Technology Services Resource Policy
Effective Date: June 17th, 2013

PURPOSE

This policy defines the appropriate use of technology resources that are owned or leased by Bell County and provided for employee use. The inappropriate use of technology resources exposes Bell County to risks including virus attacks, compromise of network systems, services and legal issues. This policy provides guidance to help protect the employee and Bell County. Departments are permitted to issue their own policies that augment or adopt this policy through reference, but not to supersede or contradict it.

[Note: Please reference Bell County Mobile Device Management (BYOD) usage policy regarding standards, procedures, and restrictions for end users who are connecting a personally-owned device to Bell County’s network for business purposes.]

APPLICABILITY

This policy applies to anyone who uses County technology resources, including full and part-time employees, temporary employees, contractors, vendors and all others.

POLICY

The Bell County Technology Services Resource Policy addresses employee use of assigned computer resources, internet and email usage, social media involvement, ownership and management of data and infrastructure security.

Computer Resources

The County’s computer resources are being provided for work-related purposes. All use of computer resources is subject to rules, regulation and oversight review. The County does not maintain these rights for the purpose of intruding into activities of employees, but does so in order to protect Bell County, its property and its interests, and those of its employees. Use of Bell County’s computer resources is subject to the following guidelines:

- Ensure the security and integrity of the County’s computer resources and all information contained therein at all times
- Safeguard and protect passwords and access codes (employees should never share password with others)
- All material maintained on the computer resources is subject to review. Employees should not maintain any unauthorized information on County computers.
- It is not intended that incidental personal use of the computers, the e-mail system and the access to the Internet provided by the County is to be entirely prohibited. However, use of County Computers, the County e-mail system or internet access by an employee for personal purposes must not interfere with the employee’s job or distract others. For that reason, the County reserves the right to instruct any or all employees to discontinue all personal use of the County computers, the e-mail system and internet access at any time.

Internet

Employees may use County resources to access authorized internet sites at any time for work related purposes. The County reserves the right to monitor internet usage to include sites visited and record internet usage time, review any materials transmitted across and/or stored in County resources connected to the infrastructure.

Limited Personal Use

County owned technology resources may be used for personal purposes on a limited basis, providing the following requirements are met:

- No marginal cost to the County
- No interference with work responsibilities
- No disruption to the workplace

Specific Prohibitions and Limitations

County policies regarding acceptable behavior and communication will apply to use of the Internet and messaging. Each user is responsible for respecting and adhering to local, state and federal law. Any attempt to break those laws using the county’s network infrastructure may result in litigation against the offender by the proper authorities. If such an event should occur, Bell County will fully comply with the authorities to provide any information necessary for the litigation process. Specifically prohibited use includes but is not limited to:

- Conducting a private business
- Political campaigning
- Accessing sites which promote exclusivity, hatred, or positions which are contrary to embracing cultural diversity
• Accessing inappropriate sites including adult content, online gambling, and dating services
• Accessing sites that promote illegal activity, copyright violation, or activity that violates the County’s ethical standards
• Using the internet to obtain or disseminate language or material which would normally be prohibited in the workplace
• Using encryption technology that has not been approved for use by the County
• The use of personally owned technology, not subject to management under the Bell County Mobile Device Management usage policy, for conducting County business, where official County records are created but not maintained by the County
• Making unauthorized general message distributions to all users (everyone)
• Installing any software that has not been approved by the County
• Sharing or storing unlicensed software or audio/video files
• Using security exploit tools (hacking tools) to attempt to elevate user privileges or obtain unauthorized resources
• Broadcasting external e-mail to large numbers of constituents unless the list members are hidden through the use of the BCC field
• Using a County e-mail address when posting to public forums e.g. blogs, social media sites, wikis and discussion lists for personal use
• Accessing sites that distribute computer security exploits (“hacking” sites);
• Accessing on-line auction sites (except for County business)
• Excessive use of online shopping
• Excessive use of social networking sites for personal use
• Excessive use of streaming media for entertainment during work hours
• The use or installation of unauthorized Instant Messaging, (e.g. AIM, Yahoo Instant Messenger, Meebo, IRC, etc)
• Using unauthorized Peer to Peer Networking, (e.g. E-Mule, Kazaa, Limewire, Warez, etc)
• The use of “Soft” VOIP phones, (e.g. Skype, Vonage, etc) without prior coordination with Technology Services

Internet Filtering

The County maintains filtering software for all county computer resources accessing the internet. Exceptions to the filtering requirement may only be made on a department basis to support appropriate governmental purposes and in extremely limited cases on an individual basis. Department Directors should forward such requests in writing to the Director of Technology Services for approval, identifying the Department requirements
and a listing of computers residing within the department requiring the exception, and the reason the exception is needed. Technology Services will maintain a list of devices and users with reduced internet filter limitations, which is subject to periodic auditing by the County’s Internal Auditor. The filtering of county computers does not relieve persons from the requirements specified in this procedure regarding access to unauthorized sites for non-governmental reasons, nor does it provide a defense concerning any violations discovered.

The internet filtering shall not be used as a resource to limit individual employee access to authorized internet sites. Instead, elected officials and department managers are responsible for the management of employees under their supervision. The County does operate other internet monitoring resources that can be used to document specific internet activity to include listing of sites visited and time spent accessing internet sites on a per computer resource basis as a way to document and manage employee internet usage.

Electronic mail

Electronic mail systems and services are provided by Bell County for the purpose of enhancing productivity and maintaining effective communication. Email sent, received, or stored on computer resources owned, leased, or administered by Bell County is not private and may be accessed by appropriate personnel.

In order to prevent system overload and introduction of vulnerabilities into the email system, county employees must limit the use of the following features to work-related purposes, including but not limited to:

Employee Mailbox

An electronic mailbox is established for each authorized employee. All authorized email users, with limited exceptions, are added to the Exchange Server global address list that is made available to all Bell County employees. The global address list helps with address lookup and supports the delivery of messages relating to Bell County business. Other shared mailing groups may also be created at the request of elected officials and department heads. Employees are added to these groups as directed by the owner of the specific mailing group.

Whenever employees send electronic mail, the employee’s name and user ID are included in each mail message. Employees are responsible for all electronic mail content originating from the employee’s user ID account.
The mailbox file size for each Bell County employee is limited to 2 GB (gigabytes). Each employee is responsible for managing messages and folders contained within individual allocated mailbox space. An automatic message from the system will be sent if the size of a mailbox is equal to or larger than 2 GB. At that time, the employee will not be able to receive additional emails until the file size is reduced below 2 GB.

[Note: The file size may be reduced by moving your email from the top folders, ex: inbox, sent, etc. (the ones listed under yourname@co.bell.tx.us), to the folders listed under Personal Folders. Also, check to ensure that you have emptied your Deleted Items folder. You may not be able to send or receive emails until you have cleaned up your mailbox space.]

Incidental Use

As a convenience to employees, incidental use of electronic mail is allowed per the following restrictions:

- Incidental use must not result in direct costs to Bell County
- Incidental use must not interfere with the normal performance of an employee's work duties
- No personal messages should be sent or saved that may cause embarrassment to Bell County
- No personal messages should be sent, read, or saved that have high likelihood to expose Bell County computer systems and network communications to viruses or other harmful programs
- Employees should remove themselves from any personal mail lists that send messages containing content incompatible with this policy
- All messages - including personal messages - are owned by Bell County, they may be subject to open records requests, and may be accessed in accordance with this policy

Abuse of incidental use privileges may result in disciplinary action.

Prohibited Use

The following activities are prohibited by policy:

- Do not send email that is intimidating or harassing
- Do not use email for conducting a personal business
- Do not use email for purposes of political lobbying or campaigning
Do not violate copyright laws by inappropriately distributing protected works
Do not access another employee’s email without that employee’s consent
Do not pose as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role

Prohibited activities identified in this section are not all inclusive. Bell County electronic mail must never be used in a manner that violates Bell County policy, state law or federal law.

Limited Use

The following activities are limited because they may impede the functioning of network communications and the efficient operations of the County’s electronic mail system:

- Do not send unsolicited messages to large groups (i.e., county wide emails) except as required for County business. County-wide messages should have the approval of an elected official or department head
- Do not send or forward chain letters
- Do not send excessively large messages. Current message size with attachments is limited to 10 MB (megabytes) per email
- Do not send or forward email that is likely to contain computer viruses. Also, URL links in emails received from external senders pose a risk of linking to a malware site that could introduce security threats to the county’s network

Email Retention

Electronic mail is subject to Texas State Library and Archives Commission retention schedule and rules for local government, record number GR1000-XX. The Bell County retention schedule is to keep all received and sent emails for a period not to exceed four years.

Employees are responsible for retaining any emails they designate requiring storage longer than four years by permanently storing the email in a local computer storage directory that is backed-up by the County’s enterprise storage system or stored in the County’s content management system within a specific case file.

The following types of sent or received email will be kept by the County’s email storage system for a period not to exceed four years:
• Policy and program development correspondence
• General email sent or received in the normal conduct of business
• Transitory correspondence
• Supervision records
• Public Information requests
• Complaints
• Unique to agency or type of organization

Email Filtering

The County maintains SPAM (anonymous, unsolicited bulk email) filters which automatically filters for and removes suspect or dangerous email from delivery and places them into a SPAM folder. Incoming email that could be interpreted as SPAM may include, but is not limited to, unacceptable file extension, excessively large size file attachments, objectionable content based upon subject title and body, and recognized malware or virus signatures. End users are provided the capability to manage their SPAM folders and remove unwanted items.

Social Media

The County supports the controlled use of social media sites and tools to reach a broader audience by sharing information to further the goals of the County and its respective departments, communicate directly to the public and increase government transparency and efficiency. We recognize the importance of participation in these conversations and are committed to ensuring we’re engaged and listening in meaningful ways.

Employee Social Media

The use of social media by employees may become a problem if: it interferes with the employee’s work; is used to harass supervisors, co-workers, customers or vendors; creates a hostile work environment; or harms the goodwill and reputation of Bell County among the community at large. Bell County encourages employees to use social media within the parameters of the following guidelines and in a way that does not produce the adverse consequences mentioned above.

Where no policy or guideline exists, employees are expected to use their professional judgment and take the most prudent action possible. If you are uncertain about the appropriateness of a social media posting, check with your manager or supervisor.
For purposes of this policy “social media” includes, but is not limited to, forums, blogging and social networking sites, such as Twitter, Facebook, LinkedIn, Pinterest, and MySpace.

- Should an employee decide to create a personal blog, be sure to provide a clear disclaimer that the views expressed in the blog are yours alone, and do not represent the views of Bell County
- If your posts on a social media site mention Bell County make clear that you are an employee of Bell County and that the views posted are yours alone and do not represent the views of Bell County
- Do not mention Bell County supervisors, employees, customers or vendors without their express consent
- Do not pick fights. If you see a misrepresentation about Bell County, respond respectfully with factual information, not inflammatory comments
- Remember, you are responsible for what you write or present on social media. You can be sued by other employees, supervisors, customers or vendors, and any individual that views your social media posts as defamatory, pornographic, proprietary, harassing, libelous or creating a hostile work environment
- Social media activities should not interfere with your duties at work. Bell County monitors its computers and networks to ensure compliance with this restriction
- You must comply with copyright laws, and cite or reference sources accurately
- Do not post Bell County material on a social media site without written permission from the County’s social media coordinator
- Employees are also prohibited from using a county e-mail address to register on social networks, blogs or other online promotions or tools utilized for personal use
- All Bell County policies that regulate off-duty conduct apply to social media activity including, but not limited to, policies related to illegal harassment and code of conduct
- Any confidential information that you obtained through your position at Bell County must be kept confidential and should not be discussed in any social media forum

Violation of this policy may lead to discipline up to and including the immediate termination of employment.
County Social Media

The County maintains an overriding interest and expectation in deciding what information is provided on behalf of the County on social media sites. This policy establishes guidelines for the use of social media by authorized Bell County employees:

The County’s Social Media Coordinator, appointed by the Technology Services Director, is responsible for maintaining the county’s social media sites on Facebook and Twitter. Individual departments are encouraged to contribute content to the existing county social media sites instead of creating separate sites.

The Coordinator duties include serving as the account contact, developing the engagement framework for posting information and responding to comments, adhering to polices, and ensuring the social media site is regularly updated. Other authorized staff may manage day-to-day operations of a social media site with close consultation with the County Coordinator.

Bell County social media sites are subject to State of Texas public records laws. Any content maintained in a social media format that is related to County business, including a list of subscribers and posted communication, is subject to the Texas Open Records Act, and considered a public record.

Information Security Management

The County’s Technology Services Director serves as the Information Security Manager and has ultimate responsibility and approval authority to examine system risks and require appropriate assurance levels of information security controls for all systems. Employees shall take all reasonable steps and precautions to ensure the security and integrity of the County’s computer system(s) and all information contained therein.

The Information Security Manager also has primary responsibility for managing the vendor technology relationship for all Internet-based or hosted business solution systems and services for the purpose of assuring appropriate technology practices are applied related to technology architecture, information system security, service level agreements, operational processes, technical support and business continuity.

[Note: Please reference Bell County Remote Vendor Access policy, effective 6/17/2013, for guidelines on how vendors may securely access the Bell County environment.]
Prohibited Use

The following activities are prohibited because they impose security risks and may impede the functioning of network communications and the efficient operations of the County’s electronic mail system:

- Using systems and/or networks in attempts to gain unauthorized access to remote systems
- Using systems and/or networks to attempt connection(s) to unauthorized systems;
- Copying of system files
- Copying of copyrighted materials, such as third-party software, without the express written permission of the owner or proper license
- Downloading items or installing items on Bell County computers, equipment or devices without special authorization from Technology Services

Disciplinary Action

Bell County is responsible for the management and security of its technology resources in a reasonable and economically feasible manner to guard against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users. Responsibility also includes informing users of punitive measures for non-compliance. Any employee who violates any provision of this policy, unless required to do so as part of his or her assigned and authorized job responsibilities, is subject to disciplinary actions.

Any unauthorized employee who intentionally receives, accesses, views, transmits, or downloads sexually explicit material from the internet on county computer resources will be disciplined up to and including termination. Sexually explicit material is defined as any description of or any picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting nudity, sexual excitement, or sexual conduct in any form. Persons subscribing to an email list will be viewed as having solicited any material delivered by the list, as long as that material is consistent with the purpose of the list. Likewise, persons conducting a search on the internet will be viewed as seeking any results generated by the search, as long as that material is consistent with the search.

Any employee who commits or is convicted of a crime related to the use of county computer resources may be terminated.
Any employee whose use of county computer resources results in damage to those resources will be required to reimburse the county for the cost of repair and reconfiguration, as well as the hours required for the repair work, and costs associated with replacing necessary hardware or software. Where damage occurs as the result of inadvertent actions, without the intent to cause damage, the employee causing the damage will not be asked to reimburse for such damage.

In determining the appropriate disciplinary action to be taken against an employee under this policy, supervisors shall apply the standards set forth in the Personnel Policies of the County for appropriate situational discipline (Section 200) and shall ensure that the employee ethics and general work rules and expectations (Section 200/201) is maintained. In addition, supervisors shall consider the nature of the employee’s job responsibilities, and the legality or illegality of the violation in determining the appropriate disciplinary action. Discipline may include any of the options contained in Section 202 of the Bell County Employee Handbook, including, but not limited to:

- Suspension of access to e-mail or internet services
- Restitution or reimbursement for the hours used to conduct personal business on County computer resources in violation of this policy
- Other disciplinary action(s) as outlined in Section 202 of Bell County Employee Handbook
- Termination of employment

Policy Acknowledgment

All employees with a computer user ID are required to sign an acknowledgement that states the employee has received and read the “Technology Services Resource Policy.”

Employee Declaration

I, [employee name], have read and understand the Technology Services Resource Policy, and consent to adhere to the rules outlined therein.

________________________________________  _________________________
Employee Signature                      Date