EIV System Security Measures

The practices and controls used by HUD and program administrators to secure UIV data that is contained in the EIV system may be grouped into three categories: technical, administrative, and physical safeguards. An Owner/Agent (O/A) may implement a combination of technical, administrative, and physical safeguards that meet acceptable standards for the protection provided by the specific safeguard and accomplish the purpose of the safeguards. At a minimum, an O/A must:

Technical safeguards

1. Reduce the risk of a security violation related to the EIV system's software, network, or applications.
2. Identify and authenticate all users seeking to the EIV system data.
3. Deter and detect attempts to access the system without authorization.
4. Monitor the user activity on the EIV system.

Administrative safeguards

1. Ensure that access rights, roles, and responsibilities are appropriately and adequately assigned.
2. Protect copies of sensitive data and destroy system-related records to prevent reconstruction of the contents.
3. Ensure authorized release of tenant information consent forms are included in all family files, before accessing and using data.
4. Maintain, communicate, and enforce standard operating procedures related to securing EIV data.
5. Train staff on security measures and awareness, preventing the unauthorized accessibility and use of data.

Physical safeguards

1. Establish barriers between unauthorized persons and documents or computer media containing private data.
2. Clearly identify restricted areas by use of prominently posted signs or other indicators.
3. Develop a list of authorized users who can access restricted areas-e.g., contractors, maintenance, and janitorial/cleaning staff.
4. Prevent undetected entry into protected areas and/or documents.
5. Notify Coordinators/Security Administrators of system breaches and penetration by unauthorized users.