3.5 Physical Security

What happens if a thief breaks into Government Office and steals classified data?

3.5.1 Perimeter Control

Policy Premises housing critical government information processing facilities must be protected from unauthorized access, damage and interference.

Standard Implement perimeter controls at all premises housing critical government information processing facilities.

Procedure

(1) External walls constructed from the real ceiling where needed of premises housing critical government information processing facilities must be of solid construction.

(2) Fire doors should be equipped with alarms and should automatically slam shut.

(3) Buildings should be protected with secure doors, grills and locking hardwares where appropriate

(4) Place a manned reception area or other means to control physical access to buildings. Access to buildings is restricted to authorized personnel only.

Guidelines

(1) The criticality of the information processing facilities shall be decided by the organization concerned.

(2) Solid construction for premises must follow construction/security standards based on :

i. JKR General Specification for Building Works.
ii. Arahan Keselamatan Negeri Sabah, Bab Keselamatan Fizikal (II-Keselamatan Bangunan)
iii. Relevant authorities Building-bylaws.

What happens if an unauthorized personnel enters Government premises and steals classified information?

3.5.2 Access Control

Policy All premises housing critical government information processing facilities should be designated as restricted areas.

Standard Access privileges for persons to restricted areas should be given on a need to enter basis.

Procedure

(1) Those who need access to restricted areas must wear a security pass, of which type is determined by the following classification :

a. Permanent - Persons who work permenantly in restricted areas must be issued with and wear a permenant security pass at all times.

b. Temporary - Persons who do not work permenantly in restricted areas but require entry to carry out official duties must be issued with and wear a temporary security pass during the duration of the work.

c. Visitor - Persons from outside who are on official visit to restricted areas must be issued with and wear a visitor security pass and escorted by authorized personnel during the duration of the visit.

(2) For each temporary and visitor entry, an access control log should be used to record the following information :

i. Name and NRIC number of the person(s) entering
ii. Employer or affiliation
iii. Name of the escorting person(s)
iv. Restricted area to be entered
v. Purpose
vi. Signature
vii. Date and time of entry
viii. Date and time of departure.

(3) The number of visitors to restricted areas must be limited accordingly to minimize security risk.

(4) The security pass must be returned upon exit from restricted areas.

(5) Lost of secuirty pass must be reported immediately.

(6) Access controls should be applied at all restricted areas by using security identification mechanism such as swipe cards, biometrics, etc.

(7) Surveillance devices such as CCTV, motion detectors and alarms should be installed in all restricted areas. The CCTV should be monitored at all times.

(8) Installation of signs boards indicating "**authorized personnel only**" or a similar message should be prominently posted at all entrances to restricted areas.

Guideline

(1) The criticality of the information processing facilities shall be decided by the organization concerned.