RESOLUTION NO.: _____

A RESOLUTION ADOPTING AN INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY AND REPEALING PRIOR RESOLUTIONS REGARDING SUCH POLICY

WHEREAS, the Board of County Commissioners of Sedgwick County, Kansas ("County") by Sedgwick County Resolutions 257-1997, 85-2001, 104-2008 and 137-2012, implemented a policy pertaining to the use of technology; and

WHEREAS, upon review of said policy, County finds it is desirable that such policy should be repealed and replaced to better serve current needs.

NOW, THEREFORE, be it resolved by the Board of County Commissioners of Sedgwick County, Kansas that:

SECTION 1. Sedgwick County Resolutions 257-1997, 85-2001, 104-2008 and 137-2012 are hereby repealed.

SECTION 2. The "Information Technology Acceptable Use" policy (Policy No.: 3.000), attached hereto and incorporated herein as Exhibit A, is hereby adopted.

Commissioners present and voting were:

DAVID M. UNRUH	_____
MICHAEL B. O'DONNELL, II	_____
DAVID T. DENNIS	_____
RICHARD RANZAU	_____
JAMES M. HOWELL	_____

Dated this _____ day of _____, 2018.

BOARD OF COUNTY COMMISSIONERS
OF SEDGWICK COUNTY, KANSAS

ATTEST:

_____
DAVID T. DENNIS, Chairman
Commissioner, Third District

_____
KELLY B. ARNOLD, County Clerk

_____
DAVID M. UNRUH, Chair Pro Tem
Commissioner, First District

APPROVED AS TO FORM:

KAREN L. POWELL
Deputy County Counselor

MICHAEL B. O'DONNELL, II,
Commissioner, Second District

RICHARD RANZAU
Commissioner, Fourth District

JAMES M. HOWELL
Commissioner, Fifth District

Exhibit A

Sedgwick County... working for you	Information Technology Acceptable Use
Last Revision Date: _____	Policy No.: 3.000
Last Enabling Resolution: _____	Developer/Reviewer: DITSS

1. Purpose

Sedgwick County encourages all employees using information technology (IT) to become adept in its use. Information technology includes Internet access, electronic and voice message systems, facsimile devices, or other electronic systems used by Sedgwick County.

The mission of the Division of Information Technology and Support Services is to provide the highest quality technology-based and support-based services, in the most cost-effective manner, while exceeding expectations in customer service, and fully supporting the organization's mission of providing quality public services to our community, to all County departments as well as the 18th Judicial District.

2. Scope

This policy applies to all divisions, departments, elected officials, contracted entities and other individuals or groups that use County equipment. Any of the offices of Sedgwick County Government as well as the 18th Judicial District may develop more specific information technology policies for application within the department or division, but none may write more lenient policies.

To assist DITSS in fulfilling its role, all employees, elected officials, department heads, and division directors must: protect computer equipment in their charge from physical damage or misuse; take appropriate steps to protect computer output containing sensitive information; prevent unauthorized individuals from viewing or having access to computer displays; obtain and delete user identifiers providing access to computer functions for employees and ensure that adequate internal office procedures are in place for their employees to logoff/sign-off networks when appropriate; make all reasonable efforts to assure passwords for the employees of their departments remain secure; maintain sufficient manual procedures to enable the functions of their department to continue in some limited fashion during a computer outage of any length; and assume responsibility for relocation of computer equipment.

3. Policy Statement

3.1 Regulatory Responsibility.

Sedgwick County will comply fully with the Kansas Open Records Act (K.S.A. 45-215 et seq.), HIPAA, PCI-DSS, and CJIS with respect to electronic data. Sedgwick County employees will not knowingly receive, install, copy, use, maintain, or provide software or any machine-readable data in violation of federal or state laws or local ordinances. Electronic and voice mail capabilities provided to employees are for official business use, and shall be subject to access by appropriate supervisory personnel without an employee's knowledge.

3.2 Payment Card Industry Data Security Standards (PCI DSS).

Sedgwick County Departments will comply with data security standards set out by Sedgwick County and in accordance with the Payment Card Industry Data Security Standards (PCI DSS). Reference County PCI DSS Policy.

3.3 Compliance with Open Records Requests.

DITSS will comply with and assist all departments in compliance with KORA laws and regulations surrounding Open Records Requests.

3.4 E-Mail, Instant Message, and Other Electronic Communications:

3.4.1 Subject Matter.

The subject matter of messages and all electronically sent and stored data should demonstrate good judgment and reflect the professionalism of Sedgwick County. Content should pass the test of being able to appear in the newspaper without being embarrassing or offensive to anyone. Specifically prohibited are political activity and campaigning, religious messages or slogans, illegal activity, gaming (betting, gambling, wagering), representing personal opinion as that of the County, unauthorized solicitations, revealing unauthorized or confidential information, slander, libel, deliberate misinformation, accessing pornographic material (other than for law-enforcement purposes) and use for a personal business enterprise.

3.4.2 Signature Blocks:

Personalized signature blocks create branding inconsistencies and an unprofessional image. When employees communicate with e-mail and other technologies, ensuring consistent messages and brand recognition is important. Therefore, all e-mails will conform to the standards outlined in the E-mail Guidelines: Signature Blocks and Other Guidelines document.

3.4.3 Unknown Sources.

Take extra caution when receiving a message or opening an attachment from an unknown source, especially from an address exterior to the County's e-mail system. The potential to spread viruses is significant and opening such a message could have devastating results to the entire County system. "When in doubt, throw it out."

3.5 Technology Usage:

3.5.1 **County Business.** Except as noted below, information technology should be used only for official County business. Care should be taken to limit the number of persons outside the organization who know your County e-mail address. By doing this, you will limit the number of unsolicited, personal, and offensive messages received. Server space is limited and should be reserved for County use. Announcements intended for all County employees and other mass mailings shall be sent to the Communications Office for approval, editing, and distribution.

3.5.2 **Personal Use.** The use of County technology for personal use should be incidental and confined to "off the clock" time periods (comparable to reasonable breaks during the day or during meal periods), and must never impact technology resources in such a way as to negatively impact the business use of the technology.
Brief and occasional messages of a personal nature may be sent and received, but sending chain e-mail is prohibited. Messages with non-County business content – for example, jokes, anecdotes or gossip, reference County policy #4.506, – must not be sent to multiple recipients nor impede County business. Large attachments, which overload the County server and thereby hinder legitimate County communications, should not be sent. Employees should, upon receiving a personal message, read or listen to the message and permanently delete it in a timely manner.

Brief and occasional access to the Internet for personal purposes is permitted as long as the sites visited meet the Subject Matter conditions above, do not interfere with County work and are not prohibited by law or departmental policy. Excessive use of internet sites such as but not limited to social media, streaming audio and video can cause strain on our limited bandwidth which could impact County business negatively, unless approved by department or division head.

Music files, pictures and videos unrelated to County business cannot be stored on servers, computers and County owned devices and are subject to removal without notice.

County printers, printing commodities and paper are not for personal use.

3.5.3 **Security.** While DITSS provides a broad array of electronic security, everyone has an obligation to protect County technology and information by adhering to good security practices that limit the threat of unauthorized use, disclosure, modification, destruction or abuse. Sedgwick County DITSS will leverage the principle of least privilege, promoting minimal privileges on computers and technology systems, based on business necessity.

Departments are responsible for restricting access to equipment. This includes materials that have become "waste." Where necessary, coverings are be used to protect equipment from environmental factors. (Public access, tampering, water, excessive dust or heat).

All software and files obtained from non-Sedgwick County sources must be screened with malicious software detection systems prior to being used. Check with DITSS

before downloading software and note that software will only be installed by DITSS or their authorized agents (and all non-standard software must be approved by the appropriate DITSS resource – contact Helpdesk for more information). Adhere to copyright laws and licensing agreements, and be aware that non-business websites, screen savers, wallpaper, and other such files often contain malicious software that will infect computers and networks. File downloads should only occur for County business purposes.

All suspected information security incidents must be reported to the Customer Support Center (Helpdesk) upon discovery. Such incidents include unauthorized release of Personal Health Information or Social Security Numbers, stolen devices and lost or stolen media (CDs, DVDs, memory drives, etc.) containing sensitive information.

3.5.4 Authorization. Accessing information without authorization is prohibited. This includes, but is not limited to, another person's electronic communication, information on the public drive where the individual is not the intended audience, reports printed for others and data stored in County applications. Employees should understand which accesses they need for their job and should notify the appropriate security administrator when they become aware that a mistake in authorization or an unapproved information disclosure has occurred. Each department will have a departmental security administrator, who is the elected official, department head, or division director responsible for that area, or an individual designated by that person.

All internal and external connections to the Sedgwick County Network shall be approved by DITSS. No one shall attempt to gain access to systems without proper authorization or use hardware or software tools on the Network that could be used to evaluate or compromise security.

Everyone is responsible for activity performed with their credentials (user ID, password, soft token) and is prohibited from performing unauthorized activity with someone else's credentials. Sharing of userid and passwords with anyone is strictly prohibited.

Access to department information is controlled by the responsible department's security administrator. Requests for access should be made to the security administrator or department head.

3.5.5 Audits. While the County does not systematically monitor or inspect Internet activity or the contents of electronic, voice mail or other data stored on County systems, DITSS may be asked to do so in accordance with the Suspected Activity section below or pursuant to a KORA request, subpoena or other legitimate request for information. Also, law enforcement officials may examine data stored on County information technology in the course of an investigation of criminal activity.

3.5.6 Privacy. No one should expect a right to privacy when using County information technology. Without his/her knowledge, DITSS may allow access to an individual's (1) electronic or voice messages, (2) addresses accessed on the Internet, and (3) data

stored on County information technology as set forth herein.. Staff in or contractors of DITSS may not access or allow access to such information unless specifically authorized by the Chief Information Officer or IT Infrastructure Director.

3.5.7 **Enforcement.** Management within Sedgwick County departments and divisions is responsible for communicating and enforcing this policy. All employees shall have read and signed the Sedgwick County Acceptable Use Agreement for Information Technology, and completed the yearly Security Awareness Training per procedure 3.000-P. No one should receive access to the Internet, electronic or voice mail or other County information technology until he/she has signed the Sedgwick County Acceptable use Agreement which shall be retained by the respective departments and the Human Resources Department.

DITSS shall administer this policy and provide assistance, procedures or forms when needed.

4 Definitions

Electronic Communications – communication by means of computer transmitted signals such as, but not limited to e-mail (electronic mail), instant messaging, and other telecommunication messaging.

Principle of Least Privilege - the practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.

HIPAA - Health Insurance Portability and Accountability Act of 1996 is United States legislation that provides data privacy and security provisions for safeguarding medical information.

PCI-DSS - Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

CJIS - The Criminal Justice Information Services Division (CJIS) is a division of the United States Federal Bureau of Investigation (FBI). The CJIS was established in February 1992 and it is the largest division in the FBI.

5 Procedures

5.1 Authorization.

5.1.1 Employees must sign the "Sedgwick County Acceptable Use Agreement For Information Technology" before authorization to access County information technology will be granted.

5.1.2 Individuals who are not County employees must sign the County's Non-Employee IT Usage Agreement before authorization to access County information technology will be granted.

5.1.3 Through the request from a Security administrator using the Personnel Action Form (PAF) or Security Access Request (SAR) access to the Sedgwick County networks will be removed.

5.1.3.1 Per County policy 4.500, supervisors may relieve an employee of his/her duties with pay or suspend the employee without pay during the administrative investigation of circumstances related to the proposed dismissal of the employee and as such may request immediate restriction of computer access to protect Sedgwick County data assets.

5.1.3.2 Once the request is received, DITSS staff will perform searches for the first and last name to remove the accounts. Actions taken will be to immediately restrict and cease any access to the Sedgwick County network.

5.2 Maintenance Windows.

DITSS will perform its regular monthly maintenance program Saturday mornings starting at 6am and concluding by noon. This monthly maintenance program, also known as "Tech Weekends" are essential to providing stable and secure systems to the County.

5.2.1.1 Notification schedules will be posted yearly for the weekends scheduled for Tech Weekend maintenance windows to allow customer department planning. Interested parties and key stakeholders will be notified of planned work the Wednesday prior to the scheduled Saturday morning maintenance windows.

5.2.1.2 There are some times where impacts will last the duration as the maintenance is scheduled for a 6 hour time period, interruption to customers generally is minimal through system reboots and patching.

5.3 Subscriber Access to Information.

On-line access to data files of the Appraiser's Office and Eighteenth Judicial District Court residing on Sedgwick County computer systems may be available to subscribers.

5.3.1.1 Requests for subscription shall be made to DITSS. The potential subscriber will be required to properly execute a standard service contract. Any deviations to the standard service contract must be approved by the Legal Department.

5.3.1.2 Subscribers with access to computer applications may be granted access to additional functions by requesting access from the elected official, division director, or department head responsible for maintaining the information, or a designated representative.

5.4 Employee Leave Access.

The Director of a department may make a request to view or gain access to an individual's email account or U drives due to termination, leave or extensive leave situations. To make the request, a Director or Deputy Director can put in the request to Helpdesk in writing and it will then be passed to the Infrastructure Director or Chief Information officer for approval.

5.5 Suspected Activity.

In the event that an employee is suspected of violation of a county policy (including but not limited to inappropriate use of information technology) or of any other workplace or personnel policy or of commission of a crime, a Department head in the employee's Department may contact the Chief Information Officer or IT Infrastructure Director to request access to the employee's electronic information, giving as much information as possible in regard to the suspected inappropriate usage, including, date, time, etc. Requests to DITSS must be made in a timely manner; otherwise, relevant information may be impossible to obtain.

5.5.1 Upon receipt of the request for access, the Chief Information Officer or IT Infrastructure Director will present the requested information back to the requestor department with inclusion of Human Resources and Legal department heads or designee on all communication.