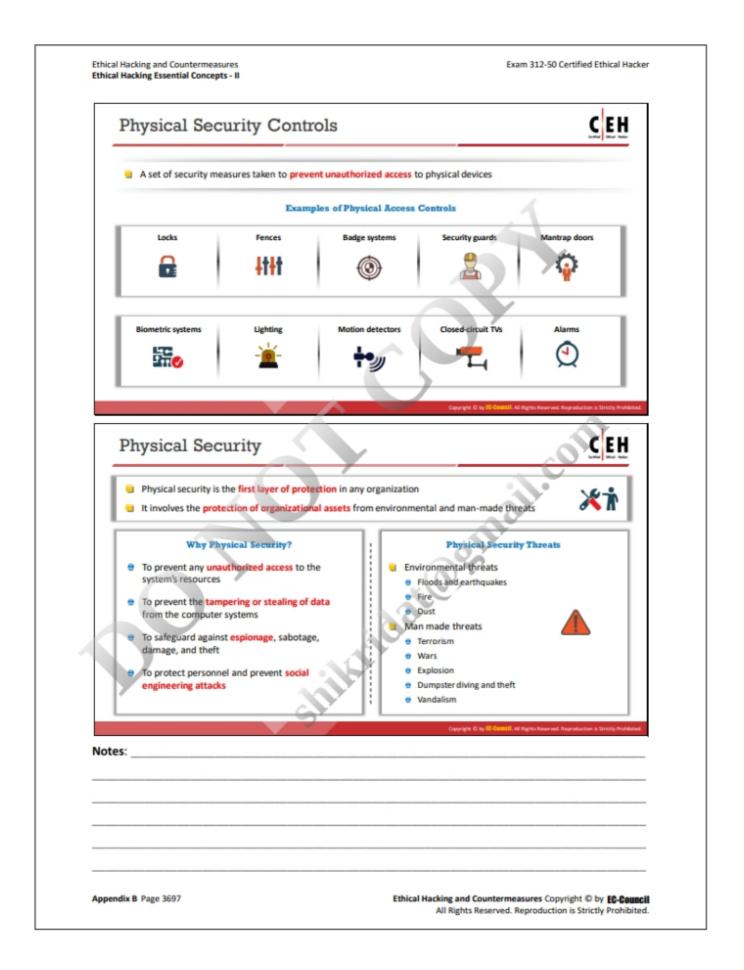
Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.



Printed by: shikridat@gmail.com. Printing is for personal, private use only. No part of this book may be reproduced or transmitted without publisher's prior permission. Violators will be prosecuted.

CEH Types of Physical Security Controls Prevent security violations and enforce various access control mechanisms Controls Examples include door lock, security guard, and other measures Detect security violations and record any intrusion attempts Detective Examples include motion detectors, alarm systems and sensors, video surveillance, and other Controls methods Used to discourage attackers and send warning messages to the attackers to discourage intrusion Deterrent Controls Examples include various types of warning signs Used to recover from security violation and restore information and systems to a persistent state Recovery Controls Examples include disaster recovery, business continuity plans, backup systems, and other processes Used as an alternative control when the intended controls failed or cannot be used Compensating Controls Examples include hot sites, backup power systems, and other means

Physical Security Controls



	Colul State
Premises and company surroundings	Fences, gates, walls, guards, alarms, CCTV cameras, intruder systems, panic buttons, burglar alarms, windows and door locks, deadlocks, and other methods
Reception area	Lock up important files and documents Lock equipment when not in use
Server and workstation area	Lock the systems when not in use, disable or avoid having removable media and DVD-ROM drives, CCTV cameras, and workstation layout design
Other equipment such as fax, modem, and removable media	Lock fax machines when not in use, file received faxes properly, disable moderns' auto answer mode, do not place removable media in public places, and physically destroy corrupted removable media
Access control	Separate work areas, implement biometric access controls (fingerprinting, retinal scanning, iris scanning, vein structure recognition, facial recognition, voice recognition), entry cards, man traps, faculty sign-in procedures, identification badges, and other means
Computer equipment maintenance	Appoint a person to look after computer equipment maintenance
Wiretapping	Routinely inspect all wires carrying data, protect the wires using shielded cables, and never leave any wires exposed
Environmental control	Humidity and air conditioning, HVAC, fire suppression, EMI shielding, and hot and cold aisles

Notes:			