

New York State Unified Court System Data Security Questionnaire and Attestation

Organization Name:

IT Security Contact Name:

Title:

Phone Number:

Email address:

Please indicate security compliance by checking the appropriate boxes below.

UCS data will be encrypted at rest.

Physical access to servers is restricted to appropriate personnel and access to the physical location is logged.
Electronic access to UCS data will be restricted to only those who need it.

All computers, workstations, and servers on this network are accessible only to organization personnel and require authentication, using at a minimum a unique User ID and Password.

Offsite access is not permitted **OR** Offsite access requires two factor authentication

All devices accessing UCS data are actively managed and are automatically updated. The devices regularly check in, in order to apply operating system and application patches.

All devices accessing UCS data must run anti-virus software with the latest patches and signatures.

Downloading of data to local drives and portable devices is prohibited by (select one):

IT restrictions
Written policy

All devices accessing UCS data must auto-lock after a reasonable period of inactivity with PIN or password required to unlock.

File transfers of individual-level data (if required) will be completed via secure methods such as SFTP or encrypted e-mail.

Custom software is maintained and supported with necessary updates, upgrades, and bug fixes to ensure it remains secure from vulnerabilities.

OR

Our organization does not use custom software.

The network has a firewall, virus monitoring, and intrusion detection systems.

If OCA data will be stored in the cloud:

All cloud servers are located in the United States

The cloud provider is FedRamp certified

The cloud provider meets CJIS Security Policy guidelines

OR OCA data will not be stored in the cloud

Upon a suspected or confirmed Data Breach, Organization shall:

Deliver immediate notice to UCS indicating the dates(s) and scope of the breach and the number and identity of any individual(s) whose Data was, or was believed to be, breached.

Take immediate steps to mitigate and remediate any Data Breach, including, but not limited to, complying, at its sole cost and expense, with all statutory and/or regulatory data breach notification requirements which may arise in connection therewith

Report such steps to UCS in writing on a routine schedule and as may otherwise be requested by UCS

If the organization no longer meets the above, UCS will be notified via email to ocadatarequest@nycourts.gov within 14 days. Otherwise, this form shall be valid for the duration of the agreement.

Signature

Printed Name

Date