Administrative Office of the Courts

Chief Justice Matthew B. Durrant
Utah Supreme Court
Chair, Utah Judicial Council

September 5, 2023

Ronald B. Gordon, Jr.
State Court Administrator
Neira Siaperas
Deputy State Court Administrator

MEMORANDUM

TO: **Management Committee / Judicial Council**
FROM: **Brody Arishita – Chief Information Officer**
RE: **Internal Information Technology Policies for Final Approval**

In response to the Legislative Auditor General's cybersecurity audit, "A Performance Audit of Cybersecurity in the State of Utah," the Technology Advisory Committee (TAC) is working with the Policy, Planning, and Technology Committee (PP&T) to overhaul the judicial branch's information technology policies. The TAC is developing a comprehensive Information Technology Policy Manual ("Manual"), similar in a format to the Human Resource and Accounting Manuals.

While the TAC continues its work on the Manual in its entirety, PP&T recommends that the Judicial Council adopt the following two sections of the Manual as final with a **September 12, 2023 effective date**. These sections were created first, as they are critical first steps for the Manual and the overarching goal of protecting the courts against cyberattacks.

IT-01000 Information Security Policy (NEW - Internal)

All Utah State Courts' (Utah Courts) Information Technology (IT) employees, contractors, vendors, interns and third-parties that create, use, maintain or handle Utah Courts' IT resources shall follow Utah Courts Information Security Policy and related sub-policies. The policy shall be subject to and superseded by applicable regulations and laws.

IT-01150 Information Security Rick Management (NEW - Internal)

The Enterprise Domain and Security Architect (EDSA) shall document and implement a risk management program to prevent, detect, contain, and correct both deliberate and inadvertent IT security incidents and emergencies.

Administrative Office of the Courts

Chief Justice Matthew B. Durrant
Utah Supreme Court
Chair, Utah Judicial Council

May 1, 2023

Ronald B. Gordon, Jr.
State Court Administrator
Neira Siaperas
Deputy State Court Administrator

Kade Minchey, CIA, CFE
Auditor General
Office of the Legislative Auditor General
W315 State Capitol Complex
Salt Lake City, UT 84114

Dear Mr. Minchey:

Thank you for the opportunity to respond to "A Performance Audit of Cybersecurity in the State of Utah". The Administrative Office of the Courts (AOC) appreciates you and your staff for reviewing risks for cyberattacks. This audit will help the AOC to better mitigate risks. The AOC supports both recommendations and we are working to implement them as outlined below.

(1) We recommend the Judicial Branch create and maintain a cybersecurity strategic plan. The 2014 cybersecurity plan of the judicial branch will be updated to help reduce security gaps, extend visibility into security threats, and meet compliance requirements. AOC-IT Department and internal administrators will work with the Judicial Council's Policy, Planning and Technology Committee to develop recommended changes to the plan. The Judicial Council will provide final approval. AOC-IT will review this plan annually. In addition, the five security related policies that are in draft form will be finalized following the same process.

(2) We recommend the Judicial Branch ensure their employees complete the annual cybersecurity awareness trainings. AOC-IT has started creating a cyber security training that is more aligned with the technology utilized by the courts and the tools we use. This module will be available through our Learning Management System (LMS), and all staff will be required to complete the training yearly. The training will be closely monitored for completion by the AOC Education Department.

The AOC is committed to making the improvements needed to increase protection against cyberattacks and ensure employees complete the required training.

Respectfully,

Ronald B Gordon

Ronald B. Gordon, Jr.
State Court Administrator

Utah State Courts Information Technology

Information Security Policy

IT-01000

Responsible Official: Chief Information Officer

Responsible Office: Information Technology

Effective Date: September 12th, 2023

Last Revision Date: August 8th, 2023

Associated Policies, Forms, and Documents

- Court Security Information
- Technology in the Courts
- Audit Services
- Human Resources
- IT-01000 Information Security Policy
- IT-01120 Software Development and Configuration Management Best Practices Policy
- IT-01150 Information Security Risk Management Policy
- IT-03000 Incident Response Plan

Definitions

AOC - Administrative Office of the Courts

AUP - Acceptable Use Policy (HR15-09)

CIO - Chief Information Officer

Cybercrime - Criminal activity or a crime that involves the Internet, a computer system, or computer technology.

Data breach - An incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. A data breach may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

DDT - Deputy Director of Technology (to CIO)

EDSA - Enterprise Domain & Security Architect

HR - Human Resources Department

IT - Information Technology Department

IT Resource - Information Technology resources are the property of Utah Courts and include, but are not limited to all network related systems; business applications; network and application accounts; administrative, academic and library computing facilities; court-wide data, video and voice networks; electronic mail; video & web conferencing systems; access to the Internet; voicemail, fax machines and photocopiers; courtroom audio/video; computer equipment; software and operating systems; storage media; Intranet, VPN, and FTP. IT Resources include resources administered by IT.

PCI - Payment Card Industry –Data Security Standard. Promotes Payment Card Industry standards for the safety of cardholder data across the globe.

PHI - Personal Health Information

PII - Personally Identifiable Information – any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

User - Any person who makes any use of any Utah Courts IT resource from any location (whether authorized or not).

Policy Statement

All Utah State Courts (Utah Courts) Information Technology (IT) employees, contractors, vendors, interns and third-parties that create, use, maintain or handle Utah Courts IT resources shall follow Utah Courts Information Security Policy and related sub-policies. Policy shall be subject to and superseded by applicable regulations and laws.

Policy Exception

Policy exemptions to Information Security Policy IT-01000 through IT-03000 will be permitted only when approved in advance and in writing by the Enterprise Domain and Security Architect (EDSA), Deputy Director of Technology (DDT) or Chief Information Officer (CIO).

Purpose

The Information Security Policy consists of related policies IT-01000 through IT-01120. It applies to all users of Utah Courts IT resources and supports the following goals:

1. Promote a “security is everyone’s responsibility” philosophy to assist Utah Courts in meeting its business and legal commitments.
2. Ensure CyberSecurity training is completed annually by all staff and proof of training is on file with the AOC Training Department.
3. Ensure that Utah Courts complies with all applicable laws and regulations.
4. Ensure the integrity, reliability, availability and superior performance of IT resources.
5. Ensure that users are protected from data breaches and cybercrime.
6. Ensure that use of IT resources is consistent with the principles and values that govern the use of facilities and services.
7. Prevent unauthorized disclosure of critical information.
8. Prevent disruption of court operations.
9. Ensure Utah Courts are protected from financial, legal, regulatory and reputational harm.
10. Ensure that IT systems are used for their intended purposes.
11. Establish processes for addressing policy violations and sanctions for violators.

General Use and Responsibilities

1. Maintain current knowledge of, and comply with, the contents of this Information Security Policy.
2. Distribute confidential and sensitive information on a limited basis to those with a business need to know the information.
3. Protect all PHI, PII, PCI, Protective Order and other regulated or proprietary data from unauthorized access.
4. Notify the EDSA and/or the IT Service Deskof any suspected breaches or violations

Policy Violation

1. Violation of the Acceptable Use Policy (HR09-15) may result in disciplinary action, up to and including termination of contract or employment.
2. Utah Courts reserves the right to report violations of federal, state and local laws and regulations governing computer and network use, as well as interactions that occur on the Internet, to authorities as deemed appropriate.
3. Users who violate the AUP may be held liable for damages to Utah Courts assets, including but not limited to the loss of information, computer software and hardware, down time, fines and judgments imposed as a direct result of the violation.
4. Utah Courts reserve the right to deactivate a user's access rights, if the user is suspected of any violation of this policy, when necessary to preserve the integrity and/or security of IT Resources.

Complaint Procedure

Information Security violations shall be reported to the EDSA, DDT or CIO. Non-security related violations (such as receipt of inappropriate content, other Human Resources (HR) policy violations, general policy violations or regulatory compliance violations) shall be reported to a supervisor or HR.

Related Governing Standards, Policies and Guidelines

1. Federal Information Security Management Act (FISMA)
2. FTC Red Flag Rule

3. Health Insurance Portability and Accountability Act (HIPAA)
4. International Organization for Standardization (ISO)
5. National Institute Standards and Technology (NIST)
6. Payment Card Industry Data Security Standard (PCI DSS)

Utah State Courts Information Technology Information Security Risk Management Policy

IT-01150

Responsible Official: Chief Information Officer

Responsible Office: Information Technology

Effective Date: September 12th, 2023

Last Revision Date: August 8th, 2023

Associated Policies

- Court Security Information
- Technology in the Courts
- Audit Services
- Human Resources
- IT-01000 Information Security Policy
- IT-01120 Software Development and Configuration Management Best Practices Policy
- IT-01150 Information Security Risk Management Policy
- IT-03000 Incident Response Plan

Definitions

- **AOC -** Administrative Office of the Courts
- **CIO -** Chief Information Officer
- **Enterprise Domain and Security Architect (EDASA)** – IT Manager, reporting to the CIO.
- **IT -** Information Technology Department

- **Risk profile** – An evaluation of an individual or organization's willingness to take risks, as well as the threats to which an organization is exposed. A risk profile is important for determining a proper investment asset allocation for a portfolio.

Policy Statement

The Enterprise Domain and Security Architect (EDSA) shall document and implement a risk management program to prevent, detect, contain, and correct both deliberate and inadvertent Information Technology (IT) security incidents and emergencies.

Policy

Security Risk Identification

1. The Information Security Risk Management Program is part of the overall Utah State Courts (Utah Courts)/Administrative Office of the Courts (AOC) IT Risk Management Program. Its primary purpose is to prevent, detect, contain, and correct deliberate and inadvertent IT security incidents.
2. Using the risk-related information generated, the IT Department shall implement a combination of policies, procedures, and physical measures to sufficiently reduce (mitigate) the vulnerabilities and risks to a reasonable level.
3. The EDSA is responsible for risk management. Using various analytic efforts, the EDSA shall identify and rank risks in order to estimate total overall risk and IT Risk Profile.
4. All IT security protocols, including software and firmware patch management, shall be evaluated in terms of risk vs. cost to further mitigate risk prior to determining a final decision on expenditure of funding.

Security Risk Analysis / Ranking

1. After potential Information Security risks are identified, analyses of the risks shall be conducted to prepare an accurate and thorough assessment of their impacts on the confidentiality, availability, and integrity of the Utah Courts sensitive information.
2. This effort also provides the information to rank risks in order of their likelihood to happen, likelihood of success if attempted, and the consequences of their occurrence.
3. The risks are defined in a format compatible with that used and described within the IT Defense In Depth and Incident Response plans.

Vulnerability Assessment

1. Security reports shall be provided by the EDSA on at least a quarterly basis for IT leadership team review.
2. Where the need is identified, vulnerabilities shall be presented and discussed.

Security Risk Mitigation

1. Using the risk-related information generated in the efforts described above, the AOC IT Department shall implement a combination of policies, procedures, and physical measures to sufficiently reduce (mitigate) the vulnerabilities and risks to a reasonable level in compliance with EDSA standards, as well as governmental requirements.

Risk Reevaluation

1. Self-audits and activity reviews shall be conducted within IT at least annually.
2. The IT Department shall constantly monitor the identified Utah Courts IT Risk Profile to measure and refine its effectiveness.

Security Incident Response and Reporting

1. All event logs shall be collected in a centralized location on secure media that is difficult to alter and is protected from unauthorized access for protected services.
2. Viewing of the logs is on a need-only basis.