ITEM 5.3.5 | ACCESSIBILITY AND SECURITY

The system must prevent access by unauthorized persons and facilitate access by authorized persons according to a defined set of user permission levels. The system must be usable by judges, and also by judicial assistants, clerks of court, and case managers as the judge may direct.

5.3.5.1 Security.

The system must comply with industry-standard security methods, including encryption and authentication protocols, to protect access to the application and associated data.

5.3.5.2 User Permission Levels.

- System-assigned User Permission Levels. The system shall provide the system administrator with the ability to configure user permissions to restrict access to the application, sub-applications (functions), and case data (as needed to comply with statutory restrictions on access to case data).

- The system shall provide a means for a judge to manage which other authenticated individual users or judge-defined user groups may view or change case-related information the judge originates, such as notes, document annotations, contents of work folders, case management information, and personal and system calendar entries.

5.3.5.3 Password Protection.

The system must authenticate users and their permission levels based on username and password, providing access to all functional modules using the same credentials.

5.3.5.4 Electronic Signatures.

The system must ensure that electronic signatures may be applied to orders only by the authenticated user.

5.3.5.5 Remote Access.

The system must be accessible remotely via the web by judges and other personnel having appropriate permission levels.

5.3.5.6 Persons with Disabilities.

The system must comply with Section 508 of the Rehabilitation Act of 1973 (as amended), which lists standards necessary to make electronic and information technology accessible to persons with disabilities.