Bourbon County, Kansas
Electronic Information Acceptable Use Policy

1.0 Overview

The Bourbon County IT Department's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Bourbon County's established culture of openness, trust, and integrity. Bourbon County IT is committed to protecting Bourbon County's employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

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 Bourbon County. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations. Please review the Bourbon County Employee Handbook policies for further details.

Effective security is a team effort involving the participation and support of every Bourbon County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. Users must be always aware that this is a government network and is shared by everyone including, Police, Fire, County Offices, Dispatch, Public Works, and Court. So, anything that you do in a reckless or unsecured manner affects not only you, but several other agencies and users.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Bourbon County. These rules are in place to protect the employee and Bourbon County. Inappropriate use exposes Bourbon County to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Bourbon County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Bourbon County.

4.0 Policy

4.1 General Use and Ownership

1. While Bourbon County's IT Department desires to provide a reasonable level of privacy, users should be aware that the data they create on the county systems remains the property of Bourbon County. All systems in all areas are the sole property of Bourbon County, this includes all electronic devices that link to the Bourbon County network. These items such as Servers, Computers, Printers, Scanners, Phone Systems, Cloud Based Systems, such as E-Mail and Software. Everything County owned that is tied to the Bourbon County Network is the sole property of Bourbon County and is excluded from individual department control. Bourbon County IT also may control, and limit use of any item linked to the Bourbon County Network either County owned or personal. This is a government owned system and users should have no

expectation of privacy, **SYSTEMS ARE FOR COUNTY BUSINESS ONLY, USING THEM FOR PERSONAL USE SHOULD BE LIMITED AND ALL SYSTEMS ARE MONITORED**.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. Bourbon County IT recommends that any information that users consider sensitive or vulnerable be encrypted. Encryption mainly is for Law Enforcement and other sensitive nonpublic information.
4. For security and network maintenance purposes, authorized individuals within Bourbon County will monitor equipment, systems, and network traffic daily.
5. The Entire Bourbon County Network is controlled by a central domain host controller which allows permissions to be set as to the security level afforded any user. All users will be allowed basic control functions of the windows environment, security will be set up on a case-by-case basis at the sole discretion of the Chief Information Officer. General users will be given less latitude and control of their systems than department heads. **NO USER HAS PERMISSION TO INSTALL ANYTHING ON ANY SYSTEM WITHOUT SPEAKING TO THE IT DEPARTMENT FIRST. MAKING CHANGES TO OR TRYINGTO CHANGE SYSTEM SETTINGS WILL RESULT IN THE SYSTEM BEING LOCKED DOWN COMPLETELY**.
6. Communications archiving is done autonomously by both the phone system and the e-mail system. This is not monitored by anyone but acts as a security layer in the event of a threat or possible litigation. Voice recordings are not public and cycle off the system every 60-90 days. The system is in place solely for the protection of our employees. If there is a need to access this archive, a request must be made in writing as soon as possible to the IT Department so it can be pulled.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Confidential information should be only stored in your personal one drive hosted offsite. This assures that this type of information is secure from a physical standpoint as well as being redundant.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, 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 when the host will be unattended.
4. Encryption is mainly used for KBI and VPN use and follows their specifications and requirements.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised.
6. Postings by employees from a Bourbon County email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Bourbon County, unless posting is during business duties.
7. All hosts used by the employee that are connected to the Bourbon County Internet/Intranet/Extranet, whether owned by the employee or Bourbon County, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
9. If a user can identify a phishing, spam, or malicious email, it is highly encouraged the user reports the email using the tools available to them on the online version of their email, or at a minimum report the email to IT. By using the online report function, the user can help not only themselves receive lass malicious mail, but also others in the county that may receive similar messages by training the automatic filter.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during 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 production services).

Under no circumstances is an employee of Bourbon County authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Bourbon County, County or State-owned resources.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

5.0 System and Network Activities

5.1 The following activities are strictly prohibited, with no exceptions

1. 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 Bourbon County or the end user does not have an active license is strictly prohibited.
2. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan's, e-mail bombs, etc.).
4. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
5. Using a Bourbon County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
6. Downloading of any pornographic materials or content.
7. Effecting security breaches or disruptions of network communication.
8. Circumventing user authentication or security of any host, network, or account.
9. Using any program/script/command, with the intent to interfere with, or disable, a user's terminal session.
10. Posting to any known anonymous forum which allows user to post without revealing their identity.
11. Posting any no employment related posts on social media on Bourbon County owned equipment, including Phones, Tablets, and PCs.
12. County owned equipment, including PCs, Laptops, Phones, and iPhones that are turned in are not to be factory reset (wiped) by the end user. The IT Department will do this for all devices turned in.

6.0 Email and Communications Activities

6.1 The following activities are strictly prohibited, with no exceptions:

1. 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).
2. Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. 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.

Employee Internet Use Monitoring and Filtering Policy

1.0 Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within Bourbon County's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner and ensure that employee web use can be monitored or researched during an incident.

2.0 Scope

This policy applies to all Bourbon County employees, contractors, vendors, and agents with a Bourbon County-owned or personally owned computer or workstation connected to the Bourbon County network. This policy applies to all end user-initiated communications between Bourbon County's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

3.0 Policy

3.1 Web Site Monitoring

The County shall monitor Internet use from all computers and devices connected to the County network. For all traffic the monitoring system will record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic.

3.2 Access to Web Site Monitoring Reports

General trending and activity reports will be made available to department supervisors as needed upon request to the Information Technology Department.

3.3 Internet Use Filtering System

The County shall block access to Internet websites and protocols that are deemed inappropriate for Bourbon County's business or network environment. The following protocols and categories of websites will be always blocked:

- Adult/Sexually Explicit Material
- Gambling
- Illegal Drugs
- Peer to Peer File Sharing
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Games
- TV or Video
- Anonymous Forums

The Filtering System will be equipped with Dynamic Filter and the above blocked content will always be blocked. The amount of time given to employees will vary by individual need and be set and agreed to by the Department Heads. After the Employee has used the block of time for personal use the System will revert to filter all traffic that is not deemed work related. Each department will have a list of websites that it uses to function daily preset into the system after the block time has expired this will be the only use permissible. This system is adaptable, and sites can be added to these lists a requested by the Department Heads. **OVERUSE DURING BUSINESS HOURS BY ANY USER OF THE SYSTEM WILL RESULT IN TIME LIMIT RESTRICTIONS BEING PUT INTO PLACE ON INDIVIDUAL PERSONNEL ON A CASE-BY-CASE BASIS**. (Overuse being

defined taking up too much bandwidth during the business day. Some social media platform services waste large amounts of bandwidth.

3.4 Internet Use Filtering Rule Changes

The Information Technology Department shall periodically review and recommend changes to web and protocol filtering rules. The IT Department and Department Supervisors shall review these recommendations and decide if any changes are to be made. Changes to web and protocol filtering rules will be recorded in the Internet Use Monitoring and Filtering Policy.

3.5 Internet Use Filtering Exceptions

If a site is mis-categorized, employees may request the site be un-blocked by submitting a written request to the Information Technology Department. An IT employee will review the request and un-block the site if it is miss-categorized.

Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their Department Supervisor. They will present all approved exception requests to Information Technology in writing or by email. Information Technology will unblock that site or category for that associate only. Information Technology will track approved exceptions and report on them upon request.

3.6 Attempts to Circumvent Filtering Protocols

Logging of employees who make ongoing attempts to go to blocked sites or trying to use a proxy or third-party device. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.7 Enforcement

The IT Department will provide, if needed, monthly reports to Commissioners and Supervisors if there is internet abuse by their employees from the monitoring and filtering systems to ensure they follow this policy. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Employees who abuse the internet on a regular basis will be whitelisted for internet use and only allowed access to sites listed by their supervisor.

Removable Media/Personal Devices Policy

1.0 Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

Definition: Removable Media: Device or media that is readable and/or writeable by the end user and can be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players, Phones/ PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; Flash drives, speed sticks, jump drives, SD and microSD cards floppy disks and any commercial music and software disks not provided by Bourbon County.

2.0 Purpose

To minimize the risk of loss or exposure of sensitive information maintained by Bourbon County and to reduce the risk of acquiring malware infections on computers operated by Bourbon County.

3.0 Scope

This policy covers all computers and servers operating in the Bourbon County Government Network.

4.0 Policy

4.1 Removable Media

Bourbon County staff may only use Bourbon County removable media in their work computers. Bourbon County removable media may not be connected to or used in computers that are not owned or leased by the Bourbon County without explicit permission of the Bourbon County IT staff. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required by other state or federal agencies. Exceptions to this policy may be requested on a case-by-case basis by Bourbon County-exception procedures.

4.2 Personal Devices and wireless network.

The wireless network is for Bourbon County users and equipment, using this system for personal use is generally accepted, however abuse will not be tolerated and will result in the personal equipment being blocked from the system at the hardware level. **NO EQUIPMENT MAY EVER BE PLUGGED INTO THE WIRED NETWORK UNLESS CLEARED THROUGH THE IT DEPARTMENT**.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and payment to Bourbon County for any damages. Users not under direct control of the commission will have their access and system rights severely limited or completely turned off and are still financially responsible for any damages. This includes very strict internet filtering and strict system limitation actions. These systems are for county work only and should be viewed as such. Elected officials should take an active role in enforcing this policy but have no direct control over these limitations as they are county (taxpayer) owned systems. Repeat violations of this policy will lead to complete access denial to a user no matter what department they are in. System and Data security is of the utmost importance to the IT Department.

Bourbon County Email Use Policy

1.0 Purpose

To prevent tarnishing the public image of Bourbon County. Email from Bourbon County to the public may be viewed as an official policy statement from the Bourbon County.

2.0 Scope

This policy covers appropriate use of any email sent from a Bourbon County email address and applies to all employees, vendors, and agents operating on behalf of Bourbon County.

3.0 Policy

3.1 Prohibited Use.

The Bourbon County email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Bourbon County employee should report the matter to their supervisor immediately.

3.2 Personal Use.

Using a reasonable amount of Bourbon County resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Bourbon County email account is prohibited. Virus or other malware warnings

and mass mailings from Bourbon County shall be approved by Bourbon County IT operations before sending. These restrictions also apply to the forwarding of mail received by a Bourbon County employee.

3.3 Monitoring

Bourbon County employees shall have no expectation of privacy in anything they store, send, or received on the company's email system. Bourbon County may monitor messages without prior notice. Bourbon County does not monitor email messages unless warranted.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. This may also include financial responsibility by the employee of repairing all systems that an employee damages due to violation of this computer use policy.

Access Control Systems

1.0 Card and Fob Policy

Many buildings owned by Bourbon County have secure access control systems that require a keycard or fob to gain entry.

This policy is to provide an expectation of what is required to receive or replace a keycard or fob.

1. The first keycard or fob must be requested by either the department head or HR.
2. In the event that a fob or keycard is lost, stolen, destroyed, or is otherwise unusable, it needs to be immediately reported to IT so that it may be disabled and a new one issued for the user.
    a. In the event that this is required unusually often, corrective measures may need to be taken in the form of training, the user purchasing the replacement card/fob, or the user no longer being allowed to use the access control system.

Device Return Policy

There are many devices that can be reused after a person is no longer employed by Bourbon County, but some may have special steps that need to be taken so that they can be reused. The purpose of this policy is to set user expectations of what is to happen with their equipment when they leave Bourbon County.

1. The user is NOT to wipe/erase/factory reset/etc. their own equipment.
2. All equipment is to be returned either to the department head or IT directly.

a. If any equipment is returned and is not operational, the cause will be determined. If the cause is determined to be due to severe negligence of the user or having been done purposefully, the user may be required to pay for damages or a replacement.

3. If there are any accounts tying a device to an unmanaged account, such as but not limited to Apple's iCloud on an Apple device, the user must provide IT with any and all information associated to it so that they may properly unenroll the device. (This is typically done with the user present or over the phone in case there is two-factor authentication enabled.)

I hereby acknowledge that I received a copy of the Bourbon County, Kansas Electronic Information Acceptable Use Policy (Herein referred to as the Use Policy). I have read the Use Policy and agree to abide by the standards, policies, and guidelines defined or referenced within the document. The information in this Use Policy is subject to change. I understand that changes in the County policies may supersede, modify, or eliminate the information summarized in this Use Policy. As the County provides updated policy information, I accept responsibility for reading and abiding by the changes. I understand that the Use Policy intends no modification to contractual relationships or alterations of at-will relationships.

Name of Employee: _____

Department: _____

Signature of Employee_____ Date_____