THIRD JUDICIAL DISTRICT
Administrative Order No. 2017-103

An Administrative Order to Adopt an Intern/Law Clerk Confidentiality Policy

1. The 3rd Judicial District of Kansas is a single county district located in Shawnee County, Kansas.
2. From time to time, this Court enters into agreements with law schools whereby students earn school credit by working with our Judges and other court personnel in return for school credit. These Student Interns are generally supervised by an assigned Judge.
3. From time to time, this Court retains law students to perform research and writing projects, and other duties as assigned. These Law Clerks are generally supervised by the Court's Staff Attorney.
4. It is advisable for this Court to adopt a formal policy to set forth the Court's understanding and expectations with these students, who are performing important functions with the Court.
5. The attached Policy is hereby adopted by the 3rd Judicial District of Kansas.
6. The attached Confidentiality Agreement, Authority for Release of Information, and Technology Security Policy forms shall be executed by each Intern and Law Clerk who performs the above-referenced functions for this Court.
7. This Administrative Order shall be effective on and after the date executed by the Chief Judge.

BY ORDER OF THE CHIEF JUDGE OF THE THIRD JUDICIAL DISTRICT OF KANSAS this 26 day of May, 2017.

Evelyn Z. Wilson
Chief Judge, Third Judicial District

FILED BY CLERK
KS. DISTRICT COURT
THIRD JUDICIAL DIST.
TOPEKA, KS
2017 MAY 30 A 9:43

INTERN/EXTERN & LAW CLERK POLICY

A clear and defined process by which a law school student enters service with the Court has never been developed. The following information shall be used to clarify issues of concern and to ensure uniformity:

Definition

- An intern (or extern) is not a Court employee, who has an unpaid, educational opportunity supervised directly by the assigned Judge, or, in limited instances, by the Court's Staff Attorney.

- A Law Clerk is a Court employee with a temporary paid position supervised by the Court's Staff Attorney.

Administrative Process

- A Judge who selects a law student to work as an intern in Chambers shall provide the successful intern candidate's name to the Court Administrator by email and direct said student to the Court Administrator's Office for administrative processing.

- Law Clerks shall be hired no more frequently than once a year, with an expected term of at least one year. The Staff Attorney shall submit a job posting to the Symplicity systems of both the University of Kansas School of Law and the Washburn School of Law, with the intent to hire for the following year's Law Clerk pool, by no later than January 1 of any given year. The Staff Attorney and such Judges as may be interested shall review any applications for these positions and shall extend interview invitations at their discretion. Upon completion of the interview process, the Staff Attorney shall extend offers of employment to the chosen candidates.

- Upon receiving written confirmation that a candidate has accepted the position of Law Clerk for the following academic year, the Staff Attorney shall provide the names of the hired candidates to the Court Administrator by email and direct said student to the Court Administrator's Office for administrative processing.

- Each Intern and Law Clerk shall complete the Court's Release of Information form no less than ten (10) business days prior to their proposed start date. A criminal background check will be conducted by the Court Services Department and the results will be forwarded to the Court Administrator. Should the report identify prior criminal history, the Court Administrator will submit the findings to the Chief Judge for further review or decision.

- Each Intern and Law Clerk shall sign a "confidentiality agreement" noting that they are prohibited from disseminating or disclosing any information they come into contact with during the course of their work, are prohibited from speaking to the media and may not remove any court file, equipment or other County or State property from the courthouse, subject to the limited exceptions set forth in said confidentiality agreement.

- Each intern and law clerk shall be entered into the Court's Personnel system noting their specific position and location.

Technology Equipment & Support

- Both classifications will be provided access to a desktop computer and network printer.
- Both classifications are expected to provide their own mobile devices.
- The IT Department will not render technical support to electronic equipment owned by either classification.
- The Court's IT Department will not provide mobile devices, fax, scanners or other hardware/software to an intern.
- Both classifications will have access to the Court's Wi-Fi.
- Both classifications shall be provided with access to the Court's network, email system, and online document retrieval system.
- West law access will be the responsibility of each individual.
- Case information is available via the Court's public access website only.

Office Space & Furniture

- Interns shall use existing space and furniture in the Chamber in which they are working.
- Law Clerks shall be assigned a cubicle in the Research Library.

Telephone

- Law Clerks shall have access to a telephone already installed in the Law Library.
- Interns will not have a dedicated telephone line established for their use.

ID Badge

- A Shawnee County issued Courthouse ID badge will only be issued to Law Clerks. This is a paid position which provides 24/7 access to the courthouse and law library. Interns do not have 24/7 access because they are dependent upon the Chambers being open in order to perform their work. The Staff Attorney is responsible for collecting the Law Clerk's ID badge upon separation from the Court.

E-Mail & Data Access

- Interns and Law Clerks will be given temporary access to the court's online document retrieval.
- Both classifications will receive a temporary court sponsored email account.
- Unless otherwise directed by their assigned Judge or the Staff Attorney, each Law Clerk and Intern's work product shall be saved in the Court's Law Library Shared Network Drive for future reference.

Keys

- The Staff Attorney shall provide each Law Clerk with a copy of key #626, which will allow access to the Research Library. The door to the Research Library must remain locked at all times, unless at least one Law Clerk and/or the Staff Attorney are present. Only personnel employed by the Court—outside of those contracted as panel counsel—may have access to the Research Library. The Staff Attorney is responsible for collecting the Law Clerk's #626 key upon separation from the Court.
- Interns will not be issued keys to chambers, offices or any other locking mechanism.

Parking

- The Court does not provide free, assigned parking spaces or subsidize the cost in full or part for either a Law Clerk or Intern with the sole exception of the first day a Law Clerk or Intern reports to the Court, in which case they shall be provided with a parking voucher for the Park-N-Shop garage.
- Parking passes may be purchased for $10.00 (refundable upon separation) from the Shawnee County Clerk's Office in order to gain access to the lot located at the NE corner of 6th Street & Monroe.

Courthouse Access

- Law Clerks may use either the public entrance or the employee entrance during normal work hours. The employee entrance must be used after normal business hours, weekends or holidays. Law Clerks must sign in and follow established security policies.

- Interns may only use the public entrance during normal operating hours.

Security

- Interns and Law Clerks are not exempt from passing through the security checkpoints at the public or employee entrance. Both classifications must adhere to established security policies.

Confidentiality Agreement

I, _____, have accepted a position as a judicial law clerk / intern (circle one), for the Third Judicial District Court of Kansas ("the Court"), beginning effective _____, 20__.

In order to perform my duties for the Court, I will be granted access to certain confidential information. As used in this Confidentiality Agreement, "confidential information" means information means information received in the course of judicial duties that is not public and is not authorized to be made public. Examples of confidential information include, but are not limited to:

(a) Information received by the Court pursuant to a protective order or under seal

(b) The substance of draft opinions or decisions

(c) Internal memoranda, in draft or final form, prepared in connection with matters before the Court

(d) The content or occurrence of conversations among judges or between a judge and judicial employees concerning matters before the Court

(e) If working with a panel of judges, the authorship of per curiam opinions or orders

(f) The timing of a decision, order, or other judicial action, including the status of or progress on a judicial action not yet finalized

(g) Views expressed by a judge either in casual conversation or in the course of discussions about a particular matter before the Court

(h) Any subject matter the appointing authority has indicated should not be revealed, such as internal office practices, informal court procedures, the content or occurrence of statements or conversations, and actions by a judge or staff

(i) Any matter on which you have been, are, or will be working as a judicial law clerk / intern (circle one)

Information that is not considered confidential includes court rules, published court procedures, public court records including the case docket, and information disclosed in public court documents or proceedings. However, I will not disclose or make public or private statements about the merits or decision making process concerning past, pending, or future cases, even if those statements entail the use of only non-confidential materials. For purposes of the ongoing responsibilities outlines later in this Confidentiality Agreement, "future cases" refers only to cases that arise between the date of this Confidentiality Agreement and the end of my term as a judicial law clerk / intern (circle one).

I will be required to communicate with the judges and the judges' staff that comprise the Court. This Confidentiality Agreement serves as a memorialization of my responsibilities with respect to this confidential material. I have placed my initials beside each of the following acknowledgments to confirm that I understand and accept the representations contained therein:

____ I promise to exercise a reasonable degree of care in order to prevent the disclosure of confidential information pertaining to cases from the time in which I served as a judicial law clerk / intern (circle one), which extends from _____, 20___, to _____, 20___.

____ I promise never to remove original copies of any Court files from the courthouse premises.

____ I promise to maintain any confidential information in my custody in accordance with the Court's Technology Security Policy and, if I am a judicial law clerk working from home, with the Working from Home: Procedures and Policies document. I acknowledge that I have been provided with a copy of both documents and have signed both documents.

____ I promise never to discuss the specifics of my case assignments with anyone outside the employment of the Third Judicial District, as this constitutes confidential information. Nevertheless, I may generally discuss the nature of my duties here and the kinds of cases I worked on in the course of my employment with the Court, subject to the limitations enunciated in the definition of "confidential information," *supra*.

____ I acknowledge that the work product I generate in the course of my employment with Court is the sole property of the Court. I promise never to share my work product with anyone outside of the Court's employment without first obtaining specific written permission from the judge for whom the work product was originally created.

____ I promise never to make statements, in generally discussing my work for the Court, that impugn the character or integrity of the judiciary as a whole or any particular judge or staff member thereof, except as required by law. (*E.g.*, I promise never to claim to have "written" a particular final order or opinion.)

____ I acknowledge that I may only release confidential information in the following limited circumstances:

(a) Pursuant to a statute, rule, or order of the Court,

(b) Pursuant to a valid subpoena issued by a court or other competent body;

(c) To report an alleged criminal violation to the appointing authority or other appropriate government or law enforcement officials;

(d) In the case of a written work product to be used as a writing sample, with the explicit written permission of the assigning judge.

I further acknowledge that all other releases of confidential information are prohibited.

____ I acknowledge that the responsibilities contained in this Confidentiality Agreement do not end at the conclusion of my term as a judicial law clerk / intern (circle one), but, instead, constitute an ongoing responsibility. I further promise to abide by the terms of this Confidentiality Agreement, as it relates to my time working for the Court, in perpetuity.

WHEREFORE, in memorialization of the above, I put my hand to this statement as an acknowledgement that I have read it, understand it, and agree to abide by it, with the understanding that my failure to do so may result in the termination of my employment with the Court or in further disciplinary action.

_____ _____

Signature Date

_____

Name (Print)

AUTHORITY FOR RELEASE OF INFORMATION

I AUTHORIZE any duly accredited representative of the Third Judicial District, including those from Personnel Management, or any other Court Management, to obtain any information relating to my activities from schools, residential management agents, employers, criminal justice agencies, financial or lending institutions, credit bureaus, consumer reporting agencies, retail business establishments, medical institutions, hospitals or repositories of medical records, or individuals. This information may include, but is not limited to, my academic, residential, achievement, performance, attendance, personal history, disciplinary, criminal history record, arrest, conviction (to include expunged records), medical, psychiatric/psychological, and financial and credit information.

I FURTHER AUTHORIZE the Third Judicial District to request criminal history record information about me from criminal justice agencies for the purpose of determining my eligibility for access to classified information, or assignment to, or retention in, sensitive duties.

I DIRECT YOU TO RELEASE such information upon request of the duly accredited representative of any authorized agency regardless of any agreement I may have made with you previously to the contrary.

I UNDERSTAND that the information you release is for official use by the Third Judicial District, and that these users may redisclose the information you release as authorized by law.

I RELEASE any individual, including records custodians, from all liability for damages that may result to me on account of compliance or any attempts to comply with this authorization. This release is binding, now and in the future, on my heirs, assigns, associates, and personal representative (so of any nature.)

Copies of this authorization that show my signature are as valid as the original release signed by me.

I UNDERSTAND the information received from this background investigation may effect my consideration for employment.

I HAVE READ and understand this authorization to release information and sign it voluntarily.

Signature (Sign in ink) / Date Full Name:

Date of Birth:

Other Names Used:Social Security Number

[ ]-[ ]-[ ]

Current Address:Telephone Number

( ) _____-_____

Drivers License #: _____

Third Judicial District
Confidentiality and Acceptable Use Policy
Dated: 11/18/2016

The purpose of this policy is to outline confidentiality and acceptable use of technology resources within the Third Judicial District (Court). This policy is in place to protect judges, staff and the public that the Court serves. Inappropriate use of Court's confidential information and technology resources exposes the Court to unnecessary risks including security breaches, information degradation, data compromises, cyber-attacks, and corrupt systems. This policy applies to all staff including: employees, judges, contractors, consultants, temporary employees, interns, externs, volunteers, and other workers assigned to the Court.

Confidentiality

Working at the Court means having access to information regarded as confidential. Types of confidential information relate to a variety of people including, but not limited to: children, victims, judges, court staff and parties involved in a case. It is the responsibility of individual staff to safeguard confidential information.

Examples of Confidential Information

- Matters involving Child in Need of Care, Juveniles, Adoptions, and Mental Health.
- Personal information regarding judges, probation officers, or other staff including hobbies, interests, family members and whereabouts when outside the courthouse facilities.
- Personal information such as social security numbers, dates of birth, addresses or telephone numbers of case participants.

Various materials containing confidential information

- Information known by individuals
- Digital records
- Telephone calls
- Meetings
- Fax
- Internet and Intranet
- Hard copy records (paper files)
- Written reports/agendas/minutes/file notes
- Letters, memos, telephone messages
- Face-to-face conversations
- Email

If staff members are unsure whether information should be shared, they should seek advice from their supervisor or department head.

Routine Handling of Confidential Information

- Materials containing confidential information shall not be left out in the open.
- Confidential data shall not be left exposed on the user's PC when unattended. PCs shall be locked and displaying a screensaver when left unattended.
- Computer files should be kept securely on the Court's network drives.
- No confidential information shall be kept on portable storage devices such as USB drives, tablets, or smart phones.
- Personnel information shall only be accessed by the Court Administrator, Chief Judge, and personnel staff.

Communicating with third parties

- Court staff shall not make any public or nonpublic statement that might interfere with matters pending with the Court.
- Court staff shall not make pledges, promises, or commitments that might interfere with the adjudicative duties of a judicial office.
- Staff shall not discuss specific or sensitive matters of the Court.
- Staff should have regard to the harm which may be done by sharing information relating to pending cases or other staff in social conversations within the Court.

Technology Resources

Computer Equipment is provided to staff so that they may perform required duties and functions. Equipment shall be maintained with care and respect to resources.

Staff shall not save any personal documents, programs, photos, images, or other non-authorized software or files to the computer's local hard drive, or to any network drives.

Staff is highly discouraged from saving or retrieving files or programs from any form of portable storage devices such as CDs, DVDs, USB drives, personal handheld devices such as smart phones and tablets.

Network and System Access is provided to each user based upon the duties and functions of the staff member.

All staff passwords must be changed every ninety (90) days. Passwords may not be repeated for at least twelve (12) months. Passwords shall not be divulged to any person under any circumstances.

Email is provided to facilitate the communication within the Court as well as between County, agencies, organizations and individuals with which the Court has business.

- All messages communicated via Email shall have the senders name attached. Users shall not attempt to obscure the origin of any message.
- Messages should be directed to the proper recipients. Broadcast messages shall be sent only to those who need to receive the information.
- Supervisors may request access to staff's Email when staff may be out for an extended period of time. This will only occur with the department head's and the Court Administrator's explicit permission.
- Email accounts must be regularly monitored. The Court archives all email 6 months or older.

Internet access is provided to staff so that they may perform job tasks, research topics related to their work, and assist in increasing job knowledge and functions.

Personal Handheld device connections are issued to limited court users such as supervisors, department heads, judges, court reporters and administrative assistants. A separate BYOD Policy is necessary for this access.

Prohibited Activities include, but are not limited to:

- Transmission of harassing, threatening, rude, or obscene material.
- Transmission of material that creates an intimidating, hostile or offensive environment or that discriminates on the basis of sex, race, color, religion, sexual orientation, age, national origin, ancestry or disability.
- Transmission of any material that is slanderous, defamatory, fraudulent, sexually oriented or derogatory.
- Sending documents or files in violation of copyright laws.
- Radio or Video Streaming except for use in official Court business.
- Use of Court equipment to create or distribute viruses, worms, Trojan, or ransomware.
- Unauthorized entry or attempts to hack into secured network drives, software applications or servers.
- Unauthorized use of encryption technology.
- Installation of any third party software and/or hardware not owned or approved by the Court Administrator.

Personal and Non-business Use

Any personal use of the Court's technology resources shall adhere to the above guidelines. Such usage shall be limited to a reasonable time period, and shall not interfere with Court business or duties.

Personal Devices

The Department of Court Technology is not responsible and does not support any personal devices and is not available to help users with any non-Court business use issues; such as problems with personal smart phones, tablets, laptops, or releasing personal Email caught in the Court Email filters.

Blocked Websites and Attachments

The Court may utilize Email and web filtering applications to block website categories and file attachment types such as:

- Adult/Sexually Explicit
- Chat
- Games
- Hacking
- Streaming Radio
- Glamour and Intimate Apparel
- Para mutual and Gambling
- Personals and Dating
- Remote Proxies
- Social Media such as Facebook, SnapChat, Pintrest
- Email attachments known to have viruses such as .bat, .exe, .dll, .js, .zip

If staff requires access to a blocked website and/or a particular file, the staff shall complete a *Request to Circumvent Filtered File/Website* form and deliver the form to the Court Administrator for approval and implementation. This form is to be published on the Court's Intranet website for all Court staff.

The Department of Court Technology, only with the express written permission of the Court Administrator and Chief Judge, may review a user's computer activity including his or her Email to ensure that the user is in compliance with these guidelines. The Chief Judge will provide written

notice to the user that such a review has occurred or will occur. The notice may be provided either before or after the review occurs, in the discretion of the Chief Judge.

Violations of these guidelines and policies may result in restrictions, or the revocation of staff's access, as well as other disciplinary action, including but not limited to termination of employment as stated in the Kansas Court Personnel Rules or prosecution per State and Federal law.

Any breach of this agreement, accidental or otherwise, or any loss of confidential information shall be immediately reported to the Court Administrator, Director of Court Technology or the Chief Judge.

Approved:

Evelyn Z. Wilson
Chief Judge
December 22, 2016

ACKNOWLEDGEMENT

I understand that in fulfilling my assigned responsibilities, I may be granted access to certain confidential information in connection with my duties with the Court.

I hereby acknowledge the need for maintaining the strictest confidentiality of the Court's information and data. I have read the above document and will adhere to the stated requirements to the best of my ability.

I understand that if I fail to secure confidential information and data under my control, my access may be restricted, revoked, or I may face disciplinary action, including but not limited to termination of employment as stated in the Kansas Court Personnel Rules or prosecution per State and Federal laws.

I further understand that I remain subject to the provisions of the Confidentiality and Acceptable Use policy during my employment and continuing after my separation from employment with the Court.

Date: _____, 20____.

Name: _____ Position: _____

Signature: _____ Department: _____

Third Judicial District

Technology Security Policy

November 18, 2016

12/22/2016

Table of Contents

Introduction

The Third Judicial District (Court) considers data and technology assets to be an indispensable resources to the Court and must be adequately protected. For this reason the Court has created and adopted the Technology Security Policy (Policy). Contained in this document are policies and guidelines to insure that the Court's data and technology assets are adequately protected.

Data is a Court asset requiring protection commensurate with its value. Measures must be taken to protect data and technology resources from unauthorized access, modifications, destruction, or disclosure whether accidental or intentional, as well as to assure its authenticity, integrity, availability, and confidentiality.

For the purpose of this Security Policy, technology assets includes all Court owned computers, peripherals and related equipment and software; data communications infrastructure, peripherals, and related equipment and software; all other associated tools, instruments, and facilities; and the service that makes use of any of these technology resources. The components may be individually controlled (i.e. assigned to a user) or shared in a single-user or multi-user manner; they may be stand-alone or networked; and they may be stationary or mobile.

Scope

This policy applies to judicial and non-judicial employees, agents, associates, representatives, interns, contractors, consultants, temporary employees, auditors, assignees, vendors or any other designates involved in the consulting, development, implementation, maintenance and use of the Court's data and technology assets.

Compliance

All Court employees, agents, associates, representatives, interns, externs, volunteers, contractors, consultants, temporary employees, assignees, other designates, and vendors are responsible for understanding and complying with all security policies; including the Confidentiality and Acceptable User Policy. Non-compliant situations will be brought to the attention of the Chief Judge and Court Administrator for appropriate action. Violations of these guidelines and policies may result in restrictions, or the revocation of the employee's access, as well as other disciplinary action, including but not limited to termination of employment as stated in the Kansas Court Personnel Rules or prosecution per state and federal law.

Outsourced services must be monitored and reviewed to ensure compliance with Court security policies, and all applicable state and federal laws. This should be accomplished through contractual commitments with provisions to permit internal and external auditing and monitoring to ensure compliance. All necessary exceptions to this policy must be clearly documented and approved by the Chief Judge or the designee of the Chief Judge.

Confidentiality and Acceptable Use Policy

All employees, both judicial and non-judicial, are required to complete and sign the Confidentiality and Acceptable Use Policy indicating that they have read, understand, and abide by the policy. This form will be stored in the employee's personnel file or applicable judicial record. Failure to sign the Confidentiality and Acceptable User Policy may result in the disconnection of the employee's (both judicial and non-judicial) access, and other disciplinary action as stated in the Kansas Court Personnel Rules.

Organizational Roles & Responsibilities

Data security requires the active support and ongoing participation of all Court employees, both judicial and non-judicial. In order to avoid confusion and to have a clear chain of command, the Court has set forth the following roles

and defined each role's corresponding responsibilities. Wherever possible, the Court has attempted to uphold the concept of "separation of duties," but because of the Court's size, some overlap will occur.

Separation of Duties is the practice of dividing the steps in a system to function among different personnel, so as to keep a single individual from subverting the process.

Data and Application Owners

Data and Application Owner is the personnel that can authorize or deny access to certain data, and is responsible for its accuracy, integrity and timeliness and also has the responsibility to ensure that the program(s) which make up the application to accomplish the specified objective of the Court. A Data and Application Owner holds the ultimate responsibility for a specific system, application and access therein.

Data and Application Owners shall assess the risk to the integrity, confidentiality, and availability of information systems and resources under their control.

Data and Application Owners within the Court are defined as follows:

Primary:	Chief Judge
Secondary:	District Court Judges
	Court Administrator
	Clerk of the District Court
	Chief Court Services Officer

Each of the aforementioned Data and Application Owner is responsible for and are authorized to grant access to Data and applications under their control. Each Data and Application Owner is to determine the value and sensitivity of the Data they control. Appropriate internal control measures shall be implemented to reduce risk to the integrity, confidentiality, and access to the Court's Data.

Court Administrator

The Court Administrator working in conjunction with the Director of Court Technology, shall have the goal to direct the Court's staff to assure confidentiality, integrity, and availability of the Court's Data and technology assets.

The Court Administrator's responsibilities include the following:

- Ensuring that Court Technology positions have job descriptions that accurately reflect appropriately segregated duties and responsibilities
- Determine any necessary security clearances for individuals working with sensitive and/or confidential data
- Conduct background checks as necessary for individuals in positions with sensitive job duties
- Establish appropriate division among several individuals for any highly secure functions
- Establish hiring, transfer, and termination procedures to promptly establish, modify, and close out security access
- Documenting that all employees sign the Confidentiality and Acceptable Use Policy.
- Require that Court Technology staff take regularly scheduled vacations
- Promptly enforce the Kansas Court Personnel Rules for any significant security violations
- Maintain staff records for mandatory annual Security Awareness training.

Director of Court Technology

The Director of Court Technology working in conjunction with the Court Administrator shall have the goal to assure confidentiality, integrity, and availability of the Court's Data and technology assets.

The Director of Court Technology shall be assigned the following responsibilities:

- Develop and maintain the Court's Security Policy, and Confidentiality and Acceptable Use Policy.
- Ensure that appropriate hardware and software security measures are in place to protect the Court's data and technology assets.
- Administer access to the Court's Data and technology assets.

- Assume responsibility for the operating, supporting, and managing of information systems and networks in accordance with the Court's Security Policy and direction from the Court Administrator and Chief Judge.
- Managing and protect access to the Court's Data for the Data and Application Owner.
- Implement security controls as specified by the Data and Application Owners
- Detect, analyze, and report unauthorized attempts to gain access to data and technology resources or inadvertent exposure due to mistake or loss of information.
- Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the Court's Data and technology assets.
- Ensure systems are backed up and have the ability to be recovered in a secure manner
- Perform ad hoc system reviews are performed to identify unusual activity and monitor resources for signs of security violations
- Conduct Security Awareness training on an annual basis
- Assume full responsibility for the design, development, organization, management, and control of the Courts databases in accordance with Security Policy and direction from the Court Administrator and Chief Judge.
- Ensuring systems and network architectures maximize security of the Court's technology assets
- Ensure that network security does not conflict with application security
- Audit the Court's information systems and applications annually to assure systems, both virtual and physical, are in compliance with this policy.
- Maintain an inventory of the Court's technology assets
- Identify and analyze threats to the critical information assets to determine the likelihood of their occurrence and their potential to harm to the Court.

Users

Users are all staff who use Court Data and court technology assets for court business. This means that the User must protect Court Data and technology assets from unauthorized access and activities including disclosure, modification, deletion, and usage.

Users have the responsibility to:

- Use Court Data and technology assets only for the purpose specified by the Data and Application Owners
- Comply with controls established by the Data and Application Owner or public law
- Prevent disclosure of sensitive information
- Comply with the Court's Confidentiality and Acceptable Use Policy
- Receive Security Awareness training on an annual basis

Third Party Relationships

In order to efficiently conduct its business, the Court must allow for third party relationships such as state agencies, vendors, consultants and other justice partners. When this need arises, the Court will enter into a contract or a memorandum of understanding with the third party.

Such documents will take into consideration the following:

- Purpose of the relationship
- Define the level of restricted access to data and other technology assets.
- Confidentiality of Court data.
- How the data will be transmitted (when applicable)
- How the data will be disposed (when applicable)
- Reserve the right to inspect vendors' security measures and pre-approve all sites or facilities.

Security Incidents

Reporting Security Incidents

A security incident is defined as a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of Court data or technology assets; interference with court technology operations; or significant violation of the Court's Confidentiality and Acceptable Use Policy. All suspected information security incidents shall be reported to the Director of Court Technology, Court Administrator and/or the Chief Judge as quickly as possible. The Director of Court Technology shall investigate, research, resolve, and document the event. If the event is serious enough, the Court may report the incident to the appropriate authorities for prosecution.

Examples of Security Incidents

- Computer system intrusion
- Unauthorized or inappropriate disclosure of sensitive institutional data
- Suspected or actual breaches, compromises, or other unauthorized access to U-M systems, data, applications, or accounts
- Unauthorized changes to computers or software
- Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USB drive, personally owned device used for university work) used to store private or potentially sensitive information
- Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, or applications
- Interference with the intended use or inappropriate or improper usage of information technology resources.
- While the above definition includes numerous types of incidents, the requirement for security incident reporting, regardless of malicious or accidental origin, is limited to serious incidents as defined below.
- Occurrences such as incidental access by employees or other trusted persons where no harm is likely to result will usually not be considered information security incidents.
- A serious incident is an incident that may pose a substantial threat to Court resources. An incident is designated as serious if it meets one or more of the following criteria:
- Involves potential, accidental, or other unauthorized access or disclosure of confidential information as defined by the Confidentiality and Acceptable User Policy
- May cause severe disruption to mission critical services
- Involves active threats
- Is widespread
- Is likely to be of public interest
- Is likely to cause reputational harm to the Court

Responding to Security Incident Reporting

All employees are responsible for maintaining the security of the Court, the Court's Data, and Technology Resources. As a result, when an employee observes a security breach they should take steps to correct it as soon as it is discovered. Employees are not to put themselves at risk, but should still take steps to neutralize the security breach.

The following steps should be taken when a security breach is identified:

- Neutralize the breach. For example, disconnect an infected PC from the network.
- Report the incident to your supervisor, department head, Court Administrator, or Chief Judge.
- The supervisor, department head, Court Administrator, or Chief Judge will then report the incident issue to the Director of Court Technology.
- If not already done so, the Director of Court Technology will report the incident to the Court Administrator and Chief Judge.
- The Director of Court Technology will investigate and take steps the necessary steps to correct the issue.
- The Director of Court Technology will then report the results of the investigation to the Chief Judge, Court Administrator and the department head as to the results of their investigation.
- The Director of Court Technology will maintain records of all security breaches.

All persons involved should record as much information as they can about the incident, to aid in the Court's investigation into the issue.

Information should include the following:

- Date and time of the event
- Description of the event
- Parties, Systems, and or equipment involved in the event
- Steps the party took, etc.
- Supervisors and Court managers shall assure that no retribution takes place toward the employee that reported the incident, so as not to discourage others from reporting incidents that they observe.

Data and Technology Asset Security

Protecting the Court's technology assets involves many issues and requires a systemic approach to ensure all aspects are considered into the overall plan.

Availability of Critical Data and Systems

COOP (Continuity of Operations Plan) – COOP planning is an effort to assure that the capability exists to continue essential agency functions across a wide range of potential emergencies.

The objectives of a COOP plan include:

- Ensuring the continuous performance of an agency's essential functions/operations during an emergency
- Protecting essential facilities, equipment, records and other Court assets
- Reducing or mitigating disruptions to operations
- Reducing loss of life, minimizing damage and losses
- Achieving a timely and orderly recovery from an emergency and resumption of full service to Court stakeholders.

The Court is mandated by the Office of Judicial Administration (OJA) to have a Continuation of Operation Plan (COOP) that includes procedures necessary to assure the continuation of vital Court operations in the event of a disaster. Each department within the Court must identify and prioritize its processes in the COOP.

The COOP must outline the internal policies and procedures that are to be employed should a disaster occur. Preparation of the recovery strategies for all time-sensitive processes must be coordinated with the Chief Judge. In the event of a disaster all time-sensitive services, systems and applications must be restored and available on a priority basis to maintain vital Court operations.

Time-sensitive applications include those systems whose loss or unavailability is unacceptable for citizens of the Third Judicial District as well as the State of Kansas as a whole. The loss or unavailability of support services provided to these applications may adversely affect the continuation of vital programs and services or the fiscal or legal integrity of the Court's operations.

Physical Security

Physical Security involves the protection of the physical technology assets or hardware as well as controlling access to such hardware.

The following practices must be adopted in order to maintain adequate physical security within the Court offices:

All servers and other sensitive pieces of hardware will be kept in the designated computer room that is locked and monitored at all times.

- **The computer room shall have the following physical control measures:**
  - Walls separating the Court Technology computer room from other court staff and public areas of the Shawnee County Courthouse.
  - Twelve (12) inch raised data center floors
  - A key fob system used to control access to the room
  - Only persons whose work requires them to be in the Court Technology computer room on a day-to-day basis shall be granted access.
  - All visitors to the secured computer room facility must sign in on a log sheet
  - Logs of all visitors to the secured computer room will be maintained for a minimum of one year for audit purposes.
  - Electronic key fob system shall be maintained by the Shawnee County Sheriff.
  - The Director of Court Technology in collaboration with the Court Administrator shall be responsible for processing requests for new fobs and removal of old fobs to the Court Technology Department and Computer Room
  - All hub rooms, communications rooms, and wiring closets must be secured, locked and monitored at all times.
  - Laptop computers and other mobile equipment must be kept in secure storage areas and checked out by contacting Court Technology.
  - Laptop computers and other mobile equipment must be password protected and use reasonable care to safeguard such device.

- **Computer Room Environmental Measures**
  - Adequate air handling equipment must be maintained to insure room temperatures are consistent with computer equipment needs. Redundant air handling units provided by Shawnee County are included to accommodate times when the primary equipment is unavailable
  - The area below the raised floor must be thoroughly checked and cleaned on an annual basis to prevent circulation of harmful dust particles by the Court Technology staff.
  - Adequate monitoring equipment must be maintained to track temperature and humidity.
  - Monitoring equipment must be capable of triggering an alarm or notifying Court Technology staff via email and/or text should one of the environmental conditions exceed predetermined thresholds.

- **Fire Suppression Measures**
  - All Court Technology work areas must have hand-held fire extinguishers available in accordance with published fire prevention standards for public access buildings. A licensed extinguisher inspector must check these extinguishers on at least a yearly basis. Fire extinguishers and their inspections shall be provided by Shawnee County.
  - Flammable solutions or materials should be stored in a locked area when not being used.
  - Fire doors shall not to be propped open for any reason.

- **Recommended Safeguards for the raised floor computer room:**
  - Use low flame spread or surface burning materials to reduce the rate at which flame will spread
  - Include dampers and shutters heating and cooling subsystems.
  - Include detection equipment that activate alarms
  - If dry chemical type extinguishing systems, such as Halon

- **Electrical Power Measures**
  - Uninterrupted Power Supply (UPS) systems must be utilized to assure continuous power to systems deemed critical to Court business.
  - Surge protection equipment shall be utilized to protect electronic equipment that might be sensitive to power fluctuations.
  - Maintenance technicians working on or around electronic data processing equipment must wear static electricity eliminating bracelets provided by Court Technology.

User Security

User Security addresses the ability to ensure that the user accessing Data and court technology assets are, in fact, who they say they are, and must present the necessary credentialing information for access through the user's User ID and password.

User IDs must:

- be unique and identify only one individual user
- not be a guest or anonymous account
- have their privileges terminated when they become inactive or dormant after a certain period of inactivity, i.e. 90 days
- use a standard format developed by the Court across all platforms to ensure uniformity
- only be issued after Department of Court Technology receives a properly authorized request through Court Administration, indicating type of access desired
- be immediately disabled by Department of Court Technology when the user's employment is terminated or the user transfers to a position where access is no longer required. The immediate supervisor or manager should initiate removal notification by contacting the Court Administrator or their designee
- be suspended after 3 unsuccessful log on attempts. When this occurs, the user is to contact Court Technology to reset the user account.

Passwords must:

- be individually owned
- be kept confidential
- not be shared with other users, or the public
- be changed whenever disclosure has occurred or may have occurred
- be changed at least every 90 days
- be a minimum of seven characters, contain alphanumeric characters, and where allowed, include special characters.

Passwords shall not:

- Be repeated for at least six cycles of change or one year
- have repeating sequences of letters or numbers
- include names of persons, places, or things that can be closely identified with the user (i.e., spouse, children, or pet names)
- be the same as the user ID
- include words that can be found in a dictionary
- be displayed during the entry process
- be written down and displayed in an obvious place
- be the same for all systems the user accesses
- be stored in any file program, command list, procedure, macro or script where it is susceptible to disclosure or use by anyone other than its owner.

Vendor installed default passwords must be changed immediately after installation. If any vendor requires access to the system, they will be provided temporary passwords that will be changed by Court Technology staff after the vendor has completed their task.

Authentication

Authentication is the process and documentation required to validate the user's claim who he/she is. Authentication can also be a process in which electronic devices validate who they are to one another.
The need for authentication is a response to the need to avoid or reduce the risk that the wrong person will access, use, change, delete or otherwise improperly interact with sensitive data or transactions.

All Court data and technology assets require users to be authenticated. This authentication will be based on a user ID and password combination. The strength of authentication can range from weak to strong. The selection of authentication strength should be based upon the level of risk consequence if security were breached.

Computer systems within the Court must implement authentication functions that are consistent with the level of confidentiality or sensitivity of the information contained on the system. When considering authentication techniques, Court Technology staff in collaboration of the data and application owner, will first determine if the confidentiality and/or criticality of the information processed by the system requires stronger authentication than passwords alone. If so, the Court will then consider other forms of authentication such as PIN, smart cards, digital certificates, or other authentication solutions

Authorization

The Data and Application Owner stipulates what Data and technology asset the user may have access to.

When making the determination, the Data and Application Owners should take into consideration:

- Users should be limited to the minimum rights and privileges to do their jobs
- Individuals may be granted a specific combination of authorities
- Access rules or profiles should be established in a manner that restricts departmental employees from performing incompatible functions or functions beyond their responsibility
- Data and Application Owners with the assistance of Court Technology staff should review users' rights and privileges on an annual basis
- The Director of Court Technology or their designee shall grant the rights and privileges to the applicable system as directed by the Data and Application Owner
- No system shall not require programmer intervention by means of programming for that specific user or 'hard-coding'
- There shall not be any special access available to a programmer that is not provided through standard, approved connections. In other words, "back doors" should not be permitted.

Auditing

The Court will have automatic logging features implemented through each of the operating systems, database toolsets, or court developed applications to log transactions taking place on its computer systems. This logging will allow for the reconstruction and/or review of transactions performed on all systems by users. The files containing the logs will be protected so that users, including Information Technology, cannot change them. These logs will be reviewed regularly by Court Technology staff.

Security Administration Activities

Access to security administration software/systems will be restricted to Court Technology personnel who have security administration duties. Operating system tools, database tools and software products used to administer security on all Court systems will record and report all security administration activity. Court Technology will also provide a means to recover current and historical information about security administration activities in the event of a system failure.

Security administration products and procedures must log all security violations. Resultant log files shall be reviewed by Court Technology personnel who have security administration duties to detect any unusual or inappropriate activity. When any unusual or inappropriate activity is detected the Court Administrator and Chief Judge shall be informed immediately.

Log data will be kept by Court Technology for a minimum of 2 years.

The logging system shall not disclose passwords through its reporting functions.

Procedures must exist to maintain the integrity of access tables within the security enforcement software.

Application Security

The Director of Court Technology in collaboration with the Data and Application Owners shall insure that the security features of applications developed by Court Technology are consistent with the overall security policies detailed in this document.

Network access to an application containing confidential data, and data sharing between applications, shall be as authorized by the Data and Application Owners and shall require a level of authentication to commensurate with the level of data confidentiality.

Applications or other software that is downloaded from the Internet shall not be used for processing confidential information until such software is thoroughly researched and tested by the Director of Court Technology or their designee and approved by the Data and Application Owner to ensure it does not contain malicious code. All research and approvals will be documented. Such documentation shall be kept for two (2) years after the software is no longer utilized.

System Security

The Court deems system security to be the analysis of all operating systems and software used to support the Court's in-house developed application software.

Whether the operating system is mainframe, server, or PC based, or a combination thereof, the staff of the Department of Court Technology should:

- Identify and document system security vulnerabilities
- Install vendor-supplied security upgrades and patches
- Review and change vendor-supplied security parameters
- Assign each staff member their own unique system administrative password
- Immediately remove all access in the event staff leaves the Court
- Utilize security standards for operating systems on servers and workstations
- "Harden" servers based on industry guidelines
- Test all upgrades or releases of software before deploying to production
- Acquire additional security software as needed to maintain a proactive environment
- Install and maintain firewalls and security appliances on a regular basis
- Install intrusion detection/prevention appliances
- Conduct periodic vulnerability scans

Data Security

Data security encompasses protecting the data from unauthorized access whether on the computer system or when transmitted. Data security also encompasses protecting the loss of data through mechanical/electrical failure, viruses, or any other destructive manner.

Data Access

Data is an important asset of the Court and shall be protected by all users by strict adherence to the following policies:

- Guest or anonymous accounts will not be allowed access to Court data.

- Court naming conventions for data sets/files shall be followed to ensure uniformity and to facilitate security access control.
- Court employees shall only access Court data that is necessary to perform their respective job responsibilities.
- Court employees shall safeguard all data labeled as confidential.
- Court employees shall be responsible for removing confidential information from printers or FAX machines as soon as the employee is aware.
- Court employees shall be responsible for securing confidential information prior to leaving their work area for the day.
- Court employees shall not make unauthorized additions, changes, or deletions to any Court data in any form.
- Court employees will defer to the Data and Application Owner regarding any decisions as to the disposition of said data.
- Court employees will use only authorized software and business applications to change, manage, or replicate Court data to allow for security and transaction logging as designed in Court production systems.

Data and System Backup

Data backup, archiving and off-site storage procedures are required to mitigate the risk of losing data. The Court understands that regularly scheduled backups are an integral part of data security. The ultimate responsibility for establishing backup guidelines lies with the Data and Application Owner, in consultation with the Department of Court Technology. Backups of mission critical data must be encrypted and kept off site in a secure location to insure recoverability in the event of a disaster. Backup media must be secured at all times during the transfer to the offsite storage location.

Depending on individual circumstances, backups can be any of the following:

- Complete file/system copies
- Incremental backup copies, which are copies of the changes since the last full backup
- Database recovery logs which track database activity since the last full backup

Data and System Recovery

Recovery procedures will be evaluated, documented and tested annually. All types of data should be included in backup procedures including but not limited to software program libraries, databases, job control libraries and electronic forms of documentation.

Firewall

The following are the Court's policies for the firewall:

- A firewall shall be placed between the Court's network and Internet provider
- All users who require access to the Internet must do so by using Court approved Internet gateways
- Users must not circumvent the firewall by to connect to the Internet
- The firewall shall protect against address spoofing
- The firewall shall not accept traffic on its external interfaces that come from an internal network addresses.
- Anonymous FTP into the Court's network will not be allowed
- The firewall must be configured to be the only host address that is visible to the outside network
- The firewall will enforce service rules to protect the identity of all Court sub-networks and users
- All external to internal electronic transactions shall go through the firewall rule base
- Firewall rules will take external requests, examine them, and forward legitimate requests to the internal host that provides the appropriated service
- When a service is required that is not supported by a firewall rule, the service shall be denied until the service and the rule can be evaluated and/or added to the firewall by Court Technology staff
- The firewall will be configured to deny all services not expressly permitted and will be regularly audited and monitored to detect intrusions or misuse

Intrusion Detection/Prevention System (IDS/IPS)

The Court shall maintain an appropriate Intrusion Detection/Prevention System (IDS/IPS). At a minimum, the IDS shall consist of at least one (1) network sensor and multiple server sensors to protect those servers that host web applications.

Reports shall be generated daily and available for review by the Court Administrator and/or Chief Judge when requested.

Remote Access

Remote access refers to connecting to the Court's network from a remote location, for example through a VPN (Virtual Private Network).

Court networked systems shall only be accessed over the Internet using encrypted passwords. The Court will use software to ensure that any device connecting to the network has the current level of security patches and anti-virus software installed. Otherwise the device will be quarantined and updated. The use of individual modems connected to single PCs, terminals, or servers provide unprotected "back doors" to the entire Court's network and must not be permitted without specific protective measures.

Virus Detection and Protection

Computers that become infected with virus and/or malicious code can jeopardize Court data and technology assets by contaminating or destroying data and/or hijacking. This policy provides controls to protect against such attacks. Refer to the Security Incidents section for appropriate action for detected or suspected viruses.

The following are controls that can reduce the chance of virus infection within the computing environment:

- Virus Detection Software: Virus detection software shall be used on all Court owned PCs, laptops, tablets, and servers. Staff accessing the Court's network from home are also required to have current virus detection software on all devices that access the Court's network.
- Scanning Executable Files: Virus scans and/or integrity checks, will be done prior to the first use of any executable file that is brought into the Court's computer environment from untrusted environments, e.g. program fixes copied from vendors' bulletin boards or websites.
- Scanning Removable Media: Virus scans or integrity checks must be done prior to the first use of each flash drive, CD, DVD, or other removable media, after the media has been out of the Court's controlled environment.
- Scanning Frequency: Virus scans of permanent media must be done at least daily on any server or PC connected to the Court's network.
- Scheduling Virus Scans: Whenever possible, virus scans will be scheduled to occur automatically.

Wireless Guest Access

Wireless guest access (Wi-Fi) shall be available in a limited manner in all areas of the Courthouse where the Court does business. This access is implemented for the purpose of providing Internet access to attorneys and other Court patrons to increase the Court's efficiency.

Wi-Fi User Authentication

All wireless guest access will be authenticated through a web-based authentication system.

Blocked Website Types

Guest access is restricted from the following network protocols:

- **Adult/Sexually Explicit**
- **Chat**
- **Games**
- **Glamour and Intimate Apparel**
- **Gambling**
- **Hacking**
- **Personals and Dating**
- **Photo searches**
- **Remote Proxies**
- **Streaming Media**

Limited Bandwidth

Guest bandwidth access shall be limited to not consume Internet resources necessary to conduct Court business.

Guidelines for Managing and Monitoring Wi-Fi Access

The Court will establish appropriate guidelines of managing and monitoring all Wi-Fi access.