

DATA CENTER TERMINOLOGY & DEFINITIONS

A guide to common language used to describe data centers and the security of data center facilities

INCLUDING: FACILITY TYPES | INFRASTRUCTURE
OPERATIONS | ENVIRONMENTAL SYSTEMS

SIA
SECURITY INDUSTRY ASSOCIATION

securityindustry.org

INTRODUCTION

The Security Industry Association (SIA) Data Center Advisory Board was established to strengthen data center security through expert collaboration, industry leadership and policy engagement. As digital infrastructure is essential to modern life, the need for practical, credible and broadly applicable security guidance has never been greater.

Data centers are foundational to nearly every other critical infrastructure sector, supporting the systems behind communications, finance, health care, transportation, government services and energy. Clear security guidance for these facilities depends on a shared understanding of the terms used to describe them.

As chair of the Data Center Advisory Board, I am pleased to introduce the Data Center Terminology and Definitions. This document is intended for the security industry, and particularly for data center security professionals, as a common reference for the terminology used to describe data center sites, environments and the physical security measures that protect them.

Owners, operators, integrators, manufacturers and consultants often use the same terms to mean different things, leading to confusion and inconsistent expectations. These definitions reduce that ambiguity and, where possible, align with terminology used across other critical infrastructure sectors.

Readers should use these definitions alongside the SIA Data Center Security Principles guidance document. The "Principles" document describes what effective physical security should achieve, and this "Definitions" document clarifies the terms used to express those ideas.

Together, they further set the foundation for the Data Center Advisory Board's upcoming work on physical security best practices for data centers. By establishing a common vocabulary now, we build toward more detailed and actionable guidance that helps organizations strengthen protection, improve consistency and adapt to evolving threats.

I sincerely thank the members of the Data Center Advisory Board for their expertise, thoughtful contributions and continued support in shaping this work.

Jim Black, CPP, PSP, CISSP
Chair, SIA Data Center Advisory Board

SIA DATA CENTER ADVISORY BOARD

The Security Industry Association (SIA) Data Center Advisory Board develops information and guidelines related to security deployments, facilitates collaboration between the security industry and data center security practitioners, and works with the SIA Government Relations team on legislative and regulatory issues, where appropriate.

Learn More and Explore Resources

TABLE OF CONTENTS

1 **Category 1**
Facility Types and Deployment Models 3

2 **Category 2**
Infrastructure, Power and Resiliency 5

3 **Category 3**
Operations and Physical Security 7

4 **Category 4**
Cooling and Environment Systems 9

More Resources 11

1 CATEGORY 1 FACILITY TYPES AND DEPLOYMENT MODELS

AI Data Center
A purpose-built computing facility designed to support the high-density, high-performance infrastructure required for artificial intelligence (AI) and machine learning workloads, including graphics processing unit (GPU) clusters, specialized interconnects, high-bandwidth storage and low-latency networking. Unlike traditional data centers, it is optimized for massive parallel processing, rapid data movement, advanced thermal management such as liquid cooling and flexible architectures that can adapt to different AI workload requirements.

Availability Zone
One or more physically separate data centers within a cloud region that have independent power, cooling and networking. Availability zones help maintain service continuity if one site experiences an outage.

Cable Landing Station
Facility where undersea fiber optic cables make landfall and connect to terrestrial networks. These specialized facilities are engineered with rigorous technical and security specifications to manage the complex transition of high-capacity data transmission from undersea environments to continental communication grids.

Carrier Hotel/Internet Exchange Facility
Colocation facility with a high concentration of telecommunication carriers and network providers. Allows different telecommunications providers to directly interconnect their networks through physical infrastructure known as meet-me rooms. These dedicated spaces provide a neutral ground where lessees can establish direct peering relationships, dramatically reducing data transmission costs and latency compared to traditional routing methods.

Cloud Region
A geographic area containing one or more data centers connected through high-speed networks. Cloud regions provide redundancy, performance and compliance capabilities for customers.

Colocation
A colocation (colo) data center is a facility where customers can lease (rent) physical space to house their own servers, networking gear and other information technology (IT) hardware. Instead of building and maintaining its own data center, customers place their equipment in a third-party facility that provides power, cooling, bandwidth and physical security of the site/facility. In this model, hardware remains owned by the lessee customer, while the colocation provider ensures the environment is optimal for uptime and may also service and maintain customer equipment. Lessees may manage physical security of the spaces being leased and the business assets therein. This setup is especially useful for users that need control over their assets and infrastructure but want to avoid the high costs of building and operating an enterprise data center.

Critical Infrastructure
A facility or system whose disruption could significantly impact economic security, public safety, government operations or national security. Large cloud and data center environments are increasingly viewed as critical infrastructure.

Data Center (Also Datacenter, Data-Center)
A specialized facility that houses the computing infrastructure needed to run digital services, store data and process information. The facility typically includes servers, networking equipment, storage systems, power systems and cooling infrastructure. The facility may be a free-standing structure, a grouping of freestanding structures or a facility within a larger structure.

©2026, Security Industry Association. All Rights Reserved.

Edge Data Center
Typically smaller facilities positioned closer to end users or data sources to reduce network latency. Unlike hyperscale data centers, edge sites are intentionally distributed across many disparate locations rather than consolidated into larger sites, with deployments occurring closer to population centers.

Enterprise
Owned and operated by a single organization for its own internal IT needs, rather than for commercial hosting of other companies' data.

Hyperscale
Largest facilities in terms of land and power usage. Designed to support massive, cloud service and computing workloads, AI training/inference, data storage and processing.

Hyperscaler
An organization that owns or operates cloud infrastructure at global scale and can rapidly scale compute, storage and networking resources through highly standardized, automated and distributed data center architectures.

Micro Data Center
Smallest footprint, often remote/unattended, placed closest to users.

Modular (Containerized) Data Center
A data center consisting of equipment contained within shipping containers or similar portable containers. Components of the data center can be prefabricated and standardized, which may speed up deployment and facilitate moving if needed.

Neocloud
A cloud infrastructure provider specializing in AI, machine learning and high-performance computing workloads through the delivery of GPU-centric compute, AI-optimized networking, and high-density data center infrastructure. Unlike hyperscale cloud providers, neoclouds focus primarily on GPU-as-a-service and AI compute capacity rather than broad enterprise cloud services.

Retail Colocation
Facilities comprised of a number of smaller internal areas such as segregated racks or cages. Segregation often includes physical and/or logical barriers.

Social Permission
The public trust and community support necessary for data center development and operation, earned by demonstrating that the facility provides meaningful economic and societal benefits while responsibly managing its impacts on energy, water, land use and local infrastructure.

Sovereign Cloud
Exists within a defined geographical boundary of a nation, is deployed to meet the unique requirements of that nation, is strictly isolated from any other cloud services and may not be accessible from outside of that boundary.

Wholesale Colocation
A facility comprised of larger internal areas (suites/halls/floors) within a third-party-owned and operated site. Customers are more likely to control access into their leased premises and in some cases may sublease space to business partners. The facility owner remains responsible for critical environment systems serving these spaces (water/power/cooling), while lessees sometimes control physical security and maintenance of business assets therein.

2 CATEGORY 2 INFRASTRUCTURE, POWER AND RESILIENCY

2N Redundancy
Fully redundant system with two independent, complete paths for power and cooling, each capable of carrying 100% of the demand.

Automatic Transfer Switch (ATS)
An electrical switching device that automatically transfers load from the primary utility source to a backup power source when a power failure is detected, then transfers the load back when utility power is restored.

Cold Site
A leased or owned facility with fundamental utility infrastructure (i.e., electrical capacity, cooling systems and telecommunications connectivity) without pre-installed servers, networking gear or preconfigured data storage systems. When a primary data center fails, organizations must rapidly procure, transport and deploy critical hardware to transform the cold site into a functional recovery environment. This process can take days or weeks, depending on equipment availability and technical complexity.

Commissioning/Integrated Systems Testing
The process of validating that all critical building and operational systems function properly before a facility enters operational use (production).

Data Center Infrastructure Management
Software used to monitor and manage power, cooling, capacity, assets and environmental conditions within a data center.

Data Hall (Also Server Room, Computer Room, Colocation, Colo)
The secure area (typically a segregated room) where server racks and networking equipment are installed and operated.

Generator
Diesel or natural gas engine converting fuel to electricity for backup power. Failsafe against power disruptions that could catastrophically interrupt operations. These machines are engineered to quickly avoid potential downtime by providing continuous electrical supply, bridging critical gaps during utility power failures.

Gigawatt (GW)
A unit of electrical power equal to one billion watts. In the data center industry, GW is commonly used to quantify large-scale power capacity across hyperscale campuses, regional markets, utility infrastructure and global data center portfolios.

Hot Site
A rapid and comprehensive disaster recovery solution that involves maintaining a fully operational, synchronized duplicate of a primary data center, capable of assuming full production responsibilities within minutes of a critical system failure at the primary site. Hot sites allow for robust, nearly instantaneous failover without significant data loss or operational interruption.

Kilowatt (kW)
A unit of electrical power equal to one thousand watts. It represents the rate of energy consumption or delivery at a specific point in time and is commonly used in data centers to describe IT load, rack density and facility power capacity.

Meet-Me Room
A secure telecommunications space within a data center where carriers, network providers, cloud providers and tenants physically interconnect equipment to exchange data traffic through cross-connects and patch panels.

Megawatt
A unit of electrical power equal to one million watts (1,000 kW). Data center size is commonly measured in megawatts of available IT capacity.

N+1 Redundancy
A resiliency model in which one additional backup component is available beyond the minimum required for normal operations.

Power Distribution Unit
Equipment that distributes electrical power from the facility's electrical infrastructure to racks and IT equipment.

Racking
The process of installing server racks and associated equipment into a data center environment.

Server Rack
A standardized cabinet used to house servers, storage systems and networking equipment.

Single Point of Failure (SPOF)
Any component, system or process whose failure would cause service interruption with no alternative path for operations to continue. Identifying and systematically eliminating SPOFs is fundamental to achieving high availability in data center design and operations.

Tier (I–IV)
The Uptime Institute uses a four-tier system to rate the redundancy and resiliency of data centers. Tier I provides basic redundancy, Tier II adds extra redundant power and cooling subsystems, Tier III requires no shutdowns when equipment needs maintenance, and Tier IV implements several independent, physically isolated capacity components, so that when a piece of equipment fails, IT operations are not affected.

Uninterruptible Power Supply
A battery-backed system that provides immediate power during utility outages until generators (or some alternate power source) assume the load.

Warm Site
Preconfigured backup facilities that include some critical hardware and networking infrastructure. These environments typically require several hours to become fully operational after a primary site failure. Organizations configure warm sites with essential server infrastructure, partial data backups and preliminary network connectivity, allowing for a rapid recovery compared to cold sites while maintaining lower ongoing operational costs compared to hot sites.

White Space
The portion of a data center allocated for IT equipment and supporting infrastructure, including servers, storage, network gear, racks, rack-level power distribution and related cooling components. Commonly used as a planning term for usable production floor capacity.

3 CATEGORY 3 OPERATIONS AND PHYSICAL SECURITY

Access Control System
The technology and processes used to authorize, authenticate, monitor and record access to secured areas and systems.

Alert Fatigue
A condition in data center monitoring, where a high volume of system notifications progressively erodes technical staff's ability to distinguish meaningful signals from noise. As facilities infrastructure scales, complexity increases, and monitoring becomes more sophisticated, personnel can find themselves overwhelmed by continuous streams of alerts that dilute the urgency of genuine performance or security risks.

Asset Management System
A system used to inventory, track, manage and maintain equipment throughout its life cycle.

Building Management System (BMS)
A centralized platform used to monitor and control major facility systems such as mechanical, electrical, environmental, lighting and related building services. In a data center, the BMS helps operations teams maintain visibility into facility conditions and respond to abnormal system behavior.

Capacity Planning
Process of forecasting and provisioning resources to meet future demand.

Crime Prevention Through Environmental Design (CPTED)
A multidisciplinary approach to security that integrates architecture, engineering, landscaping, lighting, technology and operational procedures to reduce vulnerabilities and strengthen protection of critical infrastructure. Within data centers, CPTED principles help create layered defenses that improve visibility, control access, establish clear ownership of space and support resilient operations.

Electrical Power Monitoring System (EPMS)
A system that monitors the electrical distribution network in real time, including parameters such as voltage, current and energy consumption. In data centers, EPMS data supports power reliability, capacity awareness, alarm response and operational troubleshooting.

Emergency Operating Procedures (EOP)
Documented, step-by-step procedures used during an emergency or incident to protect personnel, preserve critical load, mitigate customer impact and stabilize data center operations. EOPs are executed during unplanned events such as power failures, cooling failures, fire alarms, control-system failures, utility disruptions or other conditions that threaten normal operations.

Facility Operations Center or Network Operations Center
The centralized onsite operations hub of a data center or data center campus where personnel continuously monitor critical infrastructure systems, manage alarms and incidents, coordinate operational activities and maintain situational awareness of facility operations. Security monitoring typically is located separately, but these functions can be co-located within the same room if the design of the space allows.

Layered Security
A security strategy that applies multiple protective controls (physical, technological and operational) from the property boundary to the server rack. Implementing layered security shapes the environment to deter, detect, delay and respond to threats.

Lockdown
The point in a data center's development when operational security assumes responsibility for controlling site access from the construction teams.

Mantrap
A controlled-entry vestibule that verifies a person's identity and authorization before granting access to a secure area.

Radio Frequency (RF) Detection
The monitoring, sensing, identification and analysis of RF emissions within and around a data center to detect, locate and assess authorized and unauthorized wireless devices, communications and signals that could present operational, cybersecurity, physical security, compliance or safety risks.

Ready for Network Install
A project milestone indicating that a facility is sufficiently complete to begin installation of networking infrastructure.

Release to Engineering Group
The final handoff milestone in the development life cycle where the facility transitions into operational service.

Remote Hands/Smart Hands
Authorized on-site personnel who perform physical tasks on behalf of remote customers or operators.

Root Cause Analysis (RCA)
Process of identifying the underlying cause of incidents to prevent recurrence. A critical diagnostic methodology for data center professionals seeking to transform reactive problem solving into proactive system resilience. RCA uncovers the fundamental factors driving performance disruptions, equipment failures and systemic vulnerabilities. Effective RCA demands a nuanced, blame-free organizational culture that prioritizes systemic understanding over individual fault finding.

Runbook
Documented procedures for routine operations and incident responses. A well-constructed runbook functions as a critical knowledge transfer mechanism that standardizes responses to both predictable and unexpected scenarios.

Security Operations Center (SOC)
A centralized location where personnel monitor alarms, cameras, access control systems and security incidents.

Service Level Agreement (SLA)
Contract specifying performance commitments, uptime guarantees and penalties for failures. An SLA establishes quantifiable performance metrics that data center operators must consistently meet. Typically, these metrics center on uptime guarantees, with industry-standard availability targets ranging from 99.67% (approximately four hours of potential downtime annually) to 99.995% (less than 26 minutes of potential annual interruption). Agreements typically include explicit penalty structures where service providers must offer monetary credits or compensation if performance targets are not met. Agreements increasingly incorporate detailed provisions around network latency, data transfer speeds, security response times, environmental conditions, power quality and cybersecurity preparedness.

Standard Operating Procedure
Documented procedures that provide step-by-step instructions for performing a recurring operational or security task consistently, safely and in accordance with organizational policies and standards.

4 CATEGORY 4 COOLING AND ENVIRONMENTAL SYSTEMS

Cold Aisle Containment
A rack arrangement and internal barrier strategy that separates server intake air from server exhaust air to improve cooling efficiency. Enclosing cold supply aisles with physical barriers prevents mixing with hot exhaust air. Transparent polycarbonate panels, sliding doors, or rigid barriers create a dedicated "cold air corridor" between the intake side of server racks. These barriers ensure that only precisely temperature-controlled air reaches server intake zones, reducing the thermal load on cooling systems.

Computer Room Air Conditioner
A cooling unit used to regulate temperature and humidity in data center environments.

Computer Room Air Handler
A cooling system that uses chilled water to remove heat from the data hall.

Direct Liquid Cooling
A cooling technology that removes heat directly from servers and AI GPUs using liquid circulated through cold plates or similar devices.

Emergency/Tornado Mode
Allows chilled water Ssystems to continue operation when their cooling towers are isolated from the data center due to a tornado or other emergency in the area. Heat rejection from the cooling systems is diverted from the cooling towers to the emergency water tank when this operating mode is initiated.

Evaporative Cooling
Cooling method using water evaporation to reduce air temperature. Typically employing large air handling units where warm incoming air passes through water-saturated media or gets directly misted. Water transitioning from liquid to gas creates a substantial cooling effect without mechanical refrigeration.

Hot Aisle Containment (HAC)
A strategy of isolating the heated air expelled from server equipment to improve thermodynamic efficiency using modular physical barriers like polycarbonate panels, curtains, or rigid partitions that extend from rack tops to ceiling levels. These barriers create "hot zones" where exhaust air is concentrated, enabling more targeted cooling interventions. Due to the extreme temperatures found inside HACs, work in these areas is often time restricted.

HVAC
Heating, ventilation and air conditioning systems that maintain temperatures and environmental conditions required for IT equipment.

Power Usage Effectiveness
An industry metric that measures the energy efficiency of a data center by comparing total facility power consumption to IT equipment power consumption. The lower the value, the better energy efficiency the facility has (a value of 1.0 being theoretically perfect).

Raised Floor
Elevated floor creating plenum space below for cold air distribution and cable routing. Typically constructed with modular tiles supported by adjustable pedestals, these elevated flooring structures create a dedicated plenum space beneath the walking surface, enabling airflow management and cable distribution. The typical raised floor height ranges from 12 to 24 inches.

Rear Door Heat Exchanger

A rack-mounted cooling system installed on the rear of an IT rack that removes heat from exhaust air using a liquid-based heat exchanger before it is discharged into the data hall.

Water Usage Effectiveness

An industry metric that measures the water efficiency of a data center by comparing total facility water consumption to the IT workload it supports (expressed in liters per kilowatt-hour (L/kWh)).

MORE SIA RESOURCES FOR DATA CENTER SECURITY



Data Center Security Principles

This resource from the SIA Data Center Advisory Board is a reference guide for data center security professionals. This document is intended for the security industry, and particularly for data center security professionals, as a practical reference for strengthening physical security throughout sites and across the critical environments therein.



Securing Data Centers: A Guide to Trends and Strategies for the Physical Security of Data Center Facilities

This paper, produced within the SIA Perimeter Security Subcommittee, examines the challenges shaping physical security for data centers today, with a focus on integration, interoperability and life-cycle management.



Vertical Insights: 2025 Data Center Security Symposium

This virtual symposium examines the physical security and cybersecurity challenges facing today's data centers and the technology solutions and best practices data centers are using to safeguard their facilities and information.



Protecting Data Centers: A SIA Breakfast Event

This event presented by SIA's Data Center Advisory Board and hosted at ISC and ISC East highlights the security challenges facing today's data centers in design and construction.



SECURITY INDUSTRY ASSOCIATION

securityindustry.org

©2026, Security Industry Association
All rights reserved.