ITEM 7.3.0 | DATA EXCHANGE SECURITY

As noted in the Introduction section, version 1.0 of these standards will cover the exchange of data between local CMS, CAPS, and state-level JDMS systems and may include interactions with other state-level systems such as the Comprehensive Case Information System ("CCIS") as appropriate. Subsequent versions of this standard may expand upon and include data exchange between additional systems or stakeholders.

The Data Security Model should contain the following elements:

- Data Storage Encryption: All data stored electronically in locations other than those where the systems are located must also be encrypted, (e.g., an offsite backup facility). This also applies to any data extracted from the CMS with the intention of performing bulk transfers into other systems.

- Workstation Security: All end-user workstations or devices must maintain an up-to-date, industry-standard anti-malware system to protect the information being consumed by the end-user. This may be exempted only in the event that a business case has been developed showing that the end device cannot be kept current. In this event, the organization providing the data must be notified before the exchange.

- Mobile devices: No data may reside in mobile devices beyond the current session. If such a device is deployed or used for the "consumption" of information, a VPN solution must be deployed and managed by the courts.

- Cleaning Hard Disks: If at any moment a portable Hard Disk Drive or similar technology is used to transfer data among systems, the storage device must be sanitized using the DoD 5220.22-M approach.

- Firewalls: Firewalls are required when data must transport through an external network to reach its destination. This will be through a firewall specific source and destination (IP and port) defined in the firewall to prevent unintentional access to source/destination servers.

- User Credentials: When credentials (passwords) are necessary to access or transmit data among systems, the password should be a complex (upper, lower, numeric, and special character) combination password no shorter than 8

characters and renewable every 90 days. Provisions should be taken to deny the reuse of the previous 5 passwords.

• Security Updates: To mitigate vulnerabilities at the host and PC level, systems must have security updates applied frequently (preferably via automatic update); checks to ensure any system is not vulnerable should be performed before bringing it into production.