2.5.2 Key Control Logs

(1) Key control logs must be maintained for keys listed in 2.5.1 above.

(2) All key control logs must contain, at a minimum, with the ability to electronically or manually record, the following information for each of the keys mentioned in paragraph 2.5.1 above:

(a) Date and time the keys are obtained;

(b) Electronic ID or signature, printed name and company identification number of the custodian releasing the keys;

(c) Electronic ID or signature, printed name and company identification number of the person obtaining the keys;

(i) In the event that a key is required outside of approved clearance times, the reasons for the use and removal of the key; and,

(ii) Date and time the keys are returned to the custodian;

(d) Electronic ID or signature, printed name and company identification number of the person returning the keys; and

(e) Electronic ID or signature, printed name and company identification number of the custodian receiving the keys.

(3) Key control logs, electronic or manual books, must be periodically forwarded to the Internal Audit function for scrutiny and retention. Electronic logs must be printed and filed for audit purposes.

(4) (a) All entries in the manual keys control logs must be in indelible ink or some other form of permanent record.

(b) (i) Electronic format must have read-only access to users for audit purpose.
(ii) All personnel required to utilize the electronic key cabinets, must complete an application, for approval by the Surveillance and Security department Managers.
(iii) All approved user applications must be filed for a period of 5 years.
(iv) Access levels to be contained in the licensees ICS.