Rule Proposal: Branchwide Technology and Data Security Guidelines

Hon. Tara M. Desautels,
Associate Justice, Court of Appeal, First Appellate District
Jenny Grantz,
Attorney, Legal Services

Meeting of the Technology Committee
November 14, 2024

Overview

- Joint Information Security Governance Subcommittee (JISGS) proposes rule amendments to allow the Judicial Council to adopt branchwide guidelines for technology and data security
- Action requested: Approve draft invitation to comment on rule proposal
- Next steps:
  - Approval by Rules Committee on December 5 (approved by JISGS & RPS on Nov. 7, ITAC on Nov. 13)
  - Circulate for public comment from December 6, 2024 to January 6, 2025
  - Recommend Judicial Council approval at April 25, 2025 meeting
  - Proposed effective date: July 1, 2025

Rule Proposal Background

- JISGS goal is to create branchwide technology and data security guidelines to:
  - Ensure minimum level of technology and data security across the branch
  - Help the branch apply technology and data security best practices
- Today we present our first proposed rule changes:
  - Clarifies the division of responsibility for physical security vs. technology and data security;
  - Creates a process for developing, adopting, and revising the technology and data security guidelines; and
  - Enables guidelines to be developed after rules adoption

Amendments to Rule 10.172

- Rule 10.172 requires each superior court to develop a court security plan with their local sheriff's office and other justice partners that addresses the security of our courts
- JISGS proposes edits to clarify that the focus of rule 10.172 is physical court security by:
  - Revising subdivision (a) to clarify that rule 10.172 addresses security in court facilities
  - Deleting "computer and data security" from the list of topics included in a court security plan
  - Adding a sentence to the Advisory Committee Comment to directing readers to rule 10.405 for computer and data security

Amendments to Rule 10.172

Rule 10.172. Court security plans

(a) Responsibility

The presiding judge and the sheriff or marshal are responsible for developing an annual or multiyear comprehensive, ~~countywide~~ court security plan that applies to each court facility in the county.

(b) Scope of security plan

(1) Each court security plan must, at a minimum, address the following general security subject areas:

* * *

~~(V) Computer and data security;~~

* * *

Advisory Committee Comment

* * *

Former subdivision (b)(1)(V), on computer and data security, is now addressed in rule 10.405, on judicial branch technology and data security standards.

New Rule 10.405

- Creates procedures for adopting and revising branchwide technology and data security guidelines
- Key provisions:
  - Guidelines will be developed by ITAC (can be delegated to JISGS); approved by Technology Committee and Judicial Council
  - 30-day period for courts to comment on proposed new guidelines and substantive amendments
  - Guidelines apply to all courts and the Judicial Council
  - Guidelines are exempt from public disclosure under rule 10.500

New Rule 10.405

Rule 10.405. Judicial branch technology and data security guidelines

(a) Purpose

This rule creates procedures for the adoption and maintenance of judicial branch guidelines for technology and data security.

(b) Adoption and maintenance of guidelines

(1) The Information Technology Advisory Committee is responsible for making recommendations to the Judicial Council regarding guidelines for technology and data security.

(2) Before recommending to the Judicial Council the adoption of any new guidelines or substantive amendments to the guidelines, the Information Technology Advisory Committee must make the proposed guidelines available to the entities listed in subdivision (c) for 30 days for comment.

(3) The Judicial Council delegates to the Technology Committee the authority to make nonsubstantive technical changes or corrections to the guidelines. Upon the recommendation of the Information Technology Advisory Committee, the Technology Committee may approve nonsubstantive technical changes or corrections to the guidelines without the comment period required in subdivision (b)(2) and without approval by the Judicial Council.

(c) Application of guidelines

The guidelines apply to the Supreme Court, the Courts of Appeal, the superior courts, and the Judicial Council.

(d) Disclosure of guidelines

The guidelines are exempt from public disclosure consistent with the provisions of rule 10.500 that exempt records whose disclosure would compromise the security of a judicial branch entity.

Questions or comments?