PROCEDURE 403-2 - USE OF INFORMATION TECHNOLOGY

The purpose of Johnson County Government's information technology resources is to conduct County business. Employees must ask their supervisor or the Department of Technology and Innovation (DTI) before acting if they are uncertain about whether their actions comply with this procedure.

Definitions

"County Information technology resources" means all computer, communication and related systems and all related hardware and software including, without limitation, computers, servers, networks, tablets, mobile devices, facsimile machines, pagers, printers, scanners, recording devices, cameras, radios and electronic equipment, Internet access, Intranets, messaging programs, electronic mail, voice mail, storage systems, and other devices owned, leased, licensed, or otherwise provided for use by the County through the use of public funds, and all data created, sent, received, or stored using any of the above.

Ownership and Privacy

County-owned resources. All County information technology resources, including all communications and data created, sent, received, or stored using those resources, are the sole property of Johnson County. Employees have no privacy rights and should not expect privacy in their use of the County's information technology resources whether that use is for County purposes or personal purposes. The County may monitor and audit use and may intercept, access, read, disclose, and delete all data and communications, including personal communications, created, accessed, received, or sent using County information technology resources or stored on such resources. Employees should not use County information technology resources for communications that they want to remain private such as communications with their health care providers or personal attorneys. Electronic data and communication created, sent, received, or stored on County information technology resources is generally an open public record and may also be subject to disclosure for legal purposes. Employees should take into consideration the possible disclosure of data before sending it electronically.

Personal resources. The County, without advance notice to the employee, may also monitor, audit, intercept, read, disclose, and delete all communications and data related to County business that is created, received, accessed, sent or stored using employee-owned information technology resources in conducting County business. All such communications and data are the sole property of Johnson County Government and employees have no right of privacy in such communications and data. Such information is generally an open public record and may also be subject to disclosure for legal purposes. In order to comply with records preservation requirements, employees are discouraged from conducting County business by text message on personal devices.

Clarifying County Versus Personal Purpose

Employees should ensure that any personal communication sent via County information technology resources does not appear to be an official communication of the County. Employees may not use their County titles in personal communications. If a reader could reasonably assume the personal communication is an official County communication, the employee must include a statement that the communication is personal and has not been authorized by the County.

Protecting Confidential Information
Employees should use care in communicating and storing confidential information electronically and should take reasonable steps to ensure that the communication is properly identified as confidential and directed to the appropriate recipient. Proprietary information generally should not be transmitted via email, facsimile, cellular telephones, or any other unsecure communication system. Employees must comply with the required levels of security related to governmental information systems and records, including but not limited to the level of confidentiality required under the Health Insurance Portability and Accountability Act (HIPAA) for the protection of protected health information. Employees must obtain DTI approval before using encryption devices to protect confidential information.

Passwords
Passwords, access codes, and security procedures are for the County's protection and should not be interpreted as creating any personal right of privacy for any user. Passwords provide unique access and should not be shared. Employees with access to Oracle, personnel records including employee medical records, HIPAA-protected information, or confidential legal documents must be particularly vigilant about not sharing their passwords, and in the rare occasion where sharing is necessary, must change their password at the first available opportunity. Employees designated as social media administrators may share passwords to social media sites with the persons identified in the *Social Media Standard for Business Use* maintained by the Public Information Office.

Intellectual Property and Licensing
Employees must comply with the terms of the County's software licensing agreements. All software loaded onto a Johnson County Computer must be legally licensed for that computer. Employees may not share or duplicate software from County information technology resources and may not download software or materials that are copyrighted, patented, trademarked, or otherwise identified as intellectual property without express permission from the owner of the material or as otherwise allowed by law.

Maintenance of Records and Management of Email, Voicemail, and Texts
All records of County business contained on County or personal information technology resources (e.g., email, texts, voicemail, and social media posts) must be maintained pursuant to the County's records retention policies.

Prohibited Use
Any use of the County's information technology resources that is illegal or that is inconsistent with the County values, Code of Ethics, or any County policy, procedure, or rule is prohibited. Any unauthorized access or attempt to gain unauthorized access to data, systems, or passwords is prohibited.

Protection of the County's Information Technology Resources
As responsible stewards of the County's information technology resources, all employees should take steps to protect those resources. Employees are expected to comply with all DTI procedures regarding the safeguarding of County information technology resources.

- **Viruses and Malware.** Internet and e-mail use, as well as file sharing, can expose the County to viruses and malware resulting in the loss of information, damage, or network systems shutdown. Employees must exercise caution to prevent computer viruses from being received or transmitted through the County's information technology resources. Employees should not open e-mail messages or attachments unless they are reasonably

certain of the trustworthiness of the source. Messages that contain inappropriate material should be deleted immediately. Messages that could be a potential security threat should be reported through established email security guidelines. If uncertain, employees should contact the DTI Support Center for guidance.

- **Streaming Services.** To avoid congestion of network systems, employees may not access services that provide streaming media or other continuous data, audio or video that is not business related.

- **Other Services.** Employees may not load, install, or run software to visit Internet sites that facilitate peer-to-peer file sharing, gaming, gambling, or other unauthorized activity.

Remote Access
Employees may be permitted to access the County's information technology resources from mobile devices or home computers, either County-owned or personal, only upon approval of a department/agency/office leader and prior installation of mobile device management software selected by DTI to reasonably ensure the security of County systems and data. The use of personally owned communication devices to access County systems will be granted only in the furtherance of County business purposes and subject to reasonable restrictions and conditions. Employees seeking such access must agree to the Remote Access Business Practice and must ensure the suitability of their personal device(s).

Non-Exempt Employees
Non-exempt employees may not access County information technology resources remotely for purposes of performing work without prior supervisor approval. Non-exempt employees who use information technology devices to work remotely, must report and be paid for their work.

Departments/Agencies/Offices
Each department/agency/office must implement and enforce this procedure unless it has business or operational requirements that justify deviation from specific provisions. Alternative provisions must be: (1) justified by business need or purpose, (2) consistent with the intent of this procedure, (3) proposed in writing by the department/agency/office leader, and (4) submitted to the County Manager for approval. Department/agency/office provisions may be more restrictive than those contained in this procedure, but, generally, not less restrictive.

County criminal justice departments/agencies/offices that have access to or make use of criminal justice information systems, including without limitation KCJIS, NCIC and ALERT, are required to comply with all state, federal, and contractual requirements related to the use of such systems. Department/agency/office leaders are responsible for ensuring compliance with the requirements related to the use of criminal justice information systems and must develop protocols for their use where appropriate.

Effective 05.01.2021, Resolution No. 014-21