

Data Center Physical Infrastructure - Space

PHYSICAL SECURITY · SECURITY POLICY · LAYERED ACCESS · ACCESS MANAGEMENT · CCTV & RFID · WHITE & GRAY SPACE · SPACE OPTIMIZATION

STUDY & REVIEW

01 MUST KNOW

if you remember five things, remember these

- 01 Three kinds of security:** every data center layers **data security** (protects stored information), **network security** (protects the network elements and their end connectivity), and **physical security** (protects the facility and equipment from theft and damage and keeps unauthorized people out). This module is about physical security — and good protocols need a blend of **technology, automation, and human intervention**.
- 02 Layered security:** a clearly defined physical security *policy* comes first. **Layered security** then places a level of protection at every access-control gate, from the perimeter main gate to the server room, so no one reaches the inner layers unchecked. Its two elements are **access management** and **technology-based security**.
- 03 Access management + tech measures:** access management has three parts — **access list** (who may enter), **secure access points** (badged entry, secured doors, animal traps), and **biometric access** (fingerprint, voice, face). Technology-based measures add **video surveillance (CCTV)** and **RFID** asset tracking.
- 04 White vs gray space:** **white space** houses all IT equipment — servers, storage, racks, network devices — and is the *productive*, revenue-generating area. **Gray space** houses the electrical and mechanical backend that supports it: **cooling systems, switchgears, generators, UPSs, and chillers**.
- 05 Optimize, don't overcrowd:** space demand always grows, but a data center cannot expand forever — so optimize the *existing* space. Overcrowding generates more heat, demands more cooling, and raises cost while lowering efficiency. Gray space is sized in **proportion** to the white area, so growing one grows the other.

02 KEY TERMS

TERM	DEFINITION
Physical security	Protection of a data center's physical infrastructure from internal and external threats — theft, damage, and unauthorized entry
Security policy	Defines the protocols and procedures for physically accessing a data center; applies to vendors, utility staff, and security personnel
Layered security	Provides a level of security at each access-control gate, from the perimeter main gate to the server room
Access list	Determines who can access data center premises and equipment; updated weekly, monthly, or whenever access changes
Secure access points	Measures that restrict entry to sensitive zones — badged entry, secured doors, animal traps, and proximity-alert zones
Biometric access	Uses personally identifiable physical or behavioral attributes (fingerprint, voice, face) to identify a person and grant access
Video surveillance (CCTV)	Closed-circuit television that records activity on the building's exterior and interior walls for incident reporting
RFID	Radio-frequency identification; tracks assets from a central server and alerts staff to tampering or due maintenance
White space	The area dedicated to IT equipment — servers, storage, racks, network devices — the productive area of the data center
Gray space	The area for backend support systems — cooling systems, switchgears, generators, UPSs, and chillers

TERM	DEFINITION
DCIM	Data center infrastructure management software used for estimates, predictive analysis, and cost-efficient methods
Economizer mode	A cooling alternative that uses outdoor air in colder months so chillers and compressors run reduced or off — less investment and running cost

03 TWO ELEMENTS OF LAYERED SECURITY

they work together to secure the data center

ACCESS MANAGEMENT <i>who gets in — and how it's verified</i> — Access list — who may enter (employees, guards, contractors); updated weekly/monthly — Secure access points — badged entry, secured doors, animal traps; proximity-alert zones — Biometric access — fingerprint, voice, face; logs entry/exit; national-ID background checks	TECHNOLOGY-BASED SECURITY <i>automation that watches and tracks</i> — Video surveillance (CCTV) — records exterior/interior walls; pan, zoom, freeze; backed up, remote — RFID — alerts on tampering or due maintenance; tracks assets from a central server, no scan needed
--	---

04 LAYERED SECURITY — PERIMETER TO CORE

a checkpoint at every zone

01 Main gate / perimeter → 02 Parking lot → 03 Lobby & administrative space → 04 Lift & utility rooms → 05 Server room (innermost)

05 WHITE SPACE VS GRAY SPACE

which equipment lives where

DIMENSION	WHITE SPACE	GRAY SPACE
Houses	All IT equipment — the productive area	Electrical & mechanical backend support
Examples	Servers, storage, racks, network devices, power distribution systems, AC units	Cooling systems, switchgears, generators, UPSs, chillers
Role	Runs the workloads that generate revenue	Powers, cools, supports — and monitors — the white space
Sizing	Maximize during initial design; more white space, more revenue	Sized in proportion to the white area; grows as servers grow

06 STRATEGIES TO OPTIMIZE SPACE USE

match the strategy to the space

SPACE	STRATEGIES
White space	Virtualization software · DCIM infrastructure-management tools · proper planning · use of the cloud · adopting SSDs · avoiding old power strips for new equipment
Gray space	Momentum captured by flywheels during power fluctuation · solar energy where climate allows · cooling alternatives (economizer modes)

- × “White space is empty or wasted space.” — The opposite: white space is the **productive** area that houses all IT equipment, and more white space means more revenue.
- × “Gray space is just overhead you can shrink at will.” — Gray space holds the electrical and mechanical backend (cooling, switchgears, generators, UPSs, chillers) that keeps the white space running, and it is sized in **proportion** to the white area.
- × “Adding buildings or locations is the best way to grow white space.” — Each new white space needs an equivalent new **gray** space, which raises cost; virtualization and more efficient equipment are the better route.
- × “Biometric access only unlocks doors.” — It also **records entry and exit times** and can verify a person's background when connected to national ID systems.
- × “Layered security means one strong gate at the entrance.” — It places a level of security at **every** access-control gate from the perimeter to the server room, so the innermost layers stay protected.
- × “A UPS and a power distribution system belong to the same space.” — A **UPS is gray space** (backend support); a **power distribution system is white space**, alongside the servers it feeds.
- × “Reducing power fluctuations is a white-space optimization.” — It is not. White-space strategies are virtualization software, DCIM tools, proper planning, the cloud, SSDs, and avoiding old power strips.
- × “Old power strips are fine to reuse on new equipment.” — New devices have different specifications; use the power strips their specs recommend. Reusing old strips is a common, avoidable mistake.

08 SELF-QUIZ

answers are upside-down below

Q1 What are the three main kinds of security every data center needs?

Q2 Layered security is built from two main elements — name them.

Q3 List the three parts of access management.

Q4 Which technology-based measure records activity on closed-circuit television to protect a building's exterior and interior walls?

Q5 Which technology-based measure tracks assets from a central server and alerts staff when an asset ID is tampered with or due for maintenance?

Q6 Which data center space category is dedicated to IT equipment such as servers and racks?

Q7 Name three types of equipment found in gray space.

Q8 The size of the gray area is determined by what?

Q9 Why should a data center optimize existing space instead of overcrowding equipment?

Q10 Sample exam: which THREE optimize white space use — DCIM tools, using the cloud, avoiding old power strips, reducing power fluctuations, solar energy, or cooling alternatives?

ANSWER KEY (rotate the page)

Q1 Data security, network security, and physical security **Q2** Access management and technology-based security **Q3** Access list, secure access points, and biometric access **Q4** Video surveillance **Q5** RFID (radio-frequency identification) **Q6** White space **Q7** Any three of: cooling systems, switchgears, generators, UPSs, chillers **Q8** The size of the white space it supports **Q9** Overcrowding generates more heat, which requires more cooling and increases cost while lowering efficiency **Q10** DCIM tools, using the cloud, and avoiding old power strips for new equipment