13.01 INFORMATION RESOURCES

13.01.1 Policy on Use and Security of Information Resources

I. Policy

A. This policy governs the use of the Technology resources owned and operated by Brazos County by employees, and all other authorized users. Technology, called Information Resources includes, but is not limited to: desktops, laptops, mobile devices, networking equipment, networked devices, servers, software, email, phones, cellular phones, control systems, Internet, Intranet, and all other Enterprise electronic systems or devices. This policy is consistent with policy standards laid out in ISO 27002.

B. This policy establishes specific rules and standards relating to the safe and secure operation of all devices and the storage of data while connected to County Information Resources. Adherence to these rules and standards is a requirement for all persons utilizing County-owned devices or storing and accessing data on County technology infrastructure. These rules and standards shall be amended as necessary to remain current with various needs and risks, and are included in this policy. Failure to comply with these rules and standards shall be considered an improper use and may result in disciplinary action up to and including termination. This policy shall be reviewed yearly by a committee set by the Chief Information Officer (CIO).

C. Brazos County makes Information Resources available to employees that require them as a part of their normally assigned duties. The purpose of this policy is not to discourage the use of these Information Resources, but to provide a uniform approach to their use, safeguard County interests, meet all applicable laws, and to protect Information Resources from unauthorized access. Brazos County reserves the right to monitor all usage of County-owned and/or County network connected devices.

D. This policy establishes procedures whose primary purpose is information Confidentiality, Integrity, and Availability.

1. Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access.

2. Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct.

3. Availability means that authorized users have access to the systems and the resources they need.

E. Terms used in this document will be defined in the 'Security Policy Standard Definitions' document located here.

II. Procedures

A. Applicability

1. This policy shall apply to all County employees, volunteers, vendors, contractors, and other authorized users as defined herein. Departments may develop departmental policies and procedures which provide more specific direction to their employees.

B. Authorized Use

1. County Information Resources are provided for the purpose of conducting County business. Personal usage is permitted, as long as the personal use is reasonable and prudent. Responsibility and accountability for the appropriate use of County Information Resources ultimately rests with the individual authorized user.

2. No authorized user shall use any County Information Resources in violation of any applicable law.

3. No authorized user shall use any County Information Resources to conduct personal for-profit business, political campaigning, or distribution of protected copywritten works.

C. Exceptions

1. Exceptions to this policy which are deemed expedient and prudent, shall be documented as part of each information security audit undertaken by Brazos County. Known exceptions include, but are not necessarily limited to, declared states of emergency and other emergency management and law enforcement situations.

D. Privacy

1. No authorized user accessing or using Brazos County Information Resources has any expectation of privacy. Brazos County reserves the right to monitor, intercept, archive, view, or distribute any communications and/or content created with, modified with, stored on, or transmitted over the resources which it owns, leases, or operates subject to all applicable laws.

    a) IT Staff may be required to access any and all material located on those resources. Examples include but are not limited to; computer forensics, technical support, supervision, open records requests.

    b) Department Heads may monitor employee use of the Internet and email and may revoke an employee's access to the Internet and/or email by notifying the helpdesk.

    c) Authorized users must be aware that any digital record residing on County Information Resources may be subject to lawful open records requests. In addition, any data regarding County business stored on a personal device or file sharing service is also subject to lawful open records requests.

E. Resource Access - Requirements, Restrictions, and Exceptions

1. Work Product

    a) No employee shall use the Internet or email to present his or her own personal views, ideas, questions, or actions, as representing the positions or policies of the County unless doing so in an official capacity and authorized by an elected official or his/her designee.

    b) When possible sensitive data must be encrypted when transmitted outside the County network or off County Information Resources.

    c) All work produced by an employee of Brazos County acting as an agent of the County is the property of Brazos County. All data stored on County Information Resources regardless of origin is considered property of Brazos County and is subject to review, modification and/or deletion, unless that data access and/or use is defined by state or federal law. Examples include but are not limited to Health Insurance Portability and Accountability Act (HIPAA) and Criminal Justice Information System (CJIS)

    d) Unless otherwise specified by contract, any work produced by a vendor, contractor, or other third party acting as an agent, consultant, or contractor to the County, is the property of the County, and employees shall take steps to ensure that such property is properly stored on County Information Resources to prevent loss.

2. Identity

a) Each person authorized to access County Information Resources must do so using a unique username (login id) assigned by the IT Department. Authorized users shall not share their account information or permit others to log in using their credentials. The use of group accounts will be limited to only those circumstances deemed necessary and approved by IT, and these exceptions will be documented and maintained by IT.

b) Electronic communications authored by the employee must clearly originate from the authorized user's unique account, unless the employee is communicating on behalf of a department or the County as a part of their job duties.

c) Each authorized user's access to County Information Resources will only be as much as necessary to complete their assigned duties and no more.

3. Account Management

a) It is the responsibility of each department to notify the IT Department prior to the start date of any new employee or authorized user who needs access to County Information Resources, so that appropriate access can be provided on a timely basis.

b) It is the responsibility of each department to immediately notify the IT Department in the event of a separation (defined in section 8.01 of Brazos County Personnel Policy Manual) of any employee within their department who previously had access to County Information Resources, so that such user accounts may be removed or disabled.

c) It is the responsibility of each department contracting with an outside agency to notify the IT Department at the conclusion of the contract, or anytime there is a change in contract personnel that would necessitate a change in login credentials.

4. Remote Access to Resources – The County maintains various systems to permit users to access internal systems from non-secured locations, like the Internet. These services are intended to augment the productivity of employees.

a) Any device connected to County Information Resources needs antivirus software and a vendor supported Operating System with the latest security patches.

b) It is the responsibility of the Authorized User using remote access to ensure that unauthorized persons cannot utilize their account to gain access to County Information Resources. Employees are not to provide their passwords to anyone, including family members or coworkers.

c) Personally owned devices that are used to conduct official County business may be subject to Freedom of Information Act (FOIA) or other legally binding search and discovery requests.

5. Data Storage

a) Employees should not store information exclusively on the local drive (C:, D:, etc.) of a PC or laptop or tablet. By storing the file outside of network or cloud storage provided by the County, the data is neither centrally searchable nor backed up. Employees are instead required to utilize network drives, County-provided cloud storage such as Microsoft OneDrive and SharePoint Online, or County-owned content management systems for the purposes of data storage.

b) County IT is not under any obligation to spend resources restoring data that is not stored on County provided data storage systems. This includes, but is not limited to, hard drive crashes or malware infestations of County supplied personal Information Resources, USB drives, and personally owned computing devices.

c) The department to whom an Information Resource has been issued is responsible for all costs associated with damage or loss of any device which has been issued by the IT department.

6. Training - Properly educating users about information security, best practices and risks serves to help reduce overall information security risks and probability of incidents.

a) All County employees and County contractors are required to take security awareness training per House Bill 3834. The state mandated cyber security training will be managed by the Information Technology Department and the Information Security Officer (ISO). It is the ISO or designee's responsibility to track completion of the training. It is the employee's responsibility to complete the training assigned. It may not be delegated to another individual. The ISO or designee will report the status of the County's progress to the Texas Department of Information Resources as required by law.

b) For certain users, there are other training requirements which include but are not limited to CJIS, Department of State Health Services, HIPAA. These training requirements are implemented at the state and federal level and will be managed by the responsible department.

7. Internet and Email

a) Bringing improper material into the work environment or workplace, or possessing any improper material at work to read, display, or view at work, or otherwise publicizing it in the work environment is prohibited.

b) No employee shall connect to any web site that contains improper material. The County reserves the right to block employee access to such web sites.

c) No employee shall operate or advertise any non-County business on the Internet using County Information Resources at any time.

d) No employee shall send chain letters, pyramid schemes, or unsolicited bulk email using County Information Resources at any time. Non-IT employees are not to send warnings about viruses or technology related risks relating to County Information Resources to their co-workers. They are required to forward these to the ISO or designee, or the helpdesk for review.

e) County Information Resources, including Internet and email, are to be used for County business. Incidental personal use of County Information Resources by County authorized users is permitted, provided such use does not result in direct costs to Brazos County, nor interfere with the employee's ability to fulfill their job requirements.

f) All employees shall use only their County-assigned email address during the performance of their assigned job duties. All requests for exceptions to this policy must be approved by IT.

g) Email received from citizens should be handled with the same seriousness as any other form of citizen contact. Employees should always maintain professional decorum in their responses, seek approval from supervisors where appropriate, and reply to messages promptly.

h) Unless specifically approved by the CIO, all County email transmissions shall be routed though the official County email system. No department or employee shall operate within County networks any email servers, mail forwarding services, or other email transmission or reception services for use by any person or automated system.

i) Internet traffic will be filtered to prevent access to inappropriate sites and those deemed detrimental to County business.

j) Internet access for non-business use is a privilege. Use of streaming sites (for example YouTube, Pandora, etc.) should be kept to a minimum to prevent a negative impact on business-critical bandwidth. Failure to self-moderate (excessive use) can result in remediation including loss of internet access or termination.

F. Personal Device Usage

1. Personally owned devices may be used to connect to County provided Information Resources remotely and through County approved remote access methods only. County owned software will not be installed on personally owned devices, unless approved by CIO and requesting employee's department head

2. Brazos County will not provide technical support for any problems that may arise from use of a personally owned device to conduct County business. Brazos County will not provide material support for any loss of non-county data resulting from using a personally owned device to conduct County business.

3. Brazos County reserves the right to disconnect or prevent connection to County network resources of any device, by any user, at any time, for any reason, without any notice whatsoever.

4. The employee attaching their personal device remotely to a County Information Resource assumes full liability for any risks, including, but not limited to, partial or complete data loss, errors, bugs, hardware loss or damage, viruses, malware, or any other issue which may damage the device, in any way whatsoever.

5. The CIO, or designee, shall be solely responsible for determining which devices may be used to connect to County Information Resources. Employees should contact the IT helpdesk to determine whether their device is eligible, and to obtain proper user credentials for their device.

6. The IT department will provide limited support for network connectivity issues. However, hardware and software support for personal devices will not be provided.

7. Connection to County-owned network resources is provided to employees as a convenience only. The County will not reimburse any expense, partial or otherwise, for any usage of a personal device, including cell phones, regardless of purpose.

8. Personal Device Security

    a) Rooted or "jailbroken" devices are not allowed to access County Information Resources, including email, messaging or online files. By making changes to the phones base operating system, the user is altering the phone in a way unsupported by the device manufacturer.

    b) Employee-owned personal devices are not allowed to connect to County Information Resources unless given an exception in writing by their Department Head and the CIO or designee. Excluded from this provision are publicly accessible services including but not limited to Microsoft Office 365, Oracle, and VPN. The County provides a complementary wireless network for non-County owned devices to connect to the Internet. The County reserves the right to filter, moderate, monitor, and restrict internet traffic on this network without warning. The user accepts full responsibility for any damage done to a device because of online actions taken while connected to this network.

G. Communications Network

1. No employee or other person shall install, remove, or move any network device onto the County communications network under any circumstances unless they have received permission to perform such actions from the CIO or designee.

2. No authorized user may install any device or software intended to monitor, capture, or eavesdrop upon, any portion of data traversing the County Network, excepting employees of IT, and then only to conduct County business. Vendors may do this if done as a part of a contract with IT to provide necessary services (for example Security, auditing)

3. Employees shall not attach any form of personal network equipment including, but not limited to, switches, routers, cellular repeaters/extenders, or access points to any County owned communications network.

4. No employee will permit any third party to connect any device to any ethernet port or secure wireless service without the express permission of the CIO or designee.

5. No employee shall install or operate any equipment, program, or service which has the effect of redirecting or proxying any network traffic to or from any other network, or with the purpose of disguising the source of any network transmission.

H. Software - The County is committed to preventing copyright infringement. It is the policy of Brazos County to respect all computer software copyrights and to adhere to the terms of all software licenses to which the County is a party. The County is subject to all laws governing the use of copyrighted software and documentation. Unless expressly authorized by the software licensor/developer, Brazos County has no right to make copies of the software except for backup or archival purposes.

1. All software used on a County computer must be licensed to the County for that computer/user.

2. Employees may not install any software not provided to them by the IT Department without specific authorization by the CIO or designee. Installing software necessary for holding meetings is allowed; this includes products like Zoom and GotoMeeting.

3. County employees shall not duplicate, copy, or reproduce any software purchased by and/or licensed to the County, or any related documentation without prior written approval from the CIO. County employees shall not give County-purchased or licensed software to any non-employees, including, but not limited to clients, contractors, customers, family members, and others without prior written approval from the CIO.

4. Software developed by employees on County time, on County-owned equipment, or for County projects shall be the property of Brazos County. Such software is for the exclusive use of the County, its officers, agents, and employees. Such software may not be sold, transferred, or given to any person without the prior written approval of the Commissioner's Court.

5. Software must be registered in the name of Brazos County. Software shall not be registered in an individual employee’s user ID or name.

6. Game software is an inappropriate use of County equipment and shall not be allowed on County Information Resources. Games discovered on County owned equipment will be removed.

I. Security - It is the responsibility of every employee to operate all County Information Resources in such a way as to minimize the risk of unauthorized access to, or loss of, any County Information Resources, to ensure that County Information Resources are not misused by any other person, and to act so as to protect the integrity of the data and resources of the County.

1. Each County authorized user must have a unique password. Passwords may not be written down where they can be found by unauthorized personnel or be shared with other individuals. It is the responsibility of the employee to maintain the secrecy of their passwords.

2. All employees shall immediately report any unauthorized access or unauthorized access attempt, virus infection, spyware infection, or other unauthorized or illegal resource use to the IT helpdesk.

3. Any County Information Resource that gets a virus or other form of malware must be turned over to IT immediately and retained for investigative purposes until it is no longer needed. A temporary replacement will be provided to the user until the original is returned or a permanent replacement is procured. Once the investigation is complete the device will be reimaged. All files on the infected device will be considered infected and will not be recovered. Only files stored on network storage will be considered for recovery efforts.

J. Technology Procurement

1. Departments will coordinate all technology or software related purchase requests (including grant proposals, RFPs, bids, contracts, purchase orders, and County credit card purchases) with the CIO or designee in writing prior to purchase. The purpose of this review is:

a) To ensure that the product(s) obtained are compatible with County standards and existing infrastructure.

b) To avoid unnecessary and costly duplication of capabilities.

c) To minimize impacts on support personnel and assure proper staffing is maintained.

d) To ensure all costs are properly considered.

e) To ensure that the proposed equipment or software does not interfere with the operation of existing systems, or create any undue risk to County Information Resources.

f) To ensure that ongoing vendor support is acquired where applicable and necessary.

g) To ensure that technology service providers are reviewed for appropriate security posture.