SECTION XI | CLERK SECURITY

No sensitive security information should be presented on the user interface. Sensitive data shall be exchanged over trusted paths or by using adequate encryption between users; between users and systems; and between systems. The system must employ appropriate security and encryption measures to prevent disclosure of confidential data to unauthorized persons.

Minimum Technical Requirements:

1. Encryption (general public and authenticated)**;
2. No "cutting and pasting" of workable links;
3. Hyperlinks must not include authentication credentials;
4. No access to live data, replicated records will be used for public access;
5. Authenticated access for access beyond general public access; and
6. Monitor bulk data transfers to identify and mitigate abuses of the system by utilizing access programs using automated methods.

**Encryption protects the integrity of the record and prevents exposure to potential security risks. It also prevents authenticated users with higher access from sending links to information to non-authorized users.