UNIVERSAL CASE MANAGEMENT SYSTEM

DUTIES AND OBLIGATIONS OF USER ORGANIZATION

4.1 Compliance With Laws, Rules, Etc. User Organization shall comply, and shall ensure compliance by its Authorized Users, with all applicable laws, rules, regulations, restrictions and professional standards pertaining to access to and the use of UCMS Family Web Inquiry and the System Data.

4.2 Compliance With Agreement/Terms of Use. User Organization shall take all necessary steps to ensure compliance by its Authorized Users with the terms and conditions of this Agreement and the Terms of Use. User Organization shall familiarize its Authorized Users and other related personnel with the limitations on access to UCMS Family Web Inquiry and use and dissemination of System Data, and security measures required to be followed in connection therewith.

4.3 Internal Access Compliance. User Organization shall take such necessary measures as may be required to ensure only Authorized Users have access to UCMS Family Web Inquiry.

4.4 Change of Authorized User Status. User Organization *must immediately provide to UCS, via UCS Security Administration Unit Email Address*, the name of any Authorized User who is no longer employed by User Organization (as the term, "employee" is used in Section 3.1 herein), or who changes job functions so that the employee no longer performs a function related to a Permitted Purpose.

4.5 System Data Security. User Organization shall take all reasonable measures to keep access to UCMS Family Web Inquiry and System Data contained in any medium or location, physically and electronically secure from unauthorized access. Such measures shall include, but not be limited to:

(i) maintaining a firewall, password access and encryption to restrict access to UCMS Family Web Inquiry and System Data;

(ii) storing hard copy and removable media containing System Data in locked areas with restricted access; and

(iii) u t i l i z i n g up-todate encryption technology in file transfer or other access mechanisms sufficient to prevent unauthorized access to UCMS Family Web Inquiry and System Data. User Organization may not copy, backup or otherwise archive System Data for any purpose other than its Permitted Use.

4.6 User Organization and Authorized User Computers/Devices. Any device used by an Authorized User to access UCMS Family Web Inquiry must be secure and must meet the below minimum standards:

• *Actively managed device*: Device must be automatically updated. The device must regularly check in, in order to apply operating system and application patches.

• *No unsupported applications*: Device may not be running any vendor unsupported applications.

• *Encrypt device*: Device hard drives and storage must be encrypted using modern/accepted encryption algorithm.

• *Use PIN*: Device must auto lock after a reasonable period of inactivity with PIN or password required to unlock.

• *Not jailbroken*: Device must be running vendor supported operating system and not be compromised or jailbroken.

• *Anti-virus*: Device must run anti-virus software with the latest patches & signatures.

UCMS Help Center (800) 622-2522.