to protect Bedford County’s network, management cannot guarantee the confidentiality of information stored on any network or non-network electronic device belonging to Bedford County.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating specific guidelines concerning personal use of Internet/Intranet/Extranet systems for their departments that would be more restrictive than the policies stated in this document. In the absence of such policies, employees should be guided by the county’s policy on personal use, and if there is any uncertainty, employees should consult their supervisor or director.

For security and network maintenance purposes, authorized individuals within Bedford County Government may monitor equipment, systems and network traffic at any time.

Bedford County Government reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 SECURITY AND PROPRIETARY INFORMATION

The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential, or not confidential. Examples of confidential information include but are not limited to: personnel records, research data and court records that include child adoption information. Employees should take all necessary steps to prevent unauthorized access to this information.
Password Policy

Objective

The objective of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. The scope of this policy includes all personnel who have, or are responsible for any form of access that supports or requires a password on any system that resides on resources owned by Bedford County Government, or resources acquired from customers or third-party suppliers of this government entity.

Controls and Procedures

1. Passwords must be changed on a regular and consistent basis as defined herein:

   a. All system-level passwords (e.g., root, enable, Server/OS admin, application administration accounts, accounts tied to financial accounts of Bedford County Government, etc.) must be changed on a minimum of a quarterly basis.

   b. All user-level passwords (e.g., email web, desktop computer, etc.) must be changed a minimum of a quarterly basis.

   c. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user to include personal passwords used by that user for access to personal, non-work or business related accounts.

   d. Passwords must not be inserted into email, text, SLS, or any other messages type or other form of electronic communications.

   e. All user-level and system-level passwords must conform to the following characteristics:
      • Contain both upper and lower case characters (e.g., a-z, A-Z)
      • Have digits and punctuation characters as well as letters (e.g., 0-9, @#$%^&*()_=+|{}[]:;"'<>/)
      • At least fifteen alphanumeric characters long and is a passphrase.
      • Not words in any language, slang, dialect, jargon, etc.
      • Not based on personal information, names of family, pets, etc.

   f. Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase.

   g. Do not use the same password for work and non-work access such as a personal ISP account, banking and utility or shopping accounts.

   h. Do not share work passwords with anyone. To reinforce this statement, do not share any password with administrative assistants or secretaries, supervisory level persons, or family members.
i. You are responsible for the protection of Bedford County Government owned sensitive information and may be legally responsible for the protection of such information as well as any similarly owned intellectual property.

2. Monitoring / Controls

   a. All systems should be set by either the I.T. Department Staff or Supervisors to alert the users of password changes every 90 days in order to remove any possibility that passwords are not routinely changed. If you do not know if your system has been set in such a way, please check with the I.T. Department.

   b. The I.T. Department and the State Comptrollers’ Office of I.T. Auditing (Fee collecting/managing offices only) will periodically monitor password usage, including all change activity.

   c. The I.T. Department will periodically scan all mail and messages for unauthorized usages. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination or employment.

Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. While a more frequent change of passwords creates a higher level of security, it is far more important that employees remember their passwords rather than write them down. Employees are allowed to make up their own passwords as long as they follow these minimum standards.

Additionally, each workstation should be set in such a way that their MS Windows® passwords automatically expire every 90 days. Concurrent to changing the MS Windows password, workstations with access to a departments’ proprietary accounting software (i.e., Local Government Corporation or Business Information Systems), must also change those passwords on the same schedule.

All PC’s, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off or by pressing the “windows” key simultaneous with the “L” key upon leaving their workstations unattended. This will immediately bring their system to the password screen and thereby keep unauthorized persons from using an employee’s system.

All hosts used by the employee that are connected to the Bedford County Government Internet/Intranet/Extranet, whether owned by the employee or Bedford County Government, shall be continually executing approved virus-scanning software with a current virus database unless overridden by a departmental policy. If any employee receives a screen warning that their anti-virus software is in a state of near expiration, contact the I.T. Department immediately for an update/renewal of their anti-virus software.
Employees must use extreme caution when opening e-mail attachments received from unknown or out-of-network senders. These emails may contain viruses, e-mail bombs or Trojan horse code. Employees who receive a personal email that contains an attachment should only open such an email on their personally owned computers or smart phones. If, during the course of your employment, an unknown or suspicious email attachment sent for business purposes should require downloading or opening, employees should save the attachment to a flash drive/thumb drive or other removable media and scan the file with their virus software before the file is opened.

All computers, computer related equipment, smart phones, software, individual components and peripherals, systems, telecommunication services or equipment purchased, regardless of the funding source, or donated for use in any Bedford County Government department must be approved by the Director of IT or his/her designee.

All telephones, cabling, systems, network and telephone lines donated or purchased, regardless of the funding source, must be approved by the Director of IT or his/her designee.

All workstations should be manually shut down at the end of every work shift. To accomplish this, all users SHALL do this as follows: Left mouse click on the Start icon/menu. Left click on the Shut Down icon.

4.3 PROHIBITED USES & COMMUNICATIONS

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting services). Under no circumstances is an employee of Bedford County Government authorized to engage in any activity that is illegal under State, local, Federal or international law while utilizing Bedford County Government-owned resources. The lists below are by no means exhaustive, but they do attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

1. Violations of the rights of any person or company protected by copyright, trade secrets, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Bedford County Government.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Bedford County Government or the end user does not have an active license is strictly prohibited.

3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4. Making fraudulent offers of products, items or services originating from any Bedford County Government account.

5. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service and forged routing information for malicious purposes.

6. Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.

7. Circumventing user authentication or security of any host, network or account.

8. To prevent computer viruses from being transmitted through the company’s computer system, unauthorized downloading of any unauthorized software is strictly prohibited. Including, but not limited to instant message, games and remote control programs. Only software registered and/or approved through Bedford County I.T. Department may be downloaded. Employees should contact the IT Department if they have any questions.

**Email and Communication Activities**

Electronic media/devices cannot be used for knowingly transmitting, recording, retrieving or storing any of the following type of communications:

1. Discriminatory or harassing;

2. Derogatory to any individual or group;

3. Obscene, sexually explicit or pornographic;
4. Defamatory or threatening;
5. In violation of any license governing the use of software;
6. Engaged in for any purpose that is illegal or contrary to Bedford County Government policy or business interests; or
7. Designed to embarrass, coerce, intimidate, defame or threaten any individual for any reason; or
8. Knowingly do harm to computer and electronic hardware or software;
9. Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam);
10. Any form of harassment via email, telephone or paging, whether through language, frequency or size of messages;
11. Unauthorized use or forging of email header information;
12. Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies;
13. Creating or forwarding “chain letters”, “Ponzi” or other “pyramid” schemes of any type;
14. The posting of non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam);
15. E-mail shall not be used to circumvent requirements of the Open Meetings Act.

4.4 BLOGGING/Social Networking

Limited and occasional use of Bedford County Government systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Bedford County Government policies, is not detrimental to Bedford County’s best interests and does not interfere with an employee’s regular work duties. Employees may also not attribute personal statements, opinions or beliefs to Bedford County Government when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Bedford County Government. Employees assume any and all risks associated with blogging.

Social networking sites (i.e., Facebook, Twitter, etc.) may NOT be accessed using systems owned or provided by Bedford County Government. Limited and occasional use of personally owned smart phones or iPad’s or similarly capable and portable devices during an employee’s
lunch break or other break to access such a site is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Bedford County Government policies, is not detrimental to Bedford County’s best interest and does not interfere with an employee’s regular work duties.

**Newsgroups**

Postings by employees from a Bedford County Government email address to news-groups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Bedford County Government, unless posting is in the course of their business duties.

**Social Networking**

Bedford County Government recognizes that social networking is a valuable component of shared media and offers a platform for mass collaboration. However, social networking provides no inherent guarantee of privacy or limited distribution of original posted content. Once posted, inaccurate or inappropriate information may not be retractable or removable from the internet sites to which the information is distributed.

More importantly, social networking does not define clear lines between that which is personal and that which is business related. As a result, social networking sites have contributed to the collapse of boundaries between professional lives and personal lives. Employees must be cognizant of this when posting to social networking sites and careful not to post any information which might be business related.

**Controls**

Only authorized employees may post to any electronic media regarding the business of Bedford County Government, and then only when such posts have been reviewed and approved by management. All such posts must be treated as potentially sensitive and confidential, and therefore, multiple levels of review and approval may be required.

The blogging and social networking guidelines below are meant to clarify and define employee responsibilities when using social networking and are intended to help preserve the reputation of Bedford County Government, its employees, and those persons that our government does business with.
Procedures

1. No employee is authorized to post any sensitive, confidential, proprietary, or financial information about Bedford County Government, its members or employees. Employees are prohibited from disclosing any confidential, proprietary, or otherwise sensitive business or personal information pertaining Bedford County Government in any personal blog or on other social sites.

2. Unless specifically authorized, employees may not represent themselves in any way as representing Bedford County Government. If you identify yourself as an employee of Bedford County Government, you must make it very clear within all postings that you are doing so on your own behalf and not on the company’s behalf.

3. Bedford County Government strongly suggests, due to the sensitive nature of some elements of our business, that you not declare your place of employment publicly in any post. Such posts may become general knowledge and available to those who could potentially put an employee in danger.

4. If you do identify yourself as a Bedford County Government employee, please ensure that content within your profile and related information is consistent with how you and Bedford County Government wish to represent yourself. This includes what you write about yourself and that the types of photos you publish are consistent with the image that Bedford County Government should present to the community.

5. No employee may misrepresent themselves in social networking conversations and should not respond to any negative post on behalf of Bedford County Government, unless they are specifically authorized to do so.

6. Employees may not use any social internet sites, to include personal websites, to harass, bully, or intimidate others. Behaviors that constitute harassment and bullying include, but are not limited to, comments that are derogatory with respect to race, religion, gender, gender variance, sexual orientation, color or disability; sexually suggestive, humiliating, or demeaning comments; and threats to stalk, haze, or physically injure another employee, members or vendors. Individuals may be held personally liable for defamatory, proprietary, discriminatory, harassing or libelous commentary.

7. Employees are strongly urged to report any violations or perceived violations to supervisors, managers or the HR department. Violations include discussions of Bedford County Government, its employees and members, any discussion of proprietary information and any unlawful activity related to blogging or social networking. Should an employee discover negative comments or posts regarding
Bedford County Government, its members or employees, these should be reported to the appropriate department/official for appropriate action by an authorized by an authorized employee.

**Monitoring**

Bedford County Government investigates and responds to all reports of violations of the social networking policy and other related policies. Violation of this social networking policy will result in disciplinary action, up to and including immediate termination. Further, depending on the nature of the offense, Bedford County Government reserves the right to take legal action against employees who engage in prohibited or unlawful conduct.

**4.5 CELLULAR TELEPHONES**

Cellular phones shall be provided to a limited number of employees when essential to the operation of Bedford County Government. Whenever possible, other methods of a more economical or immediate nature shall be considered. The assignment of cellular telephones shall be approved by each department head.

Cellular telephones provided to employees are for official business only and shall not be used for personal purposes except in cases of emergencies. If an employee’s monthly cellular phone bill reflects charges greater than the customary minimum monthly bill, the excess portion of that bill shall become the responsibility of the employee to whom the cellular telephone has been issued. If the employee wishes to dispute the portion of the monthly bill for which s/he is responsible, the employee may request, at his/her own expense, a copy of the detailed billing for telephone use during the disputed period of time and present it to the department head with an explanation of said use. If no resolution can be made with the department head, final determination shall be made by the Director of Finance.

With regard to smart phones, employees who utilize personally owned smart phones in the course of their employment, whether for personal or work-related activity, are subject to all restrictions and use limitations of this policy while their device is connected to or is utilizing Bedford County wireless broadband resources.

**4.6 USE OF ELECTRONIC MAIL (E-MAIL)**

Electronic mail capability among Bedford County Government employees exists for the purpose of enhancing communications stored, created, saved or transmitted on County Government computers/devices and to better perform the tasks associated with the employees’ positions and assignments. Therefore, all employees whom have access to their
department’s network or any Bedford County Government network shall strictly adhere to the following guidelines when sending or receiving messages or files via the internet/intranet/extranet or system wide-electronic mail servers.

Because all computer hardware and software utilized by the employee during the normal course of their official duties belong to Bedford County Government, all data, including email communications, stored, created, saved or transmitted on said computers shall be subject to being monitored. Employees have no right or expectation of privacy with regard to such data. Confidentiality of e-mail communication cannot be assured. E-mail correspondence may be a public record under the public records law and may be subject to public inspection.

Messages shall substantially pertain to legitimate County Government business; e-mail shall not be used to circumvent the requirements of the Open Meetings Act.

Employees will be asked to sign an application stating the Terms and Conditions for Use of the Internet and e-mail. Employees shall not reveal their passwords to others inside or outside of the network. If anyone has reason to believe that a password has been lost, stolen, compromised or accessed by someone without authorization, s/he shall contact the Director of IT immediately.

It is the responsibility of the sender of email to respect any copyright laws that would apply to the message sent.

Messages shall not be sent that contain material that may be defined by a reasonable person as obscene, racist, sexist, offensive, and exploitive or that which promote illegal or unethical activity.

5.0 Enforcement

5.0 Enforcement

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

The computers, electronic media and services provided by Bedford County Government have been provided to employees specifically for business use to assist employees in the performance of their jobs. **Limited, occasional,** or **incidental** use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes or interfere in any way with the effectiveness or efficiency of the employee in the normal course of county business or the efficiency of the network itself. Employees are expected to demonstrate a sense of responsibility and not abuse this privilege. However, the use of or browsing on internet dating sites or other inappropriate media sites is completely prohibited on any Bedford County Government system or asset. The downloading of any games or pornography onto a Bedford County Government system is strictly prohibited. The online sale or purchase of personal items through Ebay, Etsy, or any similarly designed web site is also strictly prohibited.

6.1 ACCESS TO EMPLOYEE COMMUNICATIONS

Generally, electronic information created and/or communicated by an employee using email, word processing, utility programs, spreadsheets, voicemail, telephones, Internet and bulletin board system access and similar electronic media is not reviewed by the Bedford County Government; however, the following conditions should be noted: Bedford County Government does routinely gather logs for most electronic activities or monitor employee communications directly (e.g., telephone numbers dialed (toll records), sites accessed, client IP address leases, call length and time at which calls are made, and general internet traffic) for the following purposes:

1. Cost analysis;
2. Resource allocation;
3. Optimum technical management of information resources;
4. Detecting patterns of use that indicate employees are violating company policies or engaging in illegal activity; and
5. Other training purposes.

Bedford County Government reserves the right, at its discretion, to review any employee’s electronic files and messages to the extent necessary to ensure electronic media and services are being used in compliance with the law, this policy and other company policies. Employees should not assume electronic communications are completely private. Accordingly, if they have sensitive information to transmit, they should use other means.
7.0 Security / Appropriate Use

Employees must respect the confidentiality of other individuals’ electronic communications. Except in cases in which explicit authorization has been granted by management, employees are prohibited from engaging in or attempting to engage in:

1. Monitoring or intercepting the files, telephone calls or electronic communications of other employees or third parties;
2. Hacking or obtaining access to systems or accounts they are not authorized to use;
3. Using other people's log-ins or passwords; and
4. Breaching, testing or monitoring computer or network security measures.
   a. No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.
   b. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system.
   c. Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

8.0 Backup Procedures

Employees shall routinely backup their computer systems to ensure that no substantial loss of data occur should their system fail as a result of power outage, flood or natural disaster or equipment failure. This is especially important for system servers. While each employee's workstation should be backed up at least once per week, servers should be backed up in the following manner.

8.1 DAILY BACKUP
Systems should be backed up once daily, preferably at the end of each working day. A log should be maintained that describes the system being backed up, the type of backup, the date and time of the backup and signed by the person backing up the system. Daily backups can be made to some form of reliable removable media or external drive. If backups are made to
tapes or other removable media, that media object should be prominently labeled with the weekday written directly on the media and stored in a secure fire-proof box, safe or cabinet.

8.2 **WEEKLY BACKUP**
At the close of each work week, a weekly backup shall be made. At least one copy of each weekly backup shall be maintained off site at a secure location. If removable media such as a tape drive backup is made, then one copy shall be maintained on-site and one copy shall be maintained in an off-site location. The backup log shall be maintained as explained above (8.1) and, in addition to the above described information; the location of the weekly backup shall be named. Weekly backups can be sent electronically to an offsite secure server.

8.3 **YEARLY BACKUP**
At the end of each fiscal year, a year-end backup is performed and stored in a secure off site location or offsite secure server.

8.4 **SYSTEM BACKUP**
A system backup is performed and stored whenever the department head or Finance Director deems it necessary. All backups not stored offsite shall be stored in a secure fireproof safe or locking file cabinet.

---

9.0 **Encryption**

Employees can use encryption software supplied to them by the IT Department for purposes of safeguarding sensitive or confidential business information. Those employees that require such measures are required to provide their supervisor with a sealed hard copy record (to be retained in a secure location) and of all of the passwords and/or encryption keys necessary to access the files.
10.0 Maintenance

Problems that occur with hardware or software are reported to the Information Technology (I.T.) Department:

Information Technology
200 Dover Street, Suite 101
Shelbyville, TN 37160
(931) 488-3060
(Server Room ext. 2131)

Some problems will be directly handled by the I.T. Department while other issues may have to be dealt with by Local Government Data Processing Corp., Business Information Systems or others dependent upon the problem encountered. The I.T. technician will advise the employee or department head when problems occur that have to be forwarded to other responsible parties and assist the department in contacting the appropriate responsible party if necessary. The I.T. technician will also advise the department head if the situation requires the acquisition of new hardware or software updates including anti-virus updates.

11.0 Disposition of Surplus Computer Workstations

11.0 Disposition of Surplus Computer Workstations

All “county owned” computer workstations and servers that are replaced and no longer in service are to be turned over to the I.T. Department for proper disposal. Hard drives will be removed by the IT Department and properly disposed of pursuant to Bedford County Tennessee Digital Media and Hardware Disposal Policy. The remaining system parts will be sold as surplus property. All such equipment shall be turned over to the Mayor’s office for surplus disposal.
12.0 Violations

Any employee who abuses the privilege of their access to county-owned or provided computer equipment, e-mail or the Internet in violation of this policy will be subject to corrective action, including possible termination of employment, legal action and criminal liability.

13.0 Definitions

1. Backup – A copy of a file, directory or series of files and directories made to or on a separate storage device in case the original is accidently damaged or erased.
2. Backup Log – A written log made of each backup made to a server or desktop computer indicating the date, the scope of the backup (i.e. drives, directories, files), who made the backup and where the copy is stored.
3. Blogging – Online personal journaling with reflections, comments, concerns and ideas of the writers, the contents derived from personal thoughts and opinions about popular or important social forums.
4. Data Breaching – An incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information, personally identifiable and biographical information, trade secrets or intellectual property.
5. DeGaussing – Demagnetizing magnetic storage media such as tapes or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.
6. Digitization – Conversion of analog information in any form (text, photographs, voice, etc.) to digital form with suitable electronic devices.
7. Disintegration – A physically destructive method of sanitizing data; the act of separating into component parts.
8. Email Bombs – A type of technological attack, where the purpose is to overwhelm and shut down a mailbox or an entire e-mail server.
9. **Email Spoofing** – Email spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

10. **Encryption Software** – Encryption software is software whose main task is encryption and decryption of data, usually in the form of files on (or sectors of) hard drives and removable media, email messages, or in the form of packets sent over computer networks.

11. **Encryption Key** – An encryption key allows credentials information to be encrypted or decrypted.

12. **Extranet** – An extranet is a private network that uses Internet protocols and network connectivity. An extranet can be viewed as part of a company's intranet that is extended to users outside the company.

13. **FTP** – File Transfer Protocol. FTP technology allows you to transfer files between two computers over the internet.

14. **Hacking** – When someone modifies computer hardware or software in a way that alters the creator's original intent.

15. **HIPAA** – Health Insurance Portability and Accountability Act of 1996 that among other things established standards for the security and privacy of human health-related information.

16. **Incineration** – A physically destructive method of sanitizing media; the act of burning completely to ashes.

17. **Internal Data** – County Government Data intended for internal government business only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need.

18. **Internet** – An electronic communications network that connects computer networks and organizational computer facilities around the world.

19. **Intranet** – A local or restricted communications network; a privately maintained computer network that can be accessed only by authorized persons.

20. **Media** – Material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CD’s and DVD’s, or paper-based products.

21. **Media Sanitation** – The process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.

22. **Network Sniffing** – A sniffer is a program that monitors and analyzes network traffic, detecting bottlenecks and problems. Besides being used as a review technique, network sniffing can also be used as a target identification and analysis technique.

23. **News-Groups** – An area on a computer network, especially the internet, devoted to the discussion of a specified topic. A discussion about a particular subject consisting or notes written to a central internet site and redistributed through Usenet, a worldwide network.

24. **Network Firewall** – A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny network transmissions based upon a set of
rules and other criteria for the purpose of limiting the exposure of the network to viruses, worms, adware, or other potential threats as well as other unauthorized internet uses that bog or slow the network.

25. **Packet Spoofing** – The act of capturing packets of data flowing across a computer network such as passwords, IP addresses, protocols, etc, then using that information to infiltrate the network.

26. **Peripherals** – A computer device, such as a CD-ROM drive, or printer, that is not part of the essential computer, i.e., the memory and microprocessor, attached to a host computer, and more or less dependent on the host. It expands the host’s capabilities, but does not form part of the core computer architecture.

27. **Ping Floods** – A pinged flood is an attempt by an attacker on a high bandwidth connection to saturate a network with packets in order to slow or stop legitimate traffic going through the network. A pinged flood consists of sending a continuous series of ICMP Echo Request (Ping) packets to a target host on the network, which responds with ICMP Echo Replies. The continuing combination of requests and replies can slow the network and cause legitimate traffic to continue at a significantly reduced speed or, in extreme cases, to disconnect. A ping flood attack can effectively disable your network connectivity.

28. **Pirated Software** – The copyright infringement or unauthorized copying or use of computer software (often referred to as software piracy).

29. **Pulverization** – A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

30. **Purging** – A media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting, exceeds the value of the data to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

31. **System Level Password** – A master level or administrative password for a particular workstation, server or network.

32. **Trojan Horse Code** – A Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk drive. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

33. **User Level Password** - A password for a personal computer workstation not shared by other users. Usually set by the actual user. User level passwords are granted specific privileges not necessarily shared by other users.

34. **Viruses** – A software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer; a true virus cannot spread to another computer without human assistance.
35. **Worms** – A self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any human intervention. This is due to security shortcomings on the target computer or network.

### 14.0 Employee Agreement on Use of Email and the Internet

I have read, understand and I hereby agree to comply with the foregoing policies, rules and conditions governing the use of the Bedford County Government’s computer and telecommunications equipment and services. I understand that I have no expectation of personal privacy when I use any of the said telecommunication equipment or services and that when my personally owned smartphone is connected to county-owned Wi-Fi that my expectation of personal privacy with regard to my activity on that device is substantially diminished or non-existent. I am aware that violations of this guideline on appropriate use of the e-mail and Internet systems may subject me to disciplinary action, including termination from employment, legal action and criminal liability. I further understand that my use of the e-mail and Internet may reflect on the image and reputation of Bedford County Government to our citizens and that I have responsibility to maintain a positive representation of my employer. Furthermore, I understand that this policy can be amended at any time.

Dated: ______________. [Signature of employee] ________________________________

[Printed name of employee] ________________________________