

Physical Perimeter: Security & Defense



“Defensive Depth”

Defensive Depth combines several layered processes which make unauthorized access difficult, if not impossible, for an individual without a “right to know”. These measures complement and support one another and are designed to meet the threat to security posed by someone who has already gained access to the site, building or secure zone, rather than the intruder from outside.

Physical Security contains five distinct elements:

- Delay/Deterrence - fencing, gates, vehicle barriers, access card systems and security personnel
- Detection - alarm systems monitoring access points, CCTV and motion detection equipment
- Assessment - standard processes to determine threat levels
- Communication - redundant systems allowing information to be transmitted and received
- Response - coordinated reactions to mitigate threat situations

The purpose of a Security Perimeter is to physically or psychologically deter intruders.

Facilities that store or process sensitive materials or equipment should have as few access points as safety and the functions of the site allow.

Intrusion-detection systems (IDS):

IDS are designed to detect actual or attempted unauthorized entry, identify its location and signal a response with an alarm. These systems can provide continuous surveillance over secure areas and extend coverage into areas inaccessible to guards.

Survey to secure all possible means of access

Security surveys should be repeated at established intervals, or whenever the facilities use, its contents or the national security threat level changes. Assessments should consider security vulnerabilities from neighboring premises and should rate the level as resistance to forced entry. Ensuring a secure environment requires the cooperation of employees and all support staff in identifying actual or suspected security violations.