DATA CENTER PHYSICAL SECURITY GUIDELINES

Authors

Cliff Jones | *Meta*

Joey Arato | *Meta*

Rich Story | *Roxtec*

Marcelo Campos | *Roxtec*

Stephen Naumann | *General Services Administration (GSA)*

Contributors

Andrea Wells | *Meta*

Parth Shukla | *Google*

Mayank Sinha | *Google*

Andy Archuletta | *Meta*

Brent Kennedy

Revision History

Revision	Version	Date	Comments
1.0	1.0	TBD	First Final

Executive Summary

The purpose of this document is to guide relevant best practices for physical security of data centers and similar physical infrastructure that stores, processes, and transmits sensitive data. The Open Compute Project (OCP) foundation allows the entire industry to create a technical reference for building better data centers as demand continues to grow and is intended to provide value guidance to all partners in this field from small-scale specialty service providers to global hyperscale data center owners. This reference is intended to offer a primer on the intent of physical security and basic guidance and best practices for its application to data center infrastructure, addressing a gap in OCP's security guidance that is focused on securing the physical spaces within which OCP hardware and technology is deployed.

Traditionally, physical security is utilized to protect assets, including people, property, and information. In data centers, there are four key elements that are the focus of physical security controls: (1) data, (2) networks, (3) mechanical equipment, and (4) utilities. Each of these items is critical to the function of a data center and the failure to secure any one of them can result in data breach or failure of operations. Thus, a Physical Asset Protection (PAP) framework is detailed in this document that is intended to provide protection to those four critical elements of a data center.

This paper provides background context on the performance objectives of physical security controls followed by context on applicability, and a summary of physical security design principles. Following this contextual information, the final major section provides a list of recommended considerations when designing and operationalizing a physical security plan for data center infrastructure. This guidance is broken into campus-, building-, and space-level recommendations, along with special component-level high security recommendations to offer guidance that is applicable for anything from a single server, component, or rack, all the way to multi-building campuses common among hyperscalers.

List of Abbreviations

ACP	Access Control Point
ACS	Access Control System
ASIS	American Society for Industrial Security
CCTV	Closed Circuit Television
CoLos	Co-locations
CPTED	Crime Prevention through Environmental Design
CSLA	Civil, Structural, Landscape, Architectural
GPS	Global Positioning System
IDS	Intrusion Detection System
ILA	Inline Amplification
OCP	Open Compute Project
OTS	Operational Technology Security
PAP	Physical Asset Protection
PoLP	Principle of Least Privilege
PoP	Point of Presence
PPS	Physical Protection System
QMS	Quality Management System
SCR	Security Control Center
SLA	Service Level Agreement
SOC	SecurityOperations Center
SOP	Standard Operating Procedure
VSS	Video Surveillance System

Table of Contents

Background 8

1 What is Physical Security? 8

- Physical Security Performance Objectives 9
  - Deterrence 10
  - Detection 10
  - Delay 10
  - Response 11
- Protect-in-Depth 11
- Balanced Protection 12

2 Applicability 13

- Target of Protection 13
- Data Center Project Lifecycle 14
- Data Center Infrastructure 15
- Threat Vectors and Bad Actors 15

3 Physical Security Design Principles 15

- Environment Design and Construction 15
  - Crime Prevention through Environmental Design (CPTED) 16
  - Physical Hardening and Barriers 16
  - Spatial Layout 17
- Security Systems and Technologies 17
  - Access Control Systems (ACS) 17
  - Intrusion Detection Systems (IDS) 18
  - Video Surveillance Systems (VSS) 19
  - System Integration and Reporting 19
- Security Operations 19
  - Monitoring and Response 20
  - Secure Escort 20
  - Randomized Recurring Patrols 20
  - Incident Reporting and Investigations 20

4 Application to Data Center Infrastructure 21

- Facility Security Narrative 21
- General Requirements for All Projects 22
- Campus-Level Physical Security 24
- Building-Level Physical Security Requirements 25
- Space-Level Physical Security Requirements 27

Specialized Component-level High Security Requirements 29

5 Conclusions **30**

6 References **31**

7 License **32**

8 About Open Compute Foundation **33**

List of Figures

Figure 1: Performance Objectives for OCP Physical Security Guidelines 9

Figure 2: Protect-in-Depth Structure of OCP Physical Security Guidelines 12

Figure 3: Holistic Security Venn Diagram 13

Figure 4: Data Center Project Lifecycle 14

List of Tables

Table 1: Access Control Credential Types 18

Table 2: General Requirements for All Projects 22

Table 3: Campus-Level Requirements 24

Table 4: Building-Level Requirements 26

Table 5: Space-Level Requirements 27

Table 6: Specialized Component-Level High Security Requirements 29

Introduction

To date, discussion of security across Open Compute Project (OCP) guidelines and standards has focused on information, hardware, and network security. While these aspects of security are critical to delivering and operating secure data center infrastructure, a gap has existed in guidance for physical security best practices specifically for data centers and their supporting infrastructure (e.g., points of presence, co-locations, etc.) As information security professionals have acknowledged from the advent of the profession, physical access to network gear often enables logical access. Physical security controls must be employed along with logical security controls to offer a comprehensive security solution for data centers. To address the gap in physical security guidance within the OCP documentation and frameworks, this document provides a summary of foundational principles of physical security and general approaches to the development and deployment of physical protection systems (PPS). Finally, the document concludes with recommended best practices for physical security specifically for data center infrastructure considering a range of generalized scales from rack-level to multi-building campus-level applications.

Background

"Security" is a multi-faceted topic spanning information security, network security, hardware security, physical security, and many others. These security approaches are also considered and coordinated with related topics like crisis management, operational continuity, and incident investigations. Focusing specifically on physical security of data center infrastructure, it is often considered as the sum of three major areas of focus: (1) environmental design and construction, (2) security systems and technologies, and (3) security operations. Ideally, these aspects of physical security are built into the planning, design, construction, operation, refresh, and decommissioning phases of all projects. Moreover, the best physical security plans consider and leverage the complementary aspects of logical, and network security controls, minimizing unnecessary overlap to create a coordinated and layered security approach from the property boundary all the way to the data center's protected data, networks, mechanical equipment, and utilities. However, before these diverse approaches to security can be considered together, each approach must be articulated and understood separately. For that reason, this document focuses specifically on physical security and is intended to offer a foundational understanding of the topic as well as a reference for the application of the concepts and principles of physical security to data center infrastructure across a range of scales from rack-level security to multi-building campus applications.

1 What is Physical Security?

In Field Manual 3-19.30, the United States Army defines physical security as *that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, materials, and documents; and to safeguard against espionage, sabotage, damage, and theft.* ASIS International presents a similar definition in their Protection of Assets (PoA) Physical security book. While these definitions do not clarify what approaches are encompassed within the category of physical security, they clarify that physical security measures are typically intended to protect tangible assets like people, property, and documents. However, physical security can offer protection to intangible assets like

information and data, often by detecting bad actors, responding to incidents, and restricting access to the physical assets like hard drives, that store the intangible information assets.

The following sections present a summary of the fundamental performance objectives of physical security systems. An effective physical security strategy has four basic functions. For additional information, these functions can be found at *Physical Security Principles, ASIS, Part 1, Chapter 2.*

- controlling access
- observing an area, situation or event
- detecting events
- responding to situations

These performance objectives, or functions, are the intended goals pursued through the application of physical security measures. While they are discussed individually, many physical security measures will influence, affect, and contribute to more than one performance objective.

Physical Security Performance Objectives

To better understand physical security, the following sections provide a summary of the performance objectives of physical security controls and systems. It should be noted that, depending on the reference reviewed, physical security performance objectives can take a variety of different forms. Most often, they are presented as a list of three to five words that begin with the letter D (for reasons unknown) including some combination of Deter, Detect, Delay, Deny, Defend, Defeat, and Destroy. For the OCP Physical Security Guidelines, the approach taken by ASIS International is adopted, breaking physical security into four primary performance objective categories or "functions"; deterrence, detection, delay, and response. Additional information can be found in the *Physical Security Principles* manual by ASIS International. Each of these performance objectives is briefly summarized in Figure 1.1 described in additional detail in the following sections.

Deter	**Function** **Objective** **Examples**	**Secondary** **Create perception system is difficult to detect** **Physical presence, lighting, signage, CPTED, etc.**
Detect	**Function** **Objective** **Examples**	**Primary** **Detect & identify undesired people and activities** **Sensors, video, alarms, lighting, patrols, etc.**
Delay	**Function** **Objective** **Examples**	**Primary** **Increase time and effort to reach target** **Site & building infrastructure, procedures, etc.**
Respond	**Function** **Objective** **Examples**	**Primary** **Timely and accurate dispatch of personnel** **Guard forces, alarms, communications, etc.**

Figure 1: Performance Objectives for OCP Physical Security Guidelines

Deterrence

Unlike detection, delay, and response, which are primary functions of a physical protection system (PPS), deterrence is a secondary function. The reason it is separately classed is that there is no way to objectively quantify and measure the level of deterrence provided. Instead, deterrence is a qualitative aspect of security that is manifested through the thoughtful application of physical security measures and general design and use of spaces to reduce the opportunity for malicious actors to exploit vulnerabilities in the physical or logical controls. Because of the ambiguous nature of deterrence and the inability to quantify its effectiveness, it is discussed only for context in this document and illustrated by discussing the most commonly used approach to deterrence, Crime Prevention through Environmental Design (CPTED), discussed in Section 3.

Detection

The first of the three primary functions of a PPS is detection. Detection is most often the measure of the ability of a PPS to detect unauthorized access or attempts at unauthorized access. The ideal objective is to detect unauthorized access as early as possible to initiate an appropriate security response (discussed later) and maximize the time allowed for that security response to be carried out.

Detection may be achieved by a variety of means including physical intrusion detection systems (IDS), access control systems (ACS), and video surveillance systems (VSS). These systems are influenced and supported by thoughtful design, construction, and maintenance of the physical environment and other aspects of the physical design of spaces such as lighting, physical circulation controls (i.e., people movement controls), and physical barriers (see Section 3 below). Alerting associated with the detection function may be either covert (i.e., unknown to the bad actor) in the case of silent alarms or overt (i.e. known to the bad actor) in the case of audible and visible alerting functions.

There are trade-offs to each of these approaches. In particular, covert alerting often allows the response function to gain the *element of surprise*;. Alternatively, an overt detection may act as a deterrent stopping the bad actor in their tracks and forcing them to abandon their mission. These approaches to detection are discussed in additional detail later in this document.

Delay

Like detection, delay is another primary function of a PPS and one that, similarly, is focused on offering additional time for security response. Moreover, where sufficient delay is presented to a bad actor by the PPS, they may be entirely dissuaded from their mission and abandon it eliminating the need for a response. One critical thing to remember when considering the effectiveness of delay tactics is that their value is severely limited, or even negated if the bad actor is not detected. For example, while a fence at the boundary of a property may delay a bad actor, in principle, without detection of the bad actor bypassing this delay barrier, it offers no increased time for security response and no real value where a dedicated bad actor is determined to bypass it. Thus, in this scenario, the fence is merely performing the function of a deterrent and nothing more.

Delay can be achieved by a variety of means including permanent passive physical barriers like walls, fences, and safes; active physical barriers like motorized gates, drop-arms, and hydraulic bollards; and even dispensable barriers like deployable foams, gasses, and liquids. However, dispensable barriers are rarely used for delay except in specialized applications and would typically not be recommended in a data center application. Additional detail on delay tactics is provided later in this document.

Response

The third and final primary function of a PPS is response. Response generally refers to the function carried out by the operational security team—often called security guards or response force—in physically reacting to and responding to a security event. However, response could take other forms, particularly in "logical" space where network equipment can be segregated and protected data can be quickly wiped to eliminate threat of physical access. Additionally, while not discussed in detail in this document, physical response also relies on alerting and communication systems to coordinate the dispatch and ongoing communications with responding officers.

The time available for response is dependent on detection, which initiates the response, and delay, which can facilitate additional time for response (but only after detection). Response is the most flexible and adaptable means of altering and adjusting a PPS and its performance once a facility is constructed and operational. For example, policies and procedures can be updated to tune the PPS to the appropriate threat level present and guard force can be rapidly deployed to act as a compensatory measure when detection or delay systems are temporarily non-operational or insufficient. In addition, the response function is often considered the most critical function of a PPS because it is the one that typically intercepts, interrupts, and/or directly engages and neutralizes a bad actor. Thus, detection and delay measures must be present and functional to ensure the response team can initiate response and maximize time to respond. Finally, response does not always have to be immediately initiated, sometimes logging and follow-up are all that is required for certain protected assets. Additional information on the response function and operational security is presented later in this document.

Protect-in-Depth

Protect-in-depth refers to the strategy of layering security measures, controls, and systems such that an adversary is required to bypass (i.e., avoid or defeat) multiple protective measures in series before arriving at a protected asset. The more critical or valuable the asset, the more complex and numerous the controls. Protect-in-depth is most effective when the deployed physical security controls are chosen to be complementary and diverse rather than similar and redundant. Said differently, physical security controls should be selected such that different and diverse tactic(s) must be used to bypass the multiple layers of protection. Thus, in the most effective protect-in-depth schemes, each layer requires an adversary to perform a separate and distinct action to bypass it.

The result of multi-layered protect-in-depth security measures is a security "system". A well-designed protect-in-depth physical security system (or physical protection system; PPS) presents increased uncertainty and requires more extensive preparation, necessitating multiple challenging steps to defeat it. For this document, recommended physical security measures are defined at the campus, building, space, and rack level. By incorporating and combining these recommended controls, one can assure a protect-in-depth PPS as illustrated in Figure 1.2. In extreme cases, the protect-in-depth approach can even

be quantitative, considering detection likelihood, delay times for various barriers, response times, and attack vector times to optimize the various layers of security.

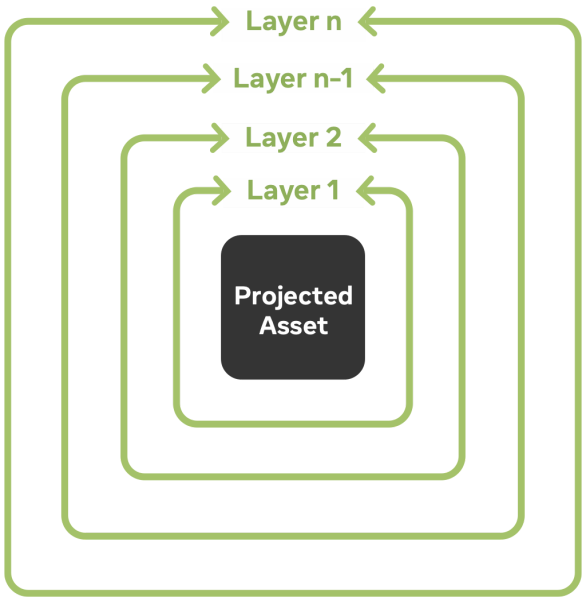

Figure 2: Protect-in-Depth Structure of OCP Physical Security Guidelines

Balanced Protection

Balanced protection is at the root of a holistically designed security system. To achieve balance in a PPS, physical security controls should be selected such that they offer complimentary performance requiring a bad actor to encounter controls that will deter, detect, or delay them and initiate an appropriate security response.

Within the physical security domain, protection should be thoughtfully balanced also among the electronic, structural, and human aspects in a complimentary fashion, leveraging the most effective and efficient means of protection and incorporating diversity to improve the overall protect-in-depth strategy.

Taking this concept further, a truly holistic and balanced protection system goes beyond considering only the physical security controls and, instead, also includes a diverse range of network and logical controls, deploying them in a complementary and efficient manner. While this holistic approach to security is beyond the scope of this document, consideration of the diverse range of physical, logical, and network security controls available to protect a data center can produce an extremely efficient and effective security system where synergies and efficiencies can be leveraged to offer very complete and balanced security system where duplicative and unnecessarily redundant aspects are minimized. Thus, truly optimal security systems live within each of these three primary security approaches as illustrated in Figure 1.3.

Figure 3: Holistic Security Systems

The holistic approach to security stated in this section, and under the Open Compute Project Foundation (OCP) conceptual framework, requires that we understand the connections between Physical Security, Network Security, and LogicalSecurity. For more information on these other OCP security domains refer to the groups below.

Current OCP Project Groups where security is a consideration:

- Data Center Facilities
    - Operational Technology Security (OTS) - The OCP DCF Security project is the sponsor of this document and focuses on the unique security considerations facing data centers and the critical infrastructure systems they are reliant on.
- Security - The Security Project creates designs and specifications to enable software security for all IT gear through collaboration with the wider Open Compute community. This project provides a foundation for securing all IT gear that is designed in other Open Compute projects.
- Telcos - The OCP Telco Project enlists participants from telecom companies and carriers as well as subsystems, software, board and semiconductor suppliers who are seeking to use data center infrastructure to deliver IT services.

2 Applicability

While physical security is a broad and diverse topic, these OCP Physical Security Guidelines are intended to provide foundational information on physical security, its performance objectives and general approaches, and application of these approaches to operational data centers and supporting infrastructure as described in the following sections.

Target of Protection

The intent of security is to provide disproportionate protection to what matters most. For typical data centers, the two most important things are data (and the associated processing, transmission, and storage media), and continuity of operations. Regarding continuity of operations, there are three categorical items that disproportionately affect data center performance: networks and associated infrastructure (both the data processing networks and those used to operate the building), mechanical equipment used in the conditioning, cooling, and powering of the spaces and services, and critical utilities like power and water. Without any one of these items, the data center would not function properly or possibly at all. As a result,

the target of the protective measures of the PPS should be (1) data, (2) networks, (3) electrical and mechanical equipment, and (4) critical utilities.

Take note that the intended target of protection is not *all* data, networks, mechanical equipment, and critical utilities. Rather, each of these items should be reviewed to determine whether and how they should be protected by focusing on whether sensitive data is stored, processed, or transmitted (typically relevant to data and networks) and/or whether it supports critical functions of the data center (typically relevant to networks, mechanical equipment and utilities).

Data Center Project Lifecycle

Data centers and their supporting infrastructures like co-locations (CoLos) and points of presence (PoPs) follow a generalized project lifecycle much like other constructed infrastructure. That lifecycle can be simplified into four discrete phases—(1) plan, (2) build (i.e., design and construction), (3) operate, and (4) refresh or decommission—as illustrated in Figure 2.1.

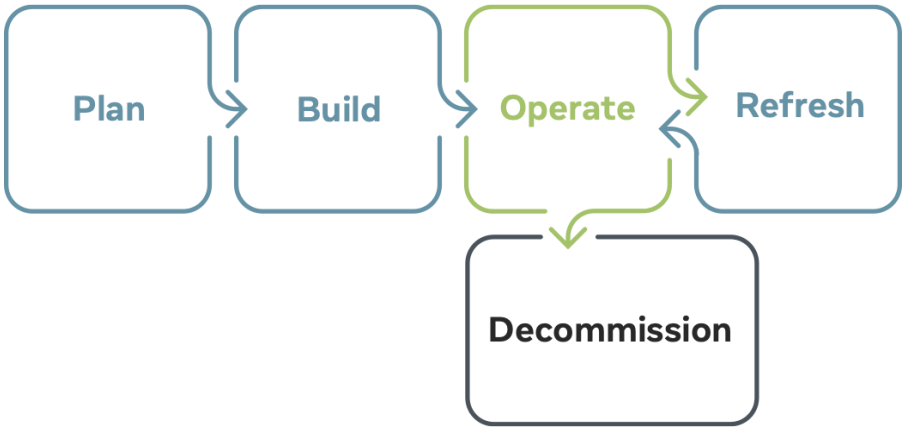

Figure 4: Data Center Project Lifecycle

Planning refers to the early stages of a project when overall performance objectives are defined, generalized strategies are established and agreed to, risk assessment is conducted, and expectations are set. Next, the build phase encompasses design and construction concluding with turnover. Operation is next and is often the longest phase of the data center infrastructure lifecycle, referring to the time in which traffic is served and spaces are functional. Finally, refresh and decommissioning either restart the lifecycle (refresh) or conclude it (decommission).

The scope of the OCP Physical Security Guidelines presented herein is intended to apply ***only*** to the operational phase of this lifecycle. Planning, build (design and construction), and retrofit and decommission are out of scope for this document. While no OCP physical security guidance exists for these remaining three phases, additional guidance in these areas will be provided in the future and their omission here does not indicate that these phases do not require physical security work. Rather, work should be done in the plan, build, refresh, and decommission to ensure that the recommendations presented in this document are appropriately captured throughout the operation phase.

Data Center Infrastructure

To provide generalized and broadly applicable guidance, the detailed guidelines presented in Section 4 are summarized for component-level, space-level, building-level, and campus-level security projects. This structure was selected by the authors to offer guidance that can be applied to many different micro- to macro-level data center infrastructure projects. Also, as discussed in Section 4, these rack, space, building, and campus-level guidelines can be applied together to present a protect-in-depth approach to physical security to larger infrastructure projects. However, where smaller projects are deployed, a more selective approach can be taking the application of these guidelines all the way down to a single rack deployment.

Threat Vectors and Bad Actors

While threat vectors and bad actors may implicitly or explicitly be mentioned in this document, detailed discussion of these topics is beyond the scope of this document. As such, the content of this document is intended to offer general best practices for physical security and not a precise approach to defeating a specific threat or bad actor.

3 Physical Security Design Principles

The following sections describe physical security design principles in three different contexts: (1) environment design and construction, (2) systems and technology, and (3) security operations. These security design principles should be applied in a balanced, thoughtful, and intentional manner to achieve the security objectives of deterrence, detection, delay, and response that are appropriate for a given facility.

Environment design and construction focuses on the built environment and the incorporation of physical security into civil, structural, landscape, architectural (CSLA), electrical, and mechanical partner scopes. Systems and technology refer to access control, intrusion detection, and video surveillance systems and their components.

Finally, security operations refer to the people that provide physical security (e.g. guard force, security, the guards, etc.); their operational policies, procedures, and practices; and the means by which they communicate. Each of these topics is discussed in detail below along with non-exhaustive relevant examples.

Environment Design and Construction

In this context, “environment” refers to the design of the physical space and the utility infrastructure that supports it. This can include everything from the overall site master planning, circulation and wayfinding, lighting, site and building hardening, interior spatial layout, and physical barriers.
Reframed, this is the security scope that generally impacts cross-functional design partners in Civil, Landscape, Structural, Architectural (CSLA), Electrical, and Mechanical disciplines. The following sections briefly describe some relevant typical strategies and considerations for the incorporation of physical security in the environmental design and construction process.

Crime Prevention through Environmental Design (CPTED)

The phrase crime prevention through environmental design (CPTED) was first introduced by C. Ray Jeffery in 1971. In principle, CPTED is a design concept intended to reduce the opportunity or fear of criminal activity through thoughtful design of a space or environment. This is achieved by designing and defining spaces in a way that encourages proper use and stewardship while discouraging abuse, misuse, and other undesirable behaviors. Thus, CPTED serves a deterrent (secondary) function in a PPS and does not explicitly influence the delay, detection, or response to a bad actor. By leveraging principles of natural access control, natural surveillance, territorial reinforcement, maintenance, and legitimate activity support to deter bad actors, CPTED can be designed into spaces and environments. While incorporation of CPTED principles is considered a good practice for a given project or design, explicit details and requirements for incorporation are beyond the scope of this document. All Example Controls are applied based upon the risk to the site:

- Disruptive landscaping and physical barriers to deter access by people or vehicles
- Separate roads/lanes for different personnel (e.g., delivery vehicles vs. support staff)
- Clear visibility across the site/area to encourage natural surveillance
- Site lighting that illuminates protected assets and potential areas of concealment

Consideration should be given to enhancement of critical locations or spaces in reducing overall visibility to bad actors as possible means to reduce targets of opportunity. Examples could include signage and or identification that might attract, focus and or simplify an individual/organization towards critical locations/spaces.

Physical Hardening and Barriers

Physical hardening can be incorporated into a project by providing barriers and incorporating special threat-resistant construction into spaces. Physical hardening is intended to delay and deny access to a facility, asset, or operation. Use of physical barriers can also offer opportunities to channel movement of people and assets through specific areas to improve likelihood of detection. The principles of protection in depth can be applied to site hardening and implemented to achieve the overall security system objectives.

A delay in depth approach considers the strength of each obstacle in relation to the resources available to an adversary to overcome them. Time afforded by obstacle delays counts toward the overall time for a response to breach, although delay times are beyond the scope of this document. While barriers create a delay for intrusion those barriers must be combined with detection and response mechanisms. Without the ability to detect and respond these barriers provided limited to no risk mitigation.

Note that barriers can come in many forms including fences, walls, doors, and cages and applied at a site, building, space, or even rack level, and can support detection while delaying a bad actor and allowing additional time for response. Based on the risk profile and identified threats,specialized barriers can be incorporated to resist vehicle impact, ballistic-resistant to protect against armed aggressors, forced entry resistant to protect against brute force and hand tools, etc.

Spatial Layout

Spatial layout is instrumental in implementing a protect-in-depth approach and can begin as early as the property boundary. Spatial layout combined with physical barriers provides a means of controlling access to and defining (CPTED) the protected site, spaces, and/or assets.
Spatial layout should be considered in site master planning in campus settings, at the building floor plan level in individual buildings, and within sub-spaces, as appropriate. High-value/risk space should generally be placed at or near the center of secure spaces, furthest from public or easily accessible space (for ease of protection and response), and ideally with the maximum total number of barriers and security controls protecting it. Spatial layout is instrumental in thoughtfully controlling the movement of people and segregating access between different spaces.

In addition, when considering spatial layout, it's typically recommended to consolidate spaces with similar use cases. This approach can greatly reduce the complexity of controlling and restricting access by providing secure zones–groups of similar spaces–instead of securing spaces individually. It also offers opportunities for operational efficiencies in the general use of the spaces by operational teams and also in alarm response.

Security Systems and Technologies

Security systems technology include access control systems (ACS), intrusion detection systems (IDS), and video surveillance systems (VSS). These systems work together to detect unauthorized access and inform security's responding personnel and, through logging, offer a historic record of access, detected intrusion, and video. The following sections provide a brief summary of the intended purpose of these systems.

Access Control Systems (ACS)

Access control systems are intended to provision access to authorized personnel and detect unauthorized access to critical spaces. Access controls are often identified based on the number of identified "factors" or credentials they review and authenticate. Credentials come in three general forms as described on the following page.

Table 1: Access Control Credential Types

Credential Type	Examples
Something you **have**	• Photo ID / Credential • Barcode / QR code • Physical Key • Magnetic Stripe Card • Proximity Card (NFC, RFID, etc.) • Token
Something you **know**	• Username / passphrase • Personal Identification Number (PIN)
Something you **are**	• Fingerprint • Palm print • Retinal / Eyeris scan • Facial geometry • Voice

These credential types can be combined for improved security. When combined into a multi-factor access control, they are often discussed as one, two, and three-factor authentication. Combining is most effective when different credential types (something you have, know, and are) are combined without duplication of the type. For example, two factor is typically deployed in a format of something you have and something you know or are like:

- Something you have + know: Proximity Card and PIN
- Something you have + are: Token and Fingerprint

Duplication of credential types should be avoided in two- and three-factor access controls as the ability to obtain or spoof the means of authentication is essentially the same within a given credential type. Access controls can be applied in many ways to control access to a campus, building, space, and rack and can be applied considering the movement of vehicles, people, assets and even (beyond the scope of the physical security) information.

Intrusion Detection Systems (IDS)

Physical intrusion detection systems (IDS) are a detection mechanism intended to identify and alert security personnel of unauthorized access by people or vehicles to physical spaces, or the presence of unauthorized materials in a space. They typically trigger an alarm to initiate an appropriate security response. When applied to people, IDS is often used to detect intrusion through barriers or into spaces where people are vehicles are not supposed to be present.

In this application, intrusion sensors may be used to monitor otherwise uncontrolled openings (e.g., roof hatches), or alert for unauthorized access through controlled openings (e.g., access controlled doors). In addition, where certain people or materials are not supposed to be present in a space, IDS can be used to alert of their presence. In this application, intrusion sensors

Video Surveillance Systems (VSS)

Video surveillance is a monitoring and assessment tool that can assist in the management of the physical security of the asset, as well as provide documentation of the events. It can serve a wide variety of purposes including:

- Remote incident assessment (response support);
- Event recording and storage;
- Post-event analysis and investigations;
- Live video surveillance (monitoring);
- Video analytics (alarm activation, tailgating identification, etc.)
- Psychological deterrence.

VSS may be simple closed-circuit systems like CCTV where cameras are networked to a local network video recording (NVR) device, or much more complex like fully networked and remotely viewable like many more modern enterprise systems.

System Integration and Reporting

While a detailed discussion is beyond the scope of this document, it is important to note that integration of the ACS, IDS, and VSS is critical to maximizing its performance. These systems work together as a system of systems to control and monitor the movement of people and initiate an alarm when unauthorized access, intrusion, or other undesirable events and behaviors are identified. Thus, they must be integrated to allow for clear display of alarms and data produced by these systems in real time to inform the security operations team and initiate appropriate alarm response processes. Such integration provides a better situational awareness to the security operations staff and helps to differentiate between accurate response to an untoward situation or a simple false or nuisance alarm.

Security Operations

The primary roles of the security operations function are to monitor and respond to alarms, provide secure escort services to personnel on site, perform routine patrols, and reporting and investigation of security incidents. When doing this effectively, on-site security operations personnel should enable efficient site operations while maintaining an appropriate security posture. The sections below describe each of these core functions in more detail. Note that, while not explicitly discussed in this document, operational teams should also ensure there are appropriate processes in place to manage, vet, review, and approve access; manage and maintain the various security systems and technologies; Some examples that address specific operational requirements include vehicle and package scanning/inspection, bomb sniffing dogs, background checks, specific timeframes for length of access and types of approval (outage vs normal) and GPS temporary access ID cards to monitor movement through approved zones.

Monitoring and Response

Monitoring refers to the concept of monitoring alarms, data from security systems and technology, and general activity in secure spaces. Response refers to the active response to monitored security information including response to alarms from technology, observed security breaches, or other security-related incidents. This function is the primary means by which the *response* objective of a PPS is achieved. Response time should be defined considering where detection is likely to occur, delay tactics in place (e.g., barriers, additional layers of access controls, etc.), and expected timeframe within which a security response should occur. From simple understanding of the physical location of targets of protection, location of responding personnel (or whether response will be carried out remotely or logically, which is outside the scope of this document), and a standard design basis for number of simultaneous alarms requiring response, a response model (e.g., staffing and posts) can be defined to meet overall security performance expectations.

Secure Escort

Secure escorting refers to the process of guiding and observing personnel that are present on site but may not be trusted with unrestricted and/or unmonitored access to the facility (referred to herein as "non-trusted personnel"). In spite of the name, secure escort services are not always provided by security personnel. Instead, where non-trusted personnel (e.g., technicians, vendors, visitors, etc.) are required on site, escorts should be provided to accompany them, particularly in spaces that house critical data or equipment. Personnel selected for escort should have a strong understanding of security practices on site and the appropriate level of subject-matter expertise to identify whether the activities of any non-trusted personnel are reasonable and appropriate, and identify and report inappropriate behaviors.

Randomized Recurring Patrols

Randomized recurring patrols refer to the recommended approach to routine observation of key areas of a secure facility. While not typical, they can conceivably be performed remotely utilizing networked video cameras or similar technology; however, this is typically challenging except for very small spaces due to the disproportionate cost of the VSS (or other remote sensing system(s)) that would be required to achieve the necessary level of remote visibility. Some of the video management platforms have features such as video patrols, which when configured flips cameras sequentially after a predetermined interval. More typically, patrols are performed by on-site security operations personnel (i.e., guards).

These patrols are routine in their coverage of all spaces and areas where critical data or equipment exist (see section 4 for additional information). However, where possible they should be randomized (e.g., varying paths, non-standard schedules, etc.) to avoid them being easy to predict and, thus, defeat. During routine patrols, patrolling personnel should identify and report atypical, unsafe, and unsecure conditions such as damaged equipment, propped doors, suspicious behaviors, etc. to initiate response and/or investigations, as appropriate.

Incident Reporting and Investigations

Investigations functions should be independent, impartial, and generally confidential. Also focuses on gathering information related to potential threats and risks to an organization which could include its

people, assets, and/or reputation. The investigative function focuses on gathering evidence, documenting relevant information, identifying relevant root cause(s) and reporting information for security incidents. Investigations are critical to security in that they provide a historic record of past incidents for posterity, compliance, etc. and that they allow for identification of lessons learned and continuous improvement of the overall security function (e.g. through a certification as defined on the following page).

- Investigations teams can consider an ISO 9001 certification, which specifies requirements for a Quality Management System (QMS). QMS aims to increase an organization's awareness of its duties and commitment in fulfilling the needs and expectations of its customers and interested parties and aims to achieve satisfaction with its products and services. The ISO 9001: 2015 QMS has seven different quality management principles: customer focus, leadership, engagement, process approach, improvement, evidence based, and relationship management.

The Investigations team is responsible for consistent adherence to fair and reasonable protocols that accomplish the task of finding and assessing relevant facts while maintaining the privacy of all concerned to the greatest extent possible. It is typically the Investigations team's responsibility to:

- Engage third parties, with advance approval from Legal partners, including without limitation, forensics experts, psychologists or private investigative firms to assist in conducting investigations.
- Interview witnesses and subjects in a respectful, impartial, professional manner to gather and comprehend relevant facts and make determinations regarding the credibility of information obtained.
- Process, investigate, and share information in a manner that is consistent, responsible, and compliant with applicable laws, Terms of Service, and its policies, including the Code of Conduct, Investigations Policy, the Security Investigations & Data Sharing Guide and the Data Policy.
- Process data in accordance with privacy and security policies.
- Research and monitor global events, and conduct analysis and risk forecasting.
- Provide organizational support on Data Management, Business Operations, and Training and Development.

Depending on the scale of protected infrastructure and the criticality of the assets, the investigation function may be served by a dedicated and trained team, integrated into the operational security function, or possibly not formally established at all.

4 Application to Data Center Infrastructure

The following sections summarize the recommended minimum physical security measures that should be employed for a range of data center infrastructure types. Refer to prior sections for additional information on physical security performance objectives and design principles.

Facility Security Narrative

Application of these requirements should consider the relative value of and risk to the protected asset(s) and the unique conditions that exist at the facility and surrounding site. Proof of application of relevant

requirements and overall compliance with these guidelines should be demonstrated by providing a *Facility Security Narrative*.

At a minimum, the *Facility Security Narrative* should include a list of all general, campus-level, building-level, space-level, and specialized high-security requirements that are applicable to the project and a description of how they are incorporated in the design, construction, and/or operations of the facility.

General Requirements for All Projects

The table below summarizes some general requirements across environment design and construction, systems and technology, and security operations. These foundational requirements should be incorporated into all projects regardless of scale.

Table 2: General Requirements for All Projects

Design Principle	Recommendation
Environment Design and Construction	
CPTED	☐ None
Hardening & Barriers	☐ None
Spatial Layout	☐ Security should be considered in master planning of the site and all buildings to ensure high-risk and high-value assets are appropriately protected and security operations can be executed efficiently. ☐ Where reasonable, site and building layouts should attempt to consolidate spaces based on use to maximize the ability to segregate access and security controls based on use case.
Systems and Technology	
Access Control	☐ Access to all critical infrastructure and equipment should be controlled including review/approval of access, logging of access data, and periodic audit of access records. ☐ To the extent reasonable, access should be controlled based on the principle of least privilege (PoLP) where access is ideally limited to only those with an explicit need for it. ☐ Identity Management systems should be used to provision, update and decommission permissions as roles change. ☐ Access reports should be generated and reviewed by all stakeholders with a set cadence based upon the risk the equipment provides. ☐ Where security barriers or layers of protection are provided an appropriate level of access control should be provided to control and monitor access.

Intrusion Detection	☐ Intrusion detection shall be in place to monitor unauthorized access to all critical infrastructure and equipment. **NOTE:** The Access Control system may also serve as intrusion detection where appropriately configured.
Video Surveillance	☐ Video surveillance should be designed to allow for day and night visibility including supplemental lighting, where required. ☐ Video surveillance data should be stored and easily accessible to investigative parties for a duration that best supports the needs of the environment and relevant regulations.
Integration and Reporting	☐ Data and alarms from all access control, intrusion detection, and video surveillance systems should be integrated and monitored as appropriate to meet security operational response expectations. ☐ Data and alarms from all access control, intrusion detection, and video surveillance systems should be logged and archived to support investigations and compliance requirements, as well as local laws and regulations.
Security Operations	
Monitoring and Response	☐ Monitoring and response functions should be established in accordance with the criticality of protected infrastructure, equipment, and data including consideration of necessary response times to inform how this function is achieved (e.g., on-site continuous monitoring and alarm response vs. off-site periodic review and investigation of alarms). ☐ Monitoring and response functions shall be informed by standard operating procedures (SOPs), escalation processes, and defined roles and responsibilities.
Secure Escort	☐ There shall be standard methods for recording, verifying, and documenting escorted personnel and identifying their responsible escorts. ☐ All personnel acting as an escort shall be appropriately trained in responsibilities, expectations, and incident reporting. ☐ When possible, escorts should be selected based on their understanding of the work of the escorted person to ensure inappropriate behaviors can be identified and reported. ☐ Where access to critical spaces or equipment is required by unvetted third parties, they should be escorted by personnel with sufficient training to identify and report inappropriate behaviors.

Patrols	☐ Where required to achieve security objectives, patrols should be performed by dedicated resources with standard procedures for conducting physical patrols that are performed on a regular basis. ☐ Where required, patrols should be performed on a varied (ideally, randomized) schedule and using varied (ideally, randomized) paths of travel.
Incident Reporting and Investigations	☐ Establish clear agreements around incident reporting and escalation with local law enforcement and local business security representatives. ☐ Investigation and reporting shall be in accordance with a standardized approach that defines how incidents are documented and reported. ☐ Security personnel performing these services shall be trained in incident reporting and investigation operations.

Campus-Level Physical Security

The table on the following page summarizes requirements for campus-level physical security across environment design and construction, systems and technology, and security operations.
These requirements should be incorporated into all multi-building campus projects. Note that multiple data centers are not required to trigger these requirements; rather, the requirements apply where one or more data center buildings is located on the same site or campus as other data center buildings, or support buildings like warehouses, water treatment plants, etc.

Table 3: Campus-Level Requirements

Design Principle	Recommendation
Environment Design and Construction	
CPTED	☐ Delineate boundaries between secure and publicly accessible spaces. ☐ Site master plan shall incorporate CPTED principles like natural visibility, natural access control, and territorial reinforcement. ☐ Secure access control points (ACPs) should be designed such that pedestrian and vehicle traffic is naturally funneled to them for access to the site.
Hardening & Barriers	☐ Provide a physical barrier to restrict pedestrian and vehicle access to either the entire site, or all identified critical infrastructure and equipment on the site.
Spatial Layout	☐ Critical infrastructure and equipment on the site should not be located in publicly accessible areas. ☐ Site access shall consider traffic and tenant types and separate their entry and circulation paths, where appropriate.

Systems and Technology	
Access Control	☐ Where a site-level barrier is used, provide secure access control points to monitor and control pedestrian and vehicle access onto the site. ☐ Where barriers are provided around identified critical site infrastructure and equipment, access through them should be monitored and controlled.
Intrusion Detection	☐ Where critical infrastructure and equipment exist on site access to it should include reasonable means to detect intrusion (i.e., unauthorized access).
Video Surveillance	☐ Video surveillance should be provided to monitor and log access to critical infrastructure and equipment on the site and to other secure areas of the site. ☐ For areas with mission critical assets, design should consider whether additional video surveillance is needed to monitor situational activity or inform response to these areas.
Integration and Reporting	☐ Plans for integration and reporting should consider potential efficiencies related to remote review of alarms.
Security Operations	
Monitoring and Response	☐ Where on-site response is required (e.g. guard force), performance expectations shall consider building citing when determining appropriate staffing levels and service level agreements (SLAs) for response.
Secure Escort	☐ There shall be documented standards and procedures outlining requirements for secure escort of personnel on the site.
Patrols	☐ None
Incident Reporting and Investigations	☐ None

Building-Level Physical Security Requirements

The table below summarizes requirements for building-level physical security across environment design and construction, systems and technology, and security operations. These requirements should be incorporated into all building projects including both the data center spaces and support spaces.

Table 4: Building-Level Requirements

Design Principle	Recommendation
Environment Design and Construction	
CPTED	☐ Building design shall incorporate CPTED principles like natural visibility, natural access control, and territorial reinforcement. ☐ Clear delineation shall be provided between secure and unsecure spaces. ☐ Secure access control points (ACPs) should be designed such that pedestrian and vehicle traffic is naturally funneled to them for access to the building.
Hardening & Barriers	☐ Physical barriers (e.g., walls) shall be provided between public (unsecure) and secure spaces. ☐ Building exterior and all successive layers of protection should be of robust construction that appropriately restricts forced entry based on use case, risk, and expected threats.
Spatial Layout	☐ Building access shall consider traffic and tenant types and separate their entry and circulation paths, where appropriate. ☐ The building exterior should be designed to act as a continuous layer of protection; where appropriate, additional layers should be deployed to protect critical areas and/or assets.
Systems and Technology	
Access Control	☐ Access through the building exterior (security layer), and any successive security layers should be controlled consistently to eliminate “soft spots” or opportunities to bypass security controls.
Intrusion Detection	☐ Intrusion detection systems and/or sensors should be deployed to detect unauthorized access by expected means of unauthorized entry through all defined security layers.
Video Surveillance	☐ Video surveillance should be provided to monitor and log access to critical infrastructure and equipment within the building and to other secure areas of the building. ☐ Where necessary, video surveillance can be deployed to serve as a means of verification of access and a historic record for investigations.

Integration and Reporting	☐ Plans for integration and reporting should consider potential efficiencies related to remote review of alarms.
Security Operations	
Monitoring and Response	☐ Plans for monitoring and response shall consider potential efficiencies related to consolidation of monitoring activities to a dedicated and purpose-built space (e.g., security operations center / SOC, security control room / SCR, etc.)
Secure Escort	☐ None
Patrols	☐ None
Incident Reporting and Investigations	☐ None

Space-Level Physical Security Requirements

The table on the following page summarizes requirements for space-level physical security across environment design and construction, systems and technology, and security operations. These requirements should be incorporated into individual data center spaces (e.g., leased data hall) or stand alone data center infrastructure like points of presence (PoPs) or inline amplification huts (ILAs).

Table 5: Space-Level Requirements

Design Principle	Recommendation
Environment Design and Construction	
CPTED	☐ None
Hardening & Barriers	☐ Space exterior should be of robust construction that appropriately restricts forced entry based on use case, risk, and expected threats.
Spatial Layout	☐ Space exterior should be designed to act as a continuous layer of protection. ☐ High security spaces should typically be located away from exterior walls and behind multiple layers of successive protection.
Systems and Technology	
Access Control	☐ Where space-level access control is insufficient to establish a reasonable principle of least privilege for access, asset-level access controls shall be considered.

Intrusion Detection	☐ Where space-level access control is insufficient to establish reasonable protections on critical assets, asset-level detection shall be considered.
Video Surveillance	☐ Video Surveillance should be provided to monitor and log access to all spaces containing critical equipment, networks, assets, personnel, and data.
Integration and Reporting	☐ None
Security Operations	
Monitoring and Response	☐ None
Secure Escort	☐ None
Patrols	☐ None
Incident Reporting and Investigations	☐ None

Specialized Component-level High Security Requirements

The table below summarizes requirements for specialized component-level high security across environment design and construction, systems and technology, and security operations. These requirements should be incorporated to protect specific high value assets (e.g. racks), electrical / communication pathways (telecom vaults, etc) and or areas where the most critical assets are located to provide elevated protection beyond what is offered by site, building, and space-level recommendations summarized previously.

Table 6: Specialized Component-Level High Security Requirements

Design Principle	Recommendation
Environment Design and Construction	
CPTED	☐ None
Hardening & Barriers	☐ Where space-level controls do not enforce principle of least privilege (PoLP) for access, physical barriers shall be provided to restrict access, as appropriate.
Spatial Layout	☐ Equipment should be secured within a space located behind multiple layers of diverse physical controls.
Systems and Technology	
Access Control	☐ Where space-level access control is insufficient to establish a reasonable principle of least privilege for access, consider asset-level access controls. ☐ Access controls should leverage multi-factor (two- or three-factor) authentication to offer increased security for high value assets and spaces.
Intrusion Detection	☐ Sensors shall be deployed to detect unauthorized access and initiate response.
Video Surveillance	☐ Video Surveillance should be established with a clear field of view of all high security components, assets, and equipment sufficient to inform assessment, response, and investigations.
Integration and Reporting	☐ Integration of sensors and technology deployed to protect high security assets should be considered to maximize effectiveness.
Security Operations	
Monitoring and Response	☐ Alarm events related to high security components should be prioritized over other alarms at the site. ☐ Alarm response to mission critical components, assets, and equipment should

	be as near to real time as feasible.
Secure Escort	☐ Third parties and visitors not approved for unfettered access to these areas shall be escorted by trained, equipped and authorized escorts only.
Patrols	☐ On-site patrols should include periodic visual assessment of all high security assets by trained and approved personnel, and include inspections for damage and tampering.
Incident Reporting and Investigations	☐ Investigations of high security assets should follow a defined procedure set that includes requirements for the establishment of a chain of custody of evidence.

5 Conclusions

This whitepaper is focused on providing guidance on how to secure a data center and its various components based upon perceived risk, value, vulnerability, and/or perceived importance. Specific technical solutions (e.g., cameras, card readers, etc.), policies (e.g., escort and visitor policies), operating procedures (e.g., alarm response and investigation guidance), or other similar execution-focused guidance should be defined and documented on a project-by-project basis in a physical security narrative. Where these solutions are defined, they should be mapped back to the guidance and recommendations offered in this guideline document. Solutions should consider the needs, expectations, and requirements of the organization that owns the facility and the customers it serves. Where controls are mentioned in this document, they are meant to be illustrative and capture high-level expectations of performance, not explicit solutions. Ultimately, designs that are built upon this guidance should strive for diverse and complementary controls that work together to provide a security posture for these sites that is in line with a defined risk appetite or threshold for the organization, facility, or service delivered.

6 References

Resources for more information and guidance related to physical security are provided below. This list is not exhaustive and is intended only to provide a starting point for additional reading on this topic.

- ASIS International General Security Risk Assessment
- ASIS International Information Asset Protection (IAP)
- ASIS International Physical Asset Protection Standard (PAP)
- ASIS International Physical Security Principles
- ASIS International Protection of Assets (POA)
- ASIS International Risk Assessment Standard
- Cyber Infrastructure Security Association (CISA) Publications
- Effective Physical Security by Lawrence J. Fennelly
- EVS-EN 50600-2-5:2021 Data Centre Facilities and Infrastructures - Security Systems
- Interagency Security Committee (ISC) Standards
- ISO/IEC 27001 Information Security Management
- The Complete Guide to Physical Security byPaul R. Baker & Daniel J. Benny
- The Risk Management Process for Federal Facilities
- U. S. Army Manual on Physical Security

7 License

Creative Commons

OCP encourages participants to share their proposals, specifications, and designs with the community. This is to promote openness and encourage continuous and open feedback. It is important to remember that by providing feedback for any such documents, whether in written or verbal form, that the contributor or the contributor's organization grants OCP and its members irrevocable right to use this feedback for any purpose without any further obligation.

It is acknowledged that any such documentation and any ancillary materials that are provided to OCP in connection with this document, including without limitation any white papers, articles, photographs, studies, diagrams, contact information (together, “Materials”) are made available under the Creative Commons Attribution-ShareAlike 4.0 International License found here: https://creativecommons.org/licenses/by-sa/4.0/, or any later version, and without limiting the foregoing, OCP may make the Materials available under such terms.

As a contributor to this document, all members represent that they have the authority to grant the rights and licenses herein. They further represent and warrant that the Materials do not and will not violate the copyrights or misappropriate the trade secret rights of any third party, including without limitation rights in intellectual property. The contributor(s) also represent that, to the extent the Materials include materials protected by copyright or trade secret rights that are owned or created by any third-party, they have obtained permission for its use consistent with the foregoing. They will provide OCP evidence of such permission upon OCP’s request. This document and any "Materials" are published on the respective project's wiki page and are open to the public in accordance with OCP's Bylaws and IP Policy. This can be found at http://www.opencompute.org/participate/legal-documents/. If you have any questions, please contact OCP.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

8 About Open Compute Foundation

At the core of the Open Compute Project (OCP) is its Community of hyperscale data center operators, joined by telecom and colocation providers and enterprise IT users, working with vendors to develop open innovations that, when embedded in products, are deployed from the cloud to the edge. The OCP Foundation is responsible for fostering and serving the OCP Community to meet the market and shape the future, taking hyperscale led innovations to everyone. Meeting the market is accomplished through open designs and best practices, and with data center facility and IT equipment embedding OCP Community-developed innovations for efficiency, at-scale operations and sustainability. Shaping the future includes investing in strategic initiatives that prepare the IT ecosystem for major changes, such as AI & ML, optics, advanced cooling techniques, and composable silicon. Learn more at www.opencompute.org.