**General Policy Note**

**AC-1 Access Control Policy and Procedures:** This control is inherited from CIT.

**AC-6 Least** **Privilege**: Permission within the system are based on group membership, and role and responsibility consummate to an individual position.

**AC-7 Unsuccessful Login Attempts:** The system enforces a limit of 3 consecutive invalid access attempts by a user in a 15-minute period. The system automatically locks the account for one hour. The account must be released by an administrator to be unlocked before one hour.

**AC-8 System Use Notification:** The system displays the CIT -approved notification message before granting access. The banner states user responsibilities, and the purpose of the system.

**AC-10 Concurrent Session Control:** The system limits the number of concurrent sessions for each system account to one (1).

**AC-14 Permitted Actions without Identification or Authentication:** No action can be performed by system users without identification and authentication.

**AT-1 – Security Awareness and Training Policy and Procedures:** This control is inherited from CIT.

**AT-2 – Security Awareness and Training:** This control is inherited from CIT.

**AT-4 – Security Awareness and Training Record:** Security Awareness Training completion logs are kept by the Information System Security Officer for a period of one year in accordance with CIT Security Awareness Policy.

**AU-1 – Audit an Accountability Policy and Procedures:** This control is inherited from CIT.

**AU-3 – Content of Audit Records:** The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

**AU-6 – Audit Review, Analysis, and Reporting:** Audit log reviews are conducted on monthly basis and the frequency of audit log review is increased to bi-weekly if the system risk level is increased.

**CP-1 – Contingency Planning Policy and Procedures:** This control is inherited from CIT.

**CP-3 – Contingency Training:** CRT management trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training on annual basis.

Contingency training records are maintained by the Information System Security Officer for a period of one year.

**IA-1 – Identification and Authentication Policy and Procedures:** This control is inherited from CIT.

**IA-2 – Identification and Authentication (Organizational Users):** The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Users access CRT through an FTP client (FileZilla) installed on their laptop by entering the Hostname/Host IP, Username, Password and Port.

**IA-6 – Authenticator Feedback:** The system obscures feedback of authentication information during the authentication process. The authentication data (password) appears as dots.