

Security for UTCFS Information Stored by Supplier (1/07)

1. UTCFS and UTCFS Participating Site wishes to ensure that Supplier has effective information security to allow the proper and secure storage and/or processing of UTCFS Information (as defined below) at Supplier's facility and to facilitate the exchange of information between UTCFS Participating Site and Supplier. As used in this provision, "UTCFS Information" means (i) information owned by UTCFS or a UTCFS Participating Site; (ii) information managed by UTCFS or a UTCFS Participating Site; (iii) information that UTCFS or a UTCFS Participating Site is obligated to manage and protect on behalf of others; and (iv) personally-identifiable information relating to an identified or identifiable employee of UTCFS or a UTCFS Participating Site or others that is protected by various privacy laws (current or future) as applicable throughout the world including, without limitation, Social Security number, address, telephone number, gender, birth date, medical records, trade union membership, driver's license number, financial account number, credit or debit card number (all subsection iv) defined as "PII").
2. Supplier agrees to install and implement security hardware, software, procedures and policies that will provide effective information security. Supplier agrees to update such hardware, software, procedures and policies as may be needed from time to time to utilize improved technology and to respond to more sophisticated security threats in order to maintain a level of security protection appropriate for the information involved and the current state of security solutions. Upon request, Supplier shall provide UTCFS with any audit reports issued under the *Statement on Auditing Standards (SAS) No. 70, Service Organizations, type II*, issued by the American Institute of Certified Public Accountants.
3. Supplier further agrees to:
 - (i) Provide to UTCFS a copy of its current information security policy, including its policy regarding physical security for access to devices that may access UTCFS Information. Supplier shall annually provide UTCFS with its then current policy and indicate any plans, including a timetable for implementation, of planned upgrades to comply with the policy. Supplier shall implement those reasonable requests for modification of such policy requested by UTCFS.
 - (ii) Allow UTCFS or its designee to conduct a security audit at its facilities on one days notice, and allow UTCFS at any time to conduct (or have conducted) a remote network audit. If the UTCFS

Information is stored in a shared environment per the agreement of UTCFS, then UTCFS shall use a third party to conduct such audits. The audits shall include any facilities with UTCFS Information including backup storage facilities.

(iii) Segregate all UTCFS Information into a separate database only accessible by UTCFS and its agents and those employees of Supplier necessary to maintain the equipment and the program on which it runs, unless otherwise agreed by UTCFS. Except for UTCFS and its agents, Supplier shall use reasonable efforts, as measured by the available technology at the time, to prevent anyone other than its authorized employees from accessing the UTCFS Information.

(iv) Assure that all UTCFS Information and applicable software is appropriately backed up and recoverable in the event of a disaster.

(v) Encryption Requirements. The following requirements apply when supplier has possession of UTCFS Information. Encryption algorithms used must be of sufficient strength to equate to 128-bit RC-4 or better. All cryptography technologies used must be published and approved by the general cryptographic community.

(a) Encrypt all UTCFS Information stored on Supplier computer systems and backup media.

(b) Encrypt all UTCFS Information transferred across public networks

(c) Encrypt all UTCFS Information stored on Supplier mobile computing devices (e.g. laptop computers, PDAs (personal digital assistants), etc.)

(vi) Notwithstanding any provision to the contrary herein, PII as defined in subsection 36.1 iv) shall not be stored on any Supplier mobile computing devices (e.g. laptop computers, PDAs (personal digital assistants), etc.)

(vii) Conduct appropriate background checks on all non-UTCFS personnel who will have access to the environment and/or UTCFS's data and approve those personnel based on the results of those checks. Supplier must disclose to UTCFS the procedures used for those employees having access to the UTCFS Information.

(viii) Provide UTCFS at the time of signing this contract with a termination plan that addresses how UTCFS Information will

be returned to UTCFS at the end of this agreement, including backup and archival information, and how all UTCFS Information will be permanently removed from Supplier's equipment and facilities. This plan should include supplying the data to UTCFS in an industry recognized non-proprietary database and, if not, a license to use the proprietary data base software to access the data.

- (ix) Describe at the time of signing of this agreement how Supplier will meet UTCFS's requirement for two (2) factor authentication access for access to UTCFS Information or, for less sensitive information, where "Strong Password" data control is sufficient, describe how this requirement will be met.
 - (x) Provide information and cooperation to UTCFS in response to any subpoena, investigation or the like seeking UTCFS Information and provide information and assistance for UTCFS to seek certification and the like relative to its information including information in the possession of Supplier. Supplier shall promptly notify UTCFS upon the receipt of any request requiring that UTCFS Information be supplied to a third party.
 - (xi) Comply, within a reasonable period of time, with UTCFS Information security policies as amended from time to time.
4. Supplier shall not provide UTCFS Information to any other entity without the prior written approval of UTCFS. A request for UTCFS approval shall include agreement by Supplier and such other entity that all of the requirements of this provision are applicable to their performance and that UTCFS shall have the right to perform the audits described above.
 5. Should Supplier fail to meet the then current standards for information security, or should Supplier fail to pass a UTCFS audit on information protection, then UTCFS may immediately terminate this MTA and/or a Releases without prejudice to any other rights or remedies and shall have no further obligation to Supplier other than to pay for Deliverables delivered to that date. UTCFS may identify the failures to Supplier and Supplier shall within thirty (30) days provide UTCFS with a plan to remedy those failures and, if requested by UTCFS, shall take certain applications off line until the issues have been resolved. If the risks identified by UTCFS are not remedied within the time frame specified by UTCFS, or if Supplier refuses to remedy the risks, then UTCFS may immediately and as of right terminate this MTA and/or Releases without prejudice to any other rights or remedies.