Xtender Imaging Payment Card Industry Data Security Standards (PCIDSS) Compliance Policy Agreement

Scope: All documents stored in the Xtender imaging system

Audience: All Xtender user departments at TTU System, TTU, and HSC

Policy Statement: All Xtender user departments must refrain from storing the full Primary Account Number and other related payment card information on imaged documents in order to comply with the Payment Card Industry Data Security Standards (PCIDSS). This policy agreement pertains to, but is not limited to, credit cards, debit cards, and procurement cards used for personal and/or business transactions.

Procedures: A department's imaged data must remain PCIDSS compliant at all times. Causes of noncompliance are:

- Storing a document containing a fully unmasked or improperly masked Primary Account Number
- Storing a document containing a CVV validation code (commonly found on the back of payment cards)
- Failing to destroy documents as required by applicable federal, state, or institutional retention policies
- Storing documents or engaging in other behavior forbidden by the current version of the PCIDSS (https://www.pcisecuritystandards.org)

If a department's folder(s) are found to contain noncompliant data, the following steps will be taken for the data and department to become PCIDSS compliant.

- All improperly stored Primary Account Numbers and CVV validation codes must be permanently and irrefutably destroyed. This must be accomplished through the TTUS Information Systems Department.
- For PCIDSS compliance, the following guidelines should be followed:
    - When using permanent markers or other writing instruments, care must be taken to ensure noncompliant information is fully destroyed and not merely rendered less readable.
    - Noncompliant information cannot be "redacted" simply by overlaying the noncompliant data using annotations subsequent to scanning or importing into the imaging system.
    - All image layers and/or other constructs intended to cover noncompliant information must be permanently merged into the document in order to prevent removal.

  - All imaging user departments must alter business processes to avoid the creation of noncompliant documents that could potentially be stored in the imaging system.
- Documents must be deleted according to all applicable retention policy guidelines
  - Reviews for newly eligible documents should be held at least once per year.
  - Documents exceeding retention policy requirements greater than one year are subject to automatic deletion or an alternate form of archival.
- Any other behavior contrary to the PCIDSS must be corrected.

<u>User Department Responsibilities</u>

- User departments are fully responsible for ensuring that all documents in the imaging system are PCIDSS compliant.
- User departments are fully responsible for any and all costs associated with the removal of documents that are not compliant with PCIDSS from the imaging system, including but not limited to the outsourcing of permanent redactions to a third-party contractor.
- For cases involving over 100 documents that are not in compliance with PCIDSS, the user must submit a cleanup proposal to the CIO Council through the Xtender imaging team or through their respective CIO.

Xtender Imaging Payment Card Industry Data Security Standards (PCIDSS) Compliance Policy Agreement

By providing my signature below, I acknowledge I have read and accept the Xtender Imaging PCIDSS Compliance Policy Agreement and understand that I am subject to additional requirements as outlined in the PCIDSS. In addition, if any folders, at any time, under my responsibility are found to contain documents that are not in compliance with PCIDSS, my department will be responsible for funding the permanent redaction process.

Department Head (Director/Chair Person)

Signature ____ Date ______________________

Title ____

Area Representative (Associate Vice President/Chancellor, Vice President/Chancellor, Dean)

Signature ____ Date ______________________

Title ____