Technology: Understanding, Respecting and Preserving Judicial Independence

In June 2015, during the meeting of President Judges at the President Judges/Pennsylvania Association of Court Management Conference, issues regarding technology, judicial independence and ethics were raised. Specifically, the typical technology arrangement in most counties – where the courts use technology resources provided by the County Commissioners, County Executive, or County Council – might compromise judicial independence, as well as conflict with provisions of the Code of Judicial Conduct.

The Information Technology Department of the Administrative Office of Pennsylvania Courts (AOPC/IT), in conjunction with the Allegheny County Director of Court Technology, was directed to look into these concerns from a technological standpoint and to develop suggestions on how technology can be set up in a county to preserve judicial independence, while also taking into consideration concerns such as cost, efficiency and practicality.

In developing these suggestions, Amy Ceraso, Director of AOPC/IT, and Sean Collins, Director of Information Systems for the Fifth Judicial District, visited with President Judge Farley Toothman, in Greene County, who has addressed some of the concerns in his county. They also gathered information on how other counties provide technology resources to the judiciary. Finally, they obtained input from Rita Reynolds, CIO for the County Commissioners Association of Pennsylvania (CCAP) and Tom Guenther, Director of Information Technology for Dauphin County.

Cybersecurity

In 2019, a few Pennsylvania courts experienced cyber attacks. These actions were debilitating to the court's operations, taking their various systems off line for days, and in some cases for weeks. Although county court infrastructures are largely furnished through the county executive function, AOPC/IT developed a list of cyber security best practices that county courts can use to have a conversation with county IT staff on proactively preventing a cyber event. It is important that AOPC Judicial District Operations and IT staff are immediately contacted if such an event occurs, and the best

practices document contains the contact information for the appropriate AOPC staff. Previously distributed at several president judge meetings in 2019, the document is attached as **Appendix E.**

Judicial Canons

Canons 1 and 2 of the Code of Judicial Conduct require judges to uphold the independence of the Judiciary, and to do so competently and diligently. Specifically, Rule 1.2 of the Code states: "A judge shall act at all times in a manner that promotes public confidence in the independence, integrity and impartiality of the judiciary, and shall avoid impropriety and the appearance of impropriety." Rule 2.5(A) of the Code provides: "A judge shall perform judicial and administrative duties competently and diligently."

These provisions of the Code require a President Judge in his or her role as head of the judicial district to act diligently to ensure the independence of the judiciary. Technology resources are provided in many counties in a manner that may lead to conflicts between the judiciary and county administration and that might impair judicial independence.

Ability of the Judiciary to Independently Contract

The AOPC's legal department has examined the ability of the judiciary to independently contract and concluded that judicial districts do not have the legal authority to independently contract, though some courts have worked out arrangements with the executive branch (county executive, commissioners, or council) empowering the judicial district to do so.

Executive Branch provides technology resources to the Judiciary in most counties

In most counties, the executive branch provides all technology resources for the judiciary. Routinely, the courts use county-provided telecommunications networks,

messaging services, Internet access, file servers, desktops and laptops, mobile devices, copiers, videoconferencing systems, audio and video recording systems, *etc.* This entire infrastructure is typically administered by county information technology staff who generally have unfettered access to the court's information. This means that court documents, including party filings, court-generated orders and opinions, court communications such as email and recordings of confidential proceedings are accessible by county IT staff.

In most counties, county IT staff members perform their duties professionally, never inappropriately viewing or disseminating court communications or information. Some judicial districts may have a dedicated IT staff person or staff to provide IT support to the court, while larger courts (such as Allegheny and Philadelphia) have their own court networks and infrastructure. Even in those larger judicial districts, the courts often share some resources, such as messaging systems, human resources and payroll systems for the sake of efficiency and cost savings.

How can a President Judge best meet his or her ethical obligation to protect court information and independence?

In looking at the different technologies in use in the counties, AOPC/IT has developed a list of ideas that a President Judge can implement – depending on the circumstances in the particular county.

It is important to note that many of the suggestions contained in this document and the related spreadsheet will be cost prohibitive in many counties and result in duplicative staffing. Balancing the cost and efficiency of any of the suggestions must be carefully considered.

Safeguarding court information can be achieved through a structured and cooperative relationship with the county executive and county IT staff, including mutually agreeable fiscal and practical restraints. As is often true, no one solution fits every court: The court management team - President Judge and his or her court administrator - will have to analyze their situation and determine what works best in their judicial district.

Ideally, a court management team will have a good working relationship with the county executive, and the county executive will recognize that it needs to do its part to preserve the independence of the judiciary. Hopefully, some of the ideas in this document will help in setting expectations and in developing solutions that both branches can embrace.

The County IT Director

In most counties, the County IT Director reports directly to the county executive or commissioners and is not accountable to the President Judge and district court administrator, even while providing technology resources and/or support for the judiciary. This is inherently a problem and can be addressed in a number of ways.

While it may be possible in some counties for there to be an independent IT director or IT staff, this is generally unfeasible in most of Pennsylvania. In the majority of judicial districts where there is no ability to have independent IT administration and support, it is important to have confidentiality agreements and policies that govern access to court information. A county IT Director could be asked to sign a confidentiality agreement with regard to judicial information and policies established to prohibit the unauthorized release of judicial information. A Memorandum of Understanding between the county and the judiciary could similarly set forth restrictions on accessing and releasing judicial information.

For example, a policy that is mutually agreed to by the County Executive and the Judiciary might provide as follows:

> The County Information Technology staff with the ability to access email and files of individual jurists and court staff shall be limited in number to XX, and shall be approved in writing by the President Judge. Additional individuals with such access may be approved by the President Judge if deemed necessary. All such individuals shall sign a confidentiality pledge, and shall not access any email or files of jurists or court staff or any other court information unless directed to do so by the President Judge. *At no time shall there be any access to such files and/or emails of a jurist without prior notice to such jurist*. To insure that there is no unauthorized access to the email and files of jurists and court personnel, access reports shall be generated and reviewed on a regular basis by the Director of Information Technology with the President Judge or District Court Administrator. Employees with administrative access must abide by all judiciary policies that pertain to confidential and private information, including the UJS Code of Conduct for Non-Judicial Employees. The President Judge may request that county IT employees with administrative access who fail to properly follow judiciary policies that pertain to confidential and private information be subject to sanctions, up to and including termination of employment.

Attached as **Appendix A** is a copy of the Unified Judicial System of Pennsylvania's Technology Resources Usage Policy. While directed primarily at system users – it does provide some useful definitions that could be used by a judicial district to develop its own access policy. A sample confidentiality pledge is also provided as **Appendix B**.

Admittedly, there are separation of powers questions (and Human Resource Issues) implicated in trying to impose these types of restrictions on county employees – but keeping the restrictions limited to only judiciary information and records may assist in cooperation from the county's executive branch. There are similar separation of powers issues with the executive branch and executive branch employees having unfettered access to judicial information. In the end, the County IT Director is often serving two different interests and must be able to effectively serve the executive and judicial branches by behaving professionally and ethically.

County Technology Resources

Each county has some type of technology infrastructure in place through which various technology services are provided. **Appendix C** lists the various components of a technology infrastructure, the "judicial independence" issues that may be associated with the service, some options for setting up the services in a way that may be less intrusive on judicial independence, and the pros and cons of each option. The list is extensive, and every county may not be using all of the services listed. Additionally, each judicial district may not uniformly have concerns about how information is handled with all of its services.

The foundational component of a technology infrastructure is the telecommunications network, including Internet access. Attached to the network are various devices, such as servers, desktops, laptops, telephones, mobile devices, copiers, videoconferencing equipment and more. Virtually any device that is attached to the infrastructure is accessible by various system administrators, as is the information contained on or transmitted by those devices. In the case of the network, Internet access and equipment such as telephones, there is generally a record of all communications that flow through those services or equipment which can be accessed by an administrator.

Moreover, data contained throughout the technology infrastructure can be stored and backed up in various places within the network and on external media, such as tapes. For example, it is possible for a copier to be set up to have a copy of every document copied or scanned stored on an internal hard drive in the copier, as well as to send a copy of each document to a remote server; and then to have that server backed up to a

tape. Replication of files and documents for backup purposes to various locations is quite common and results in additional people having access to that information, depending on where it is stored.

It is important for the court management team to have a good understanding of where and how judicial information is being generated and stored to be able to develop reasonable access policies while also ensuring that judicial information is properly stored and backed up. There may be some services where there is no good reason to keep a backup – for example, copiers, which can easily be set up to immediately delete any copied or scanned documents.

Part of addressing the independence issue will require that decisions be made about keeping and providing records associated with logging transactions. Logging of transactions is ordinarily used in computer systems to track when changes were made to data and who made those changes. This information can be important in a situation where data is improperly accessed or modified.

To insure that administrators are not improperly accessing information, the courts and counties could agree that logging reports be regularly generated for review, showing, for example, anyone who looked at files generated by court personnel. President Judges and counties could also agree that administrators seek permission from them or the district court administrator prior to accessing or providing any information from a jurist or judicial staff – even in the case of reviewing files in response to an e-discovery request or subpoena.

In 2012, to address concerns that certain IT staff could access email of appellate court jurists, the Supreme Court adopted an e-discovery policy whereby access to appellate jurists' deleted files or email could be accessed only by a certain number of administrators. Those administrators must all be approved by the Chief Justice, sign confidentiality agreements, and are not permitted to search individual documents or email. Instead, the administrators must provide the documents in question for the legal staff to search. A copy of this policy is attached as **Appendix D**.

Other records that should be addressed are records of telephone calls, either through a telephone system in the county or through mobile devices; and records of Internet access. Because telephone systems are often essentially computer systems, they have the ability to retain call history. Policies should be established on whether and how long these types of records should be stored, are also frequently kept. Similarly, this information should be included in any policy that is addressing the retention of and access to records.

Two services that are often overlooked in developing an access and retention policy are videoconferencing and audio recording. These services generally are delivered over the telecommunications network resulting in an ability to monitor and/or record proceedings that may be sealed or confidential. For example, many audio recording systems store the digital recordings on servers that are administered by county IT personnel. Efforts should be made to store these recordings on servers controlled by court personnel, or at the very least they should not be made available to any non-court personnel and subject to confidentiality agreements.

In regard to Appendix C, there is far more detail that can be provided about specific services and ways in which to secure data than provided in this high level analysis. AOPC IT is available to discuss solutions with individual judicial districts, and visit courts to help develop strategies and policies to protect the court data. If there are any questions, please contact the individuals below.

Amy J. Ceraso
Director of Information Technology, AOPC
412.565.3013
Amy.Ceraso@pacourts.us

Russel Montchal
Assistant Director of Information Technology, AOPC
717.795.2077
Russell.Montchal@pacourts.us

Larry Lichty
Senior Enterprise IT Infrastructure Architect, AOPC
717.795.2003
Larry.Lichty@pacourts.us

Damon Kline
IT User Services Manager, AOPC
717.231.3333
Damon.Kline@pacourts.us

Sean Collins
Director of Information Technology, Fifth Judicial District of Pennsylvania
412.350.4526

APPENDIX A

SUPREME COURT OF PENNSYLVANIA
UNIFIED JUDICIAL SYSTEM OF PENNSYLVANIA

Technology Resources Usage Policy

Introduction

It is the policy of the Unified Judicial System of Pennsylvania (UJS) to ensure that Users of the Pennsylvania Judiciary's Technology Resources comply with all laws and regulations, UJS policies (including the Policy on Non-Discrimination and Equal Employment Opportunity and the Code of Conduct for Employees of the Unified Judicial System), and applicable conduct rules for judicial officers.

This Policy defines the rules and responsibilities that each User must observe in order to ensure the ethical use of Technology Resources according to the high standards of conduct required of those working in the UJS and to protect the security and integrity of all UJS Technology Resources.

Scope

For the purposes of this Policy, the term "Users" includes 1) all employees and contractors of the Administrative Office of Pennsylvania Courts (AOPC), including state-level judicial district employees, 2) all appellate court judicial officers and employees, 3) all Magisterial District Judges and their staffs, and 4) all employees of boards, committees, and court-related panels established by the Supreme Court of Pennsylvania.

Definitions

Technology Resources: All computer equipment, mobile devices, software, and facilities that comprise the Judiciary's information technology infrastructure and telecommunications network.

Electronic Information: Any data, text, email, or file stored on or transmitted through the Judiciary's Technology Resources, including those transmitted through non-UJS accounts if made on equipment provided by the Judiciary.

IT Administrators: AOPC information technology staff or appellate court technical staff who have been granted administrative access to a computer system for purposes of maintenance and support.

Usage Rules

- Technology Resources are provided to Users for the purpose of conducting official UJS business. Reasonable use of Technology Resources for personal business by Users is allowed if such use does not violate this Policy or interfere with their duties or Judiciary operations. *Users will be responsible for payment of any costs the UJS incurs resulting from unauthorized or inappropriate personal use of Technology Resources.*

- If personal devices are authorized for use in accessing Technology Resources to conduct official UJS business, this Policy applies only to work-related Electronic Information stored or transmitted on those devices.

- Use of Technology Resources shall be conducted with decorum and in accordance with the highest standards of conduct and all applicable UJS policies.

- Users shall take reasonable steps to ensure the security and confidentiality of Technology Resources and Electronic Information while conducting official UJS business.

Prohibited Uses

- The use of Technology Resources in violation of any applicable statute, regulation, court order or policy is prohibited.

- Unless related to official UJS business, Technology Resources may not be used to knowingly transmit, create, download, store or print profane, offensive, or obscene language or images.

- In accordance with the UJS Policy on Non-Discrimination and Equal Employment Opportunity, Technology Resources may not be used to harass or discriminate against others because of race, color, sex, sexual orientation, national origin, age, disability, or religion.

- Unless related to official UJS business, Users may not forward work-related messages, either automatically or manually, from their UJS accounts to non-UJS accounts.

- Users may not knowingly damage or alter Technology Resources (including security devices or codes), or attempt unauthorized access to Electronic Information or Technology Resources. This includes attempting password theft, propagating computer worms and viruses, broadcasting intrusive or unsolicited advertising, or performing any action that negatively impacts Technology Resources.

- Users are not permitted to utilize Technology Resources to send messages as someone other than themselves without prior authorization.

- Technology Resources may not be used in any manner that intrudes or infringes upon the work product of any User without the User's prior authorization.

- Technology Resources may not be used to operate any commercial enterprise or to improperly provide financial benefit to a User or any other person (such as developing software intended for sale or license).

- Technology Resources may not be used in the unauthorized copying or storage of licensed software programs or data. Authorized copying of licensed software programs shall be completed by IT Administrators only.

Privacy and Confidentiality

- Users do not have personal privacy or property interests in their Electronic Information. Subject to the limitations below, the UJS reserves the right to examine all Electronic Information.

- IT Administrators routinely conduct authorized, limited monitoring of Technology Resources to assess and examine network performance and security. If, during such monitoring, IT Administrators become aware of possible violations of this Policy by a User, they will inform the appropriate person(s) based on the nature of the possible violation and work to mitigate the violation immediately.

- If there is suspected misuse of Technology Resources or a violation of this Policy by Users, IT Administrators may intercept, copy, review, block access to, and release to appropriate authorities Electronic Information without notice to or consent of the sender or recipient. Before taking such action(s), IT Administrators must receive advance approval as outlined in the next paragraph.

- Approval for *non-routine* review of Electronic Information described in the preceding paragraph may be granted only by: 1) the Court Administrator of Pennsylvania for employees and contractors of the AOPC (including state-level judicial district employees), Magisterial District Judges and their staffs; 2) the President Judges of Superior or Commonwealth Court for their respective Users; and 3) the Chief Justice of Pennsylvania for any User with notification to the respective President Judge(s) or the Court Administrator of Pennsylvania, as appropriate.

- By using Technology Resources, each User acknowledges and agrees to these conditions.

Implementation and Administration

- The Court Administrator of Pennsylvania, acting on behalf of the Supreme Court of Pennsylvania, shall be responsible for the implementation and ongoing administration of this Policy.

- The AOPC Information Technology department will work with the technical staff of each appellate court to develop, implement, and administer uniform procedures to ensure that Technology Resources are used in accordance with this Policy.

- Violations of this Policy may result in disciplinary action as prescribed by the appropriate policies, which govern the conduct of particular Users.

Published June 2015

APPENDIX B

CONFIDENTIALITY PLEDGE

I, _____, do hereby acknowledge that as a member of the Information Technology Department of the Administrative Office of Pennsylvania Courts (AOPC), I have been approved by the Chief Justice to perform the duties outlined in Section 4.1 of the Document Retention Policy of the Unified Judicial System (UJS). I further acknowledge that these duties are to be undertaken only at the specific direction of Chief Counsel or a designated attorney of the AOPC Legal Department, and are otherwise not to be exercised. I understand that employees of AOPC, are bound by the obligation "to safeguard confidential information acquired in the course of their employment" and "shall not disclose or use confidential information for any purpose not connected with the performance of their official duties." Code of Conduct For Employees of the Unified Judicial System, SectionIIIA. In addition to the requirements imposed by the Code of Conduct, I do hereby pledge to maintain the confidentiality of any and all information which I may obtain through fulfillment of my duties exercised pursuant to Section 4.1 of the Document Retention Policy and shall disclose this information solely to Chief Counsel or other designated attorney of the AOPC Legal Department, and only when specifically directed to do so. I understand that violation of this pledge may subject me to sanction.

_____
Signature

_____
Printed Name

Date:_____

Appendix C

Review of Technology Services used by the Courts

This document provides an overview of the different technology services used by the courts. It examines issues that should be discussed by president judges and court administration with their county information technology departments.

After reviewing the way in which county budgets are developed and existing law regarding the ability of the courts to contract and purchase, as well as the ability of the courts to manage technical staff, it seems clear that in most cases a county will be providing technology services to the courts. Accordingly, we have directed most of the information herein to that approach. Nonetheless, there are certainly counties where the courts have more direct involvement in managing IT work.

There are many areas in which providing a unified approach for both the county executive function and the judiciary is cost effective as it limits duplication of effort. Information technology is one example, but most counties use unified applications for payroll, human resources and purchasing.

There are ways in which the president judges and court administration can work with their county's IT departments to protect court information. A county IT director should be working with the court to decide how to deliver IT services most appropriately. Most county IT staff members recognize their responsibilities to protect the confidentiality of court communications and other data; but to be clear, these responsibilities should ideally be memorialized by an agreement between the county and the court.

As a way to recognize the significance of such an agreement and the responsibility to simultaneously serve different branches of government, it is recommended that the county executive give the president judge input into the hiring and firing of the county IT director.

Courts can assist county IT in discerning the nature of court communications and data and its need for protection. For example:

- The president judge could annually swear in county IT staff who will be providing services to the court. This action helps the IT staff realize their duty to the court as well as to the county's executive.

- A county could limit administrative privileges by removing that responsibility from the IT director out of that responsibility, leaving the technicians to make the actual changes.

- Counties could provide educational information about the courts to the IT staff, such as information on confidentiality, restrictions on accessing and providing court information, the Right-to-Know Law and its application to the courts.

In this document, we seek to identify areas for discussion between president judges, court administration and the county executive and IT director regarding responsibilities and expectations.

Technology Service:

Internet Access

Access to the Internet is required for the courts to connect to outside resources, such as legal research. Typically this service is provided to the judiciary by the county, and it is likely that county access policies are extended to and imposed on the judiciary. The court may need access to categories of sites or individual sites that are blocked by the county. In addition, Internet usage creates browsing histories that may be available to IT staff.

Some county courts may have established their own Internet connections separate from the counties, but there likely are cost savings and other efficiencies achieved by sharing services with the county. When the county provides an Internet connection, technical resources to support the connection are the responsibility of the county. This option can provide control to the court which can establish its own access policy. That policy could define what sites are available and allow the Court to control access when needed, without intervention by county IT personnel. The court's browsing history would be protected if it is not available to non-judicial county staff, or if it is not retained. These items are best addressed through the establishment of confidentiality agreements between county IT and the court.

Establishing separate Internet connections for the use of the courts and the county will likely result in additional costs, such as non-recurring setup costs and monthly recurring service-related costs. In addition, the court would need its own technical personnel to install and support its separate Internet connection. Redundant connections may be needed to provide full availability, which can further increase costs. Finally, responsibility for detecting misuse would fall to court personnel.

Areas for Discussion:

Access and storage of browsing history

The court's need to access certain categories of Internet sites that may be otherwise blocked by the county

Is network traffic and bandwidth usage monitored by the county? If so, who has access to the monitoring tools and data?

Sample Language:

The Court recognizes that it is the policy of the County's IT department to store Internet browsing history and that IT staff may need access for routine or emergency maintenance purposes. Access to the browsing history of Court personnel is limited to the following IT staff [insert staff name/s]. The Internet browsing history of Court personnel shall not be accessed or viewed by IT staff without prior notification to and approval by the President Judge, unless the information at issue is subject to the formal subpoena or similar lawful command of a proper investigative body (such as the Judicial Conduct Board) or tribunal (such as the Court of Judicial Discipline) and notice to the President Judge is expressly prohibited by an order of a court of proper jurisdiction or other proper authority. At the President Judge's discretion, such approval may be granted on an ongoing basis and withdrawn at any time. Access to information for routine or emergency maintenance purposes should not be unreasonably withheld by the Court.

The Court recognizes that Internet blocking software is used by the County to prevent access to certain categories of websites, or individual websites that may compromise the security of the County IT infrastructure, or that may be inappropriate. Nonetheless, Court personnel, in the course of performing their duties, may need access to sites that have been blocked by the County. In such a case, the affected Court employee will notify the President Judge, or his or her designee, of the need to access a blocked site, and if access is approved, will notify the County IT Director or staff to provide such access.

The Court recognizes that it is the policy of the County's IT Department to monitor network traffic for security and troubleshooting purposes, and that IT staff may need access for routine or emergency maintenance purposes. Access to the network monitoring tools and logs is limited to the following IT staff [insert staff name/s]. Network monitoring of the desktops of Court personnel shall not be performed by IT staff without prior notification to the President Judge, unless the information at issue is subject to the formal subpoena or similar lawful command of a proper investigative body (such as the Judicial Conduct Board) or tribunal (such as the Court of Judicial Discipline) and notice to the President Judge is expressly prohibited by an order of a court of proper jurisdiction or other proper authority. At the President Judge's discretion, such approval may be granted on an ongoing basis and withdrawn at any time. Access to information for routine or emergency maintenance purposes should not be unreasonably withheld by the Court.

Technology Service:

Network Infrastructure

A secure and reliable network infrastructure is required in order for the court to use technologies in performing its duties. The infrastructure encompasses not only the physical wiring and wireless framework, but also a variety of hardware and software working in concert to provide connectivity. The initial implementation of an enterprise-wide network can prove quite costly. Networking capabilities are typically provided by county IT departments for the use of court personnel. There could be a significant savings recognized under this arrangement. This configuration typically allows county IT staff, as system administrators, to have access to court information on equipment on the county's network.

If the judicial and executive branches do share a common network, it must be pursuant to a confidentiality agreement. This agreement would need to clearly define the rights and restrictions to accessing court information and resources on the county network. This arrangement would allow the court and county to continue using one network for both executive and judicial functions. A confidentiality agreement would legally restrict the ability of county IT staff to access or distribute court information. The county would bear the burden of administering and monitoring the network.

Some courts have established a network separate and distinct from the county's network. This can be configured in such a way that interaction between the court and county can be facilitated while maintaining judicial privacy and independence. Connectivity between the two autonomous networks can be accomplished by setting up a "trusted relationship" between them. Such an arrangement does allow the court to completely control access to court information, resources, and equipment; however, all systems administration would be the responsibility of the courts. Whether the courts have the expertise and/or the financial resources to perform those functions needs to be considered with this scenario.

Establishment and management of a separate network infrastructure may be fiscally and practically impossible in many counties. Because of the need to communicate and share resources between the court and court-related county offices, having multiple networks may prove difficult unless there is a "trust relationship" established between the networks. Another consideration is that the AOPC can currently connect physically to only one network in each judicial district to provide case management system access to court users. In many districts, that connection is on a county network. If there are users on both court and county networks without a trust relationship in place, different methods of access may be needed to connect to the case management system. Technical personnel would need to maintain and administer a court network. This can be accomplished by the use of either court staff or a third-party group that is acting at the direction of the court.

Areas for discussion:

Access of court information on network resources sample language:

The Court recognizes the ability of the County's IT Department to access certain Court information through the County network, and that such access is required in order to permit the IT Department to properly perform its duties as system administrators. Nonetheless, the Court and the County IT Department will work to develop written guidelines on what access is acceptable to certain information and to define protocols for notice to the President Judge or his or her designee in the event that Court data needs to be accessed.

Technology Service:

Messaging Services (Email and/or Instant Messaging)

Secure, safe email is essential for the courts. Typically, this service is provided to the judiciary by the county and its messaging policies are extended to and imposed on the judiciary. These policies may prove to be restrictive to the court.

If the court uses county-supplied messaging services, it should establish its own policies governing use that the county would need to recognize and honor. The court should include any AOPC policy requirements that apply. These policies should be enforced through confidentiality agreements and limiting access by system administrators to court email. In addition to email or instant messaging communications, email systems may also contain voice messages if the county is using a phone system that is integrated with its email system. Any policy defining access to such messages should be consistent across all types of messages that are stored. The county must then abide by the courts policies.

There may be cost savings recognized by sharing services with the county, and technical support would be the responsibility of the county. Confidentiality agreements and policies regarding system administrators in county systems should be used to protect unauthorized access to email.

Some courts have established their own email services on court hardware or via a third-party service provider. In such circumstances, the court would have control of all email service functionality and the concerns of the county having access to emails or the ability to release emails would be eliminated. However, there would be additional hardware and license costs to bear, and technical resources may need to be contracted for or court technical staff added.

Areas for Discussion:

Who has administrative access to the email system?

Is it possible to limit the number of administrators who have access to court email and other communications such as instant messaging?

What are the protocols that must be followed in response to public access requests regarding court emails/messages consistent with principles of separation of powers as described by the Commonwealth Court in Grine v. Cnty. of Centre, 138 A.3d 88 (Pa. Commw. Ct. 2016) (requiring that requests for public access to electronic records concerning judges and other court personnel be promptly forwarded to the court's open records manager for review/response), appeals denied, Nos. 333 MAL 2016 & 334 MAL 2016, 2016 Pa. LEXIS 2009 (filed Sept. 13, 2016)?

What email retention policies are in place? How long is deleted email kept?

How long are backups of the email system kept?

Does the county email system have spam filtering? If so, how are emails incorrectly identified as spam released?

Who has physical access to the area where the email system is housed? How is the area secured?

Sample language:

The Court recognizes that the County IT Department may need access for routine or emergency maintenance purposes to be able to properly manage the system. Access to the email of Court personnel is limited to the following IT staff [inset staff name/s]. The email and other electronic communications of Court personnel shall not be accessed or viewed by IT staff without prior notification to the President Judge or his or her designee, unless the files at issue are subject to a formal subpoena or similar lawful command of a proper investigative body (such as the Judicial Conduct Board) or tribunal (such as the Court of Judicial Discipline) and notice to the President Judge is expressly prohibited by an order of a court of proper jurisdiction or other proper authority. At the President Judge's discretion, such approval may be granted on an ongoing basis and withdrawn at any time. Access to information for routine or emergency maintenance purposes should not be unreasonably withheld by the Court.

The Court recognizes that the County IT Department is responsible for implementing email usage policies for the executive branch of county government. The Court's usage requirements and policies differ from the executive in certain areas. The Court and the County IT Department will identify those areas where the Court's email policies differ and work to implement the Court's policies for court personnel.

The Court recognizes that the County IT Department must backup email for recovery purposes and may archive or set retention periods for email. County IT backup and retention schedules shall follow Court record retention policies for Court records. The County IT Department shall periodically review backup schedules with the President Judge or his or her designee. Backup tapes for Court email shall be stored in a secure area, accessible only to authorized IT personnel and physically destroyed when no longer needed. When disposing of equipment, hard drives must be destroyed or securely wiped.

Technology Service:

Servers / Storage

Secure, reliable servers and data storage are necessary. They may reside on a court or county infrastructure. Typically these resources are provided to the court by the county. County-instituted rules that govern the use of and maintenance of such equipment and resources may prove to be restrictive or contradictive to requirements and procedures necessary for court operations.

While the court can establish and deploy its own servers and storage areas on a court-controlled network or engage a third-party service provider (which may be cloud-based) to provide these resources, there would be hardware and license costs associated with this endeavor. Additionally, there may be technical personnel needed to maintain and administer these resources. However, the courts would have control of all of their content running on or stored on servers or storage areas.

In most counties, court data is stored on county-supplied servers and storage. Typically backups are performed on a daily, weekly and monthly basis. In most cases, these backups are then stored onsite as well as a copy taken to an offsite location. System administrators generally have access to this data by virtue of their duties in maintaining the servers. It might be possible to control access to certain data by using encryption technologies as well as confidentiality and access agreements. It may be possible to limit the storage of court information to a single server and to limit the number of administrators maintaining that server.

Backup and archive solutions must comply with applicable court record retention schedules.

Areas for Discussion:

On which servers will court information be stored? Will it be stored "in the cloud"?

If the information is stored in the cloud, will it be stored on servers located in the United States?

Who will be the administrators of the servers on which court information is stored?

Is it possible to limit the number of administrators who have access to court information?

What kind of notice will be provided to the court before court information on servers is accessed?

What are the county policies and procedures for server backups?

Where will backups be stored and how will those backups be transported to offsite locations?

Do county backup and archive solutions comply with applicable court document and record retention schedules?

Who has physical access to the area where court servers are housed? How is the area secured?

What are the county policies and procedures for disposing of server hard drives? Sample Language

The Court recognizes that the County IT Department may need access for routine or emergency maintenance purposes to properly manage servers and storage systems. Access to the files of court personnel is limited to the following IT staff [inset staff name/s]. Electronic files of Court personnel stored on county servers shall not be accessed or viewed by IT staff or provided to others without prior notification to the President Judge or his or her designee, unless the files at issue are subject to a formal subpoena or similar lawful command of a proper investigative body (such as the Judicial Conduct Board) or tribunal (such as the Court of Judicial Discipline) and notice to the President Judge is expressly prohibited by an order of a court of proper jurisdiction or other proper authority. At the President Judge's discretion, such approval may be granted on an ongoing basis and withdrawn at any time. Access to information for routine or emergency maintenance purposes should not be unreasonably withheld by the Court.

The Court recognizes that the County IT Department must backup servers and storage systems for recovery purposes. County IT backup schedules shall take into account Court record retention policies. The County IT Department shall periodically review server and storage system backup schedules with the President Judge or his or her designee. Backup tapes for Court servers shall be stored in a secure area, accessible only to authorized IT personnel and physically destroyed when no longer needed. When disposing of equipment, hard drives must be destroyed or securely wiped.

The Court recognizes that the County IT Department controls physical access to servers housing Court files. The County IT Department shall limit physical access to Court servers and storage systems to essential county IT staff and vendors, and shall periodically review physical access lists with the President Judge or his or her designee.

The Court recognizes that the County IT Department may contract with cloud storage vendors to store Court files outside the county network, and that the County IT Department may need access for routine or emergency maintenance purposes. Access to the files of Court personnel is limited to the following IT staff [inset staff name/s]. Electronic files of Court personnel stored on cloud servers shall not be accessed or viewed by IT staff or provided to others without prior notification to the President Judge or his or her designee, unless the files at issue are subject to a formal subpoena or similar lawful command of a proper investigative body (such as the Judicial Conduct Board) or tribunal (such as the Court of Judicial Discipline) and notice to the President Judge is expressly prohibited by an order of a court of proper jurisdiction or other proper authority. At the President Judge's discretion, such approval may be granted on an ongoing basis and withdrawn at any time. Access to information for routine or emergency maintenance purposes should not be unreasonably withheld by the Court.

Telephone Service:

Office Software / Licensing

A court requires a variety of productivity software in order to perform day-to-day business processes in an efficient manner. These software tools may reside on court and/or county servers and infrastructure.

There are several ways in which a court can obtain software: purchasing its own agreement from the vendor, establish a joint licensing agreement with the county, or subscribe to a cloud- based service to provide the software. All have advantages and disadvantages. Software vendors may request audits of software use to ensure licensees are complying with licensing terms.

If a court purchases its own software, it would have control of all software versions and patches. However, there would be hardware and license costs, and technical personnel would be needed to maintain and administer licensing obligations.

There may be cost savings recognized by combining software licensing agreements, to obtain better pricing. For example, the AOPC procures its Microsoft licenses under the County Commissioners' Association Enterprise Agreement to gain cost savings. In many counties, courts are asked to include software licensing costs in their budgets.

Purchasing software from a cloud-based vendor (as opposed to an on premise solution that requires physical hardware) might also be cost effective, but presents its own set of data storage issues. Technical support would still be required to support the product and licensing. There may also be security concerns with using a cloud-based solution that would need to be addressed through licensing agreements. Typically, there is little control over where documents "in the cloud" are stored, although government agreements sometimes specify that data must be kept on servers located in the United States.

Areas for Discussion:

How many licenses are available to the court?

What costs will the court incur in software licensing?

What kind of access do the licenses provided allow the court?

Who will be responsible for installation, maintenance and upgrades? Where will documents produced by the office software be stored?

Who is responsible for retention of software licensing keys?

Who is responsible to keep software entitlement documentation and purchasing records in case there is a software audit?

Sample Language

The County IT Department is responsible for purchasing, installing, maintaining and upgrading software on Court-owned desktops, servers and laptops.

The County IT Department will provide the Court with the software licensing costs for the Court's annual budget.

The County IT Department is responsible for maintaining the Court's software entitlement documentation and software licensing keys, and upon request, shall provide this information to the Court.

The County IT Department will notify the Court in advance of any software upgrades and will schedule such upgrades to minimize disruption to the Court.

Technology Service:

Telephone Systems / Fax Machines

Most courts likely use a traditional phone system that is managed through the county. This arrangement is practical because of support, maintenance, and possible demarcation requirements. Many counties are moving towards using a Voice over Internet Protocol (VoIP) system.

There are minimal security concerns with using a county-based telephone system, but as with all computer based systems, records of calls made and received are generally available to County personnel who both support and pay invoices for these services. Use of a county-based system will permit access to county personnel to sensitive data. Access to this data can be restricted by limiting the administration of the system and by confidentiality agreements concerning county personnel and related officials.

A court may choose to implement a separate Voice over Internet Protocol (VoIP) system. A VoIP system would allow for the use of an array of innovative features. A VoIP system would allow for the telephone communication to be routed over the network infrastructure. Use of a VoIP eliminates the need for separate phone cabling and a phone can be placed anywhere there is a network connection. VOIP systems also can interface with messaging systems and are likely integrated with the county's email system for delivery of voice messages. While having a separate system allows the court to have control, hardware and licensing costs associated with these types of systems and setting up a separate VOIP system may be cost prohibitive. In addition, technical personnel likely would be needed for support and maintenance.

Areas for Discussion:

Will VoIP voicemail be integrated with the email system? If so, who will have access to that?

If VoIP voicemail is integrated with the email system, does the voicemail system hold copies of voicemail separately from the email system? If so, who will have access to that?

Sample Language

The Court recognizes that the County IT Departments may need access for routine or emergency maintenance purposes to properly manage the phone system. Access to Court voice mail and calling logs is limited to the following IT staff [inset staff name/s]. Voicemail stored on the county phone system shall not be accessed or listened to by IT staff, or provided to others without prior notification to the President Judge or his or her designee, unless the voicemail at issue is subject to a formal subpoena or similar lawful command of a proper investigative body (such as the Judicial Conduct Board) or tribunal (such as the Court of Judicial Discipline) and notice to the President Judge is expressly prohibited by an order of a court of proper jurisdiction or other proper authority. At the President Judge's discretion, such approval may be granted on an ongoing basis and withdrawn at any time. Access to information for routine or emergency maintenance purposes should not be unreasonably withheld by the Court.

When disposing of equipment, hard drives must be destroyed or securely wiped.

Technology Service:

Desktop Computers & Laptops

Secure, reliable desktop computers are essential for court personnel to perform their daily functions in an efficient manner. Computers may reside on court or county networks.

A court may deploy its own desktop computers on a court-controlled network, or county supplied desktops may be used.

If a court uses its own devices, all content, operating system versions, and software running on these devices will be under the control the court. Security of these devices would be under the control of the court. However, there would be hardware and license costs associated with the deployment of desktop computers, and technical personnel would be needed to maintain and administer these resources.

If a court chooses to use county-supplied desktops, the technical resources and costs needed to maintain desktop computers would be the responsibility of the county. Because the privacy of the judiciary may be compromised by the ability of county IT staff having access to information stored on the devices, confidentiality agreements should be used to limit access to court information.

The use of laptops includes all the same privacy and maintenance issues associated with desktop computers, as well as additional security concerns to be considered. Laptops provide an additional level of freedom and accessibility that needs to be weighed against the possibility of increased security risks.

Policies are needed to ensure that no threats are introduced into the network when laptops reconnect after external use. It may be necessary to use an encryption package to protect data contained on a laptop in the event of loss or theft. A Virtual Private Network (VPN) hardware and/or software solution will be needed to allow resources to be accessed from an external location.

Areas for Discussion:

What procurement vehicles will be used for desktops and laptops?

What type of encryption and VPN software will be needed to satisfy court requirements?

What are the county policies and procedures for disposing of desktop and laptop hard drives?

Who has administrative access to desktops and laptops?

Sample Language

The Court recognizes that the County IT Department may need access for routine or emergency maintenance purposes to properly manage the desktops and laptops. Access to the files of court personnel is limited to the following IT staff [inset staff name/s]. Electronic files of Court personnel stored on desktops or laptops shall not be accessed or viewed by IT staff or provided to others without prior notification to the President Judge or his or her designee, unless the files at issue are subject to a formal subpoena or similar lawful command of an investigative body (such as the Judicial Conduct Board) or tribunal (such as the Court of Judicial Discipline) and notice to the

President Judge is expressly prohibited by an order of a court of proper jurisdiction or other proper authority. At the President Judge's discretion, such approval may be granted on an ongoing basis and withdrawn at any time. Access to information for routine or emergency maintenance purposes should not be unreasonably withheld by the Court.

Providing Court personnel secure external access to Court computer resources is the responsibility of the County IT Department. The Court will identify computer resources that it wants available through external access, and the County IT Department shall provide a secure means to access these resources.

The Court recognizes that the County IT Department is responsible for the maintenance and disposal of Court desktop and laptop hardware. When disposing of equipment, hard drives must be destroyed or securely wiped. The County IT Department shall notify the Court in advance of any desktop or laptop upgrades and will schedule such upgrades to minimize disruption to the Court.

The Court recognizes that the County IT Department is responsible for selecting and purchasing desktops and laptops for Court use. The County IT Department shall meet with the President Judge or his or her designee to review the Court's requirements before purchasing desktops and laptops for the Court.

The Court recognizes that the County IT Department is responsible for server, desktop and laptop disposal. When Court computers with hard drives are disposed, the County IT Department shall destroy or securely wipe the hard drives.

Technology Service:

Mobile Devices

Smartphones and tablets provide a means for court employees to stay connected when they are away from the normal connection points of a brick and mortar structure. Not only do mobile devices facilitate always being "connected," but they also provide a level of security to certain users such as probation officers when they are "in the field." Due to their mobility and ability to be easily misplaced or stolen, there are more privacy and maintenance issues that need to be considered in the use of smartphones and tablets.

There are many ways in which courts deploy mobile devices. They can be managed by the court, by the county, or through a written "BYOD" policy (Bring Your Own Device) that addresses collective bargaining agreements and relevant employment law issues. There are generally licensing and hardware costs associated with the use of these devices, no matter which option is chosen.

To have email accessible on a mobile device, the device must be associated with the email service being used by the court. As most courts are using county email, they are deploying mobile devices through the county IT departments. The benefit is that maintenance and administration responsibilities lie with the county. As with other technology provided by the county, the ability to access court information is available to IT administrators and would need to be protected through confidentiality agreements.

It is possible for the court to manage its own devices, but that would require some technical expertise. If the court is using county-provided email, coordination would be necessary to access email on non-county provided devices. With mobile devices, it is vitally important to properly manage security because these devices are so easily lost or misplaced, and because they can contain confidential information.

The use of a "bring your own device" policy for mobile devices is quite common, as there are no direct hardware or license costs to the county or courts for the devices. Employees often prefer to use their own device rather than carry a second dedicated work device. Whether an employee uses a county/court provided device or a personal device, a Mobile Device Management (MDM) policy and software should be used to ensure that only appropriate devices are allowed to connect to court or county-related resources. MDM software requires technical personnel to maintain and administer.

Public access laws and e-discovery policies for the courts may govern the release of information stored on mobile devices. Employees using personal devices should be aware that court-related communications sent or stored on their devices may be subject to disclosure under these policies.

Areas for Discussion:

What policies will need to be created or updated to cover mobile devices? Which MDM software will be needed to meet Court requirements?

What are the protocols that must be followed in response to public access requests regarding mobile device communications consistent with principles of separation of powers as described by Commonwealth Court in Grine v. Cnty. of Centre, 138 A.3d 88 (Pa. Commw. Ct. 2016) (requiring that requests for public access to electronic records concerning judges and other court personnel be promptly forwarded to the court's open records manager for review/response), appeals denied,

Nos. 333 MAL 2016 & 334 MAL 2016, 2016 Pa. LEXIS 2009 (filed Sept. 13, 2016)?

What access do MDM administrators have to apps and location services on mobile devices?

Who are the administrators of the MDM system?

Does the MDM have the ability to "wipe" user data when a mobile device is lost?

Sample Language

The Court recognizes that the County IT Department may need access to the Mobile Device Management (MDM) system for routine or emergency maintenance purposes to properly manage mobile devices. Access to the mobile devices of Court personnel is limited to the following IT staff [inset staff name/s]. App inventory and location services shall not be accessed or viewed by IT staff, or provided to others without prior notification to the President Judge or his or her designee, unless the information at issue is subject to a formal subpoena or similar lawful command of an investigative body (such as the Judicial Conduct Board) or tribunal (such as the Court of Judicial Discipline) and notice to the President Judge is expressly prohibited by an order of a court of proper jurisdiction or other proper authority. At the President Judge's discretion, such approval may be granted on an ongoing basis and withdrawn at any time. Access to information for routine or emergency maintenance purposes should not be unreasonably withheld by the Court.

Court personnel shall notify the County IT Department of lost or stolen mobile devices as soon as possible after the loss. When notified of the loss of a mobile device, the County IT Department will delete all Court data and apps from the device.

When disposing of or reassigning mobile devices, hard drives must be securely wiped.

Technology Service:

Videoconferencing

Courts use videoconferencing on a regular basis for a variety of reasons, for example, as a way to include remote parties in the participation of court proceedings and for court personnel to facilitate long distance meetings while saving the cost of travel. Proper configuration is necessary to ensure the privacy of these connections. This may be an issue when the network being used is not under court control.

A court can secure its own equipment. This equipment may reside on court and/or county infrastructure. The court would have control of all configuration settings of these systems. Connections can be configured to allow only court- authorized parties. However, technical personnel may be needed to maintain and administer videoconferencing systems that are under the control of the court, creating the potential for additional costs to the court.

Videoconference environments are usually complex to establish and maintain. For this reason, most courts use county-owned/leased equipment. This equipment may reside on court and/or county infrastructure. In this situation, the connectivity and maintenance of the system is the responsibility of the county. Depending on the connection configuration, the county may have the ability to access confidential videoconferencing sessions that occur on the county equipment and network. The court should therefore address access, recording and storage of videoconferencing sessions with a confidentiality agreement.

It is possible for a court to subscribe to a cloud-based service to provide a forum for long distance meetings and, in some cases, participation of remote parties in court proceedings. Subscription services can be tailored to the needs of the court, and there is no hardware to maintain thereby providing a cost savings over maintaining a video conferencing infrastructure. The court would have control of all configuration settings of these systems. Connections can be configured to allow only court-authorized parties.

Some minor technical knowledge is required to administer users of the service. There is potential for additional costs to the court, and again the court would have to address the access, recording and storage of videoconferencing sessions with the third party vendor. This option may in fact be less controllable and secure than using a county-provided service.

Areas for Discussion:

Are there web-based video conference options that meet AOPC and court requirements?

Are videoconferencing sessions being stored or monitored by IT personnel? If so, access should be defined and limited.

Does the video conference system display a notice on screen when a session is being recorded?

Sample Language

The Court recognizes that the County IT Department must have administrative access to the video conferencing system to properly manage video sessions. Access to the video conference system and video conference recordings is limited to the following IT staff [inset staff name/s]. Live video conference sessions shall not be accessed or viewed by IT staff, except when troubleshooting technical problems with the knowledge and consent of the participants. Video conference sessions

shall not be recorded without the knowledge and consent of the participants. When a video conference is recorded, a visual indication that recording is in progress shall display on the screen to the participants.

The Court shall determine the retention period of recordings made with the video conferencing system.

When disposing of equipment, hard drives must be destroyed or securely wiped.

Technology Service:

Printers / Copiers /Multi-Function Devices/Scanners & Scanned Documents

A court routinely uses printers and copiers in the course of daily business processes. The court needs to be aware of configuration options that are possible when using this type of office equipment. For example, the systems can be configured to make an additional backup copy of every document that is copied or printed.

Most courts use county owned or leased equipment. This equipment may reside on court and/or county infrastructure. The privacy of court documents should be protected by a confidentiality agreement, and the court should require that the copiers be configured so that they do not save or backup electronic versions of documents that are printed, copied or scanned.

The advantage to this scenario is that maintenance and repair will be handled by the county. Nonetheless, county IT or other staff may have the ability to access or view confidential information that is passed through these devices.

A court may secure its own equipment, but technical personnel may be needed to maintain and administer printer/copiers that are under the control of the court. There may be additional purchase and maintenance costs if the court procures its own printers and copiers. On the plus side, the court would have control of all configuration settings of these devices and would control whether the devices produce a backup copy and where that copy is stored.

The court may routinely scan documents for electronic storage/retrieval purposes. The court would need to be aware of configuration options when performing this process. There is the potential for exposure of confidential documents, depending on who controls the scanning equipment and who controls the servers on which the documents will reside.

As discussed above for other services, it is possible for a court to secure its own equipment, which would give it control of all scanning and storage processes. However, technical personnel may be needed to maintain and administer a document management system.

It is more likely that a court will use county owned/leased equipment that resides on the county infrastructure. In this scenario, technical resources and costs needed to support this process are the responsibility of the county, but county IT personnel may have the ability to access confidential information that is handled and stored through this process. Such access would need to be addressed through agreements and limiting administrative access.

Areas for Discussion:

Will devices retain document copies on the copier hard drive for any period of time? How will the devices be connected to the network?

How will the locations for scanned documents be configured?

Will users be able to email scanned documents directly from the device? If so, then how will the email boxes on the device need to be configured?

Are hard drives removed from replaced or disposed copiers?

Sample Language

The Court recognizes that the County IT Department is responsible to configure and manage multifunction copiers. The County IT Department will configure the Court's multifunction copiers to delete copies immediately and to not store backups. Multifunction copiers that are disposed shall have their hard drives destroyed or securely wiped. The Court shall approve all email addresses and file storage areas that are configured in multifunction copiers.

Technology Service:

Courtroom Audio / Video Recording Systems

It has become commonplace for courts to routinely use digital audio/visual recording systems, such as FTR and JAVS. Proper configuration and storage are necessary to ensure the security of these recordings. This may be an issue when the network on which these systems reside is under county control.

Most courts use county owned or leased equipment. This equipment likely resides on court and/or county infrastructure. The maintenance and storage requirements of these systems are the responsibility of the county.

Depending on the configuration, non-court personnel may have the ability to access confidential recordings that occur on the county equipment or are stored on the county network. This access needs to be controlled through a confidentiality agreement and by limiting administrative access to the systems.

It is possible that a court can secure its own equipment, but technical personnel may be needed to maintain and administer recording systems that are under the control of the court. There may be additional purchase and maintenance costs if the court procures its own recording system. The benefit of this is that the court would have control of all configuration settings of these systems. Recordings are stored on court servers. Security of recordings are under the control of the court.

Areas for Discussion:

Are county IT staff monitoring the use of audio/video recording systems? If so, access should be limited and confidentiality agreements with respect to court proceedings should be entered into by IT personnel.

Are recorded court proceedings being stored on the county network? Where are they being stored and who has access to those recordings? How long are they retained and for what purpose?

Sample Language

The Court recognizes that the County IT Department must have administrative access to the audio/video recording system in courtrooms to properly manage the system. Access to the audio/video recording system is limited to the following IT staff [inset staff name/s]. Recordings made by the audio/visual system shall be stored in a secure area with access limited to authorized Court personnel and County IT staff. Live audio/visual sessions shall not be accessed or viewed by IT staff, except when troubleshooting technical problems with the knowledge and consent of the presiding judge. County IT staff shall not use the audio/visual system to record any session or meeting without the express consent of the presiding judge.

The Court shall determine the retention period of recordings made with the audio/video recording system in accordance with UJS policies and rules governing the retention of stenographic notes and audio recordings. When disposing of equipment, hard drives must be destroyed or securely wiped.

Technology Service:

Disaster Recovery and Continuity of Operations

A court has an obligation to ensure continuity of its operations, including its ability to protect and recover IT infrastructure in the event of a disaster. A disruption of services and the ability to access critical information can have a catastrophic effect on the court's ability to administer justice. The court and county may have completely different views about the priority of service recovery. The court's options and the degree of independence of a disaster recovery plan will be dictated by whether the court has established its own network or it uses a county-controlled network. These issues should be addressed in a formal agreement.

A court can establish an independent IT disaster recovery plan from that of the county. It will need to be designed in such a way that interaction between the court and the county can be facilitated while maintaining judicial privacy and independence.

Establishment and management of an independent disaster recovery plan may be fiscally impossible in many counties. The need to often share resources between the judiciary and county offices, including 911, may make this arrangement extremely difficult.

If a court is part of a county disaster recovery plan, then a formal agreement needs to clearly define the rights and restrictions with regard to the access and security of court information as well as defining the court's priority in the order of restoring systems. The county's disaster recovery schedule may not reflect the needs and time schedule of the court's COOP plan and said plan must take precedence for the court

Areas for Discussion:

How will competing priorities of the court and the county be managed during a continuity situation or a disaster?

What general time frames can be established for restoration of court systems? (Include example of AOPC IMT restoration priorities and timeframes).

Sample Language

The Court recognizes that the County is responsible for the overall County government disaster recovery plan, which includes the Court. The Court and the County will work to identify and incorporate the Court's service recovery priorities into the County disaster recovery plan.

The County IT Department is responsible for maintaining an accurate and complete inventory of all Court computing hardware and software, including replacement costs. In the event of a catastrophic loss of Court computing hardware and software, the County IT Department is responsible to submit this inventory to the appropriate entity for insurance purposes.

Establishment of Technology Use Policies

A court should develop technology policies to govern the use of technology resources by judges and court personnel.

The following areas, at a minimum, should be included in a technology use policy:

Usage Rules – defining employee and the extent of permitted personal use of court resources, if any; and

Prohibited uses of Technology Resources, Privacy and Confidentiality.

In June 2015, the Supreme Court adopted a Technology Resources Usage Policy for judicial officers and court staff using AOPC-provided technology resources. A copy of this document is attached. Courts were asked to consider adopting similar policies to govern use of technology resources at the judicial district level.

Legal Hold Data Access Policy

1.0 Purpose

1.1 Ensure the proper security of data under legal hold.

1.2 Ensure that the use and security of information resources complies with state and federal laws and regulations; the Unified Judicial System personnel policies; and the Code of Conduct for Nonjudicial Court Employees.

1.3 Ensure that sensitive court information will be protected from misuse.

1.4 Ensure the ethical use of information resources according to the high standards required of the judicial system.

1.5 Electronic documents, i.e., Word or Excel files, which are "deleted" from Supreme Court and AOPC file servers, and from the Judiciary's email servers, are nonetheless retained on the system for a period of two (2) years, after which they will be discarded unless otherwise subject to further retention, such as if directed to be retained by the Legal Department pursuant to ongoing litigation, i.e., a 'legal hold.'

2.0 Revision History

Date	Rev No.	Modification	Author	Approval
10-9-14	1.0	Final approved version		Supreme Court

3.0 Persons Affected

3.1 All staff of the Unified Judicial System (UJS) of the Pennsylvania Courts (comprised of the Supreme Court, Superior Court, Commonwealth Court, Courts of Common Pleas (case management system data only), Magisterial District Courts (email and Office documents on AOPC systems only), and the Administrative Office of Pennsylvania Courts (AOPC)) and the associated Boards and Committees, and the associated Rules Committees, excepting Justices and Judges, with access to data under legal hold.

4.0 Policy

Administrative Access

4.1 The number of individuals from Judicial Automation with ability to access deleted email and files of individual justices shall be limited in number to six, and shall be approved by the Chief Justice. Additional individuals with such access may be approved by the Chief Justice if deemed necessary. All such individuals shall sign a confidentiality pledge, and shall not access any deleted files of individual justices unless directed to do so either by Chief Counsel or a designated attorney from the AOPC Legal Department. Access to the deleted files of individual justices shall be monitored by electronic means which shall be reviewed on a regular basis by the Director of Judicial Automation. At no time shall there

be any access to such files and/or emails of a justice without prior notice to such justice. Any unauthorized access shall be promptly reported to the Chief Justice and Court Administrator. Appellate Court OLS IT Administrators must be approved for access to deleted email and files from their respective courts by each courts' respective President Judge or his or her designee.

4.2 Employees with administrative access must abide by all judiciary policies that pertain to confidential and private information, including the UJS Code of Conduct for Non-Judicial Employees.

4.3 Employees with administrative access who fail to properly follow judiciary policies that pertain to confidential and private information will be subject to the sanctions listed in the UJS Code of Conduct for Non-Judicial Employees, Section IX.

Access to Legal Hold Email

4.4 Email under legal hold remains in the production email system, accessible to the individual employee on legal hold and IT Administrators who manage the email system.

4.5 During the review and analysis phase of an e-discovery action, AOPC's Legal Department will have the ability to search email that is under legal hold. The IT Administrators of the email system will have no involvement with the search tool except demonstrating how it functions to the Legal Department.

4.6 Neither Chief Counsel nor any designated attorney from the AOPC Legal Department shall access an individual justice's deleted files without prior notice to, and consultation with, that justice unless the files at issue are subject to a request from an investigative body and notice to the individual justice is expressly prohibited.

4.7 In the event an individual justice's deleted files are subject to a litigation hold, Chief Counsel or a designated attorney from the AOPC Legal Department shall immediately notify the justice of same, unless otherwise expressly prohibited by an investigative request.

Access to Supreme Court and AOPC Legal Hold File Shares

4.8 Supreme Court and AOPC file shares under legal hold remain on the production file server for the duration of the legal hold. In the Supreme Court, each Chamber and Prothonotary office has its own separate file server that has both private and group shares. Every justice and employee has a private file share (H:) that is accessible only to themselves and at least one group share (G:) that is accessible to a defined list of individuals for collaboration purposes. The Court of Judicial Discipline, the IOLTA Board, and the Chief Justice's Central Legal staff each have separate file servers with private and group shares for their respective staffs. Private and group file shares for the Pennsylvania Lawyers Fund for Client Security, the Supreme Court Rules Committees, the Supreme Court Executive Administrator's Office, and the Middle District Prothonotary's Office exist on the Supreme Court file server at the PJC. Only designated Supreme Court OLS staff have administrative access to Supreme Court file servers. AOPC has five file servers: one in the PJC, one in Philadelphia, and three in Mechanicsburg. Every AOPC employee has a private file share (H:) and one or more group shares. Only designated

AOPC IT User Services staff have administrative access to AOPC file servers.

4.9 Supreme Court and AOPC file shares are copied nightly into the OnBase archiving system. OnBase is accessible only to the IT Administrators who manage the system.

4.10 During the review and analysis phase of an e-discovery action, AOPC's Legal Department will have the ability to search files on legal hold copied from the file servers into OnBase. The IT Administrators of OnBase will have no involvement with the search tool except demonstrating how it functions to the Legal Department.

Access to Superior Court and Commonwealth Court Legal Hold File Shares

4.11 Superior Court and Commonwealth Court file shares under legal hold remain on the production file server for the duration of the legal hold. Every judge and employee has a private file share that is accessible only to themselves and at least one group share that is accessible to a defined list of individuals for collaboration purposes. Only designated Superior and Commonwealth Court OLS staff have administrative access to their respective file servers.

4.12 Superior and Commonwealth Court have no automated method of searching file shares. During the review and analysis phase of an e-discovery action, AOPC's Legal Department will work with the OLS IT Administrators to review file shares under legal hold.

Access to Supreme Court, Superior Court, Commonwealth Court and AOPC Personal Computers

4.13 The Appellate Courts and AOPC set aside personal computers and hard drives that are under legal hold, unless the personal computers are required to remain at the user's desk. Any personal computers or hard drives removed for legal hold are kept in a secure location within each Appellate Court or AOPC, accessible only to the Legal Department upon request. Personal computers under legal hold are accessible only to their users and the IT Administrators that support the personal computers.

4.14 The Appellate Courts and AOPC do not have an automated method for searching the contents of personal computers or hard drives. During the review and analysis phase of an e-discovery action, AOPC's Legal Department will work with the appropriate Appellate Court or AOPC IT Administrators to review the contents of personal computers or hard drives.

Access to Supreme Court, Superior Court, Commonwealth Court and AOPC Backup Tapes

4.15 Each Appellate Court and AOPC maintain their own backup tapes. Backup tapes are kept in a secure location within each Appellate Court or AOPC, accessible only to the authorized IT Administrators for that Court or agency. To retrieve data from backup tapes, the data must be restored to a server or personal computer before it can be searched. IT Administrators will restore tapes to a server or personal computer, and then give access to the Legal Department to review the data.

Access Logging

4.16 Access to email, file shares and personal computers, whether by IT Administrators or

users, is logged on the system where the access occurred. Logs are available to the Chief Justice, President Judges and Court Administrator upon request or will be provided to the Chief Justice, President Judge and Court Administrator monthly for review.

5.0 Definitions

5.1 Administrative Access: Elevated privileges granted on any IT system to maintain and support the system; such privileges are granted to a limited number of Appellate Court OLS or AOPC Judicial Automation staff.

5.2 IT Administrator: An Appellate Court OLS or AOPC Judicial Automation staff member who has been granted administrative access to a computer system for purposes of maintenance and support.

5.3 Legal Hold: A communication issued by the AOPC Legal Department, as a result of current or reasonably anticipated litigation, which suspends the normal disposition or processing of electronic documents, i.e., Word and Excel files, email and other records, either electronic or paper.

5.4 Document Retention: This refers to the retention of electronic documents, as described in section 1.5.

6.0 Responsibilities

7.0 Procedures

Cybersecurity - Best Practices

June 2019

Cybersecurity Introduction

When it comes to digital data and document assets, court systems have very similar data responsibilities to that of financial institutions, health-care providers, and other government organizations. Court systems contain sensitive data for individuals and organizations. Court records are crucial to the functioning of our society. This extraordinary public responsibility makes court data a high-value target for cybercriminals.

The landscape of court technology has changed rapidly, as digital tools help facilitate the business process of the courts. This proliferation of technology has improved the judiciary's access and transparency, while also significantly increasing data storage and the digital footprint. Consequently, there are multiple potential entry points for data breaches in the judicial branch. These include the judiciary's statewide case management systems, networks, servers, email, cloud storage, software programs, file transfer, remote access, Wi-Fi systems, employee devices, and an array of additional court-specific technology.

Some of the most common cyber-attack types are listed below:

- **Phishing** uses social engineering to solicit personal information from users through emails and fake websites to name a few.
- **Code-injection** attacks involve the submission of incorrect code into a vulnerable computer program without detection.
- **Ransomware** infects software and locks access to the data until a ransom is paid.

There are numerous reports from counties, other law and judicial entities within Pennsylvania and across the country that such events are becoming more frequent. Cybersecurity is becoming a more common topic outside the IT arena as many more incidents are being reported in the mainstream news.

AOPC is providing the following security best practices and technological recommendations as guidance to courts, counties and agencies to consider implementing in order to protect their technology and information assets.

Process-based Security Layers

- **Strong authentication requirements:** Passwords should require a higher level of complexity. The use of passphrases is an easy way to increase password length while still making them memorable to the end-user.

- **Appropriate access only:** Access to data on any system should be limited to only accounts that need access.

Process-based Security Layers (continued)

- **Restricted administrative access:** Administrative ("admin") access is broad access granted to administrators of computer systems. It is normally provided to technical staff for support purposes, but this type of access should be limited to only the few specific users that are responsible for administering each individual system or server.

- **Administration accounts:** Each administrator user should have a unique account username, and a password that must be changed regularly without repeating passwords.

- **Remove unnecessary software:** Software products that are not needed regularly should be uninstalled from desktops and servers, so they cannot be exploited and perhaps not even detected.

- **Avoiding suspicious emails:** Staff members should exercise extreme care when opening email attachments or links, even if they know the sender or were expecting a document.

- **Access management:** Most organizations and departments have detailed processes for "onboarding" new staff with appropriate IDs and giving them access to systems needed to perform their job duties. Ensure that similar processes are defined and followed for staff departures or changes and all corresponding access edits or removals.

- **Security education:** Staff members benefit from persistent and focused education on potential security issues and how to avoid them. A regular security newsletter should be sent to judiciary employees to cover a wide variety of security related topics, and should be written to be understood by non-technical staff.

Technology-based Security Layers

- **Firewall devices:** Internet traffic destined for the network should first encounter perimeter firewalls, which only allow expected packets into the Internet-facing servers located in the "demilitarized zone" (DMZ) segment

- **Intrusion detection and prevention:** Intrusion detection/prevention services (IDS/IPS) should be used with a regularly updated signature library to block content that is known to be harmful.

- **GeoProtection:** This technology filters away incoming requests that originate in high-risk countries such as Russia and China that would not normally be contacting courts for regular business purposes.

Technology-based Security Layers (continued)

- **Anti-bot and anti-virus:** These software programs provide protection for workstations, mobile devices, and servers by looking for malicious traffic patterns on the network and blocking them before they reach court users or devices.

- **Internet proxy servers/appliances:** This technology exposes only a single public IP address for outbound Internet browsing, and not any internal IP address space details. The proxy device should monitor both secure (https) and non-secure (http) Internet browsing activity.

- **BOT & Denial of Service (DOS) protection:** Automated monitoring processes should alert IT staff of high volumes of Internet traffic from a single source, so that they can be investigated and a determination made whether to block the IP address.

- **Encryption:** Data that travels between two secured networks should traverse an encrypted VPN to ensure the data is not clearly available while in transit. File transfers to state agencies and all financial institutions should use secure FTP with SSL/TLS certificates.

- **Desktop protection:** Desktop-related protections should be used including anti-virus and anti-malware software that is updated daily. These applications will block infection attempts from malicious sources, such as sidebar ads on websites and infected files sent via email. Macros should be disabled by default to prevent this common infection technique.

- **Email protection:** All email that comes into the organization should go through a set of filter servers. These servers look at the messages, scan them for viruses, and inspect them to see if they meet any spam criteria. If there are viruses attached to the emails, they are blocked. If the email is likely a spam email, it will be flagged and show up in the user's junk or spam folder.

- **Mobile Device protection:** Mobile devices should be enrolled in Mobile Device Management (MDM) software in order to access court systems or email. The MDM provides device policies for applications, secure delivery of certificates needed for business wireless access, and remote wipe capability in case of device loss.

- **Monitoring:** Automated and manual monitoring processes within the infrastructure and application architecture should be used to track normal usage and make staff aware of any behavior that is suspicious.

- **Patching:** Servers, workstations, and any computer device should be kept up-to-date with security updates and patches, for both the operating system and any installed products.

- **Vulnerability and penetration testing:** Penetration and vulnerability testing should be performed regularly and noted vulnerabilities remediated quickly

Summary

Taken together, these security strategies will provide a layered "defense-in-depth" security approach to best protect you from possible data breaches and cybersecurity incidents. Unfortunately, all of the measures in the world cannot guarantee or provide absolute protection from a successful cyber-attack. If a cyber-attack is successful, courts must rely on documented, well planned incident response and Continuity of Operations Plans (COOP) or other business continuity procedures to ensure a quick and effective recovery. It is important that recurring review and testing be performed for all cybersecurity defenses and COOP plans to ensure they are kept up to date and court and county staff are familiar with procedures and protocols.

It is further recommended that an ongoing security awareness program and education for jurists and court staff be put in place by courts. There should be recurring routine audit checks to ensure that all implemented cyber security policies, procedures and memorandums of understanding are being followed. These items will assist in guiding administrators, IT staff, and users on how they can use judiciary technology resources and safeguard against ever increasing cyber threats.

Additional Resource Contacts

COOP Questions: Rick Pierce; Rick.Pierce@pacourts.us
IT Questions: Russel Montchal; Russel.Montchal@pacourts.us