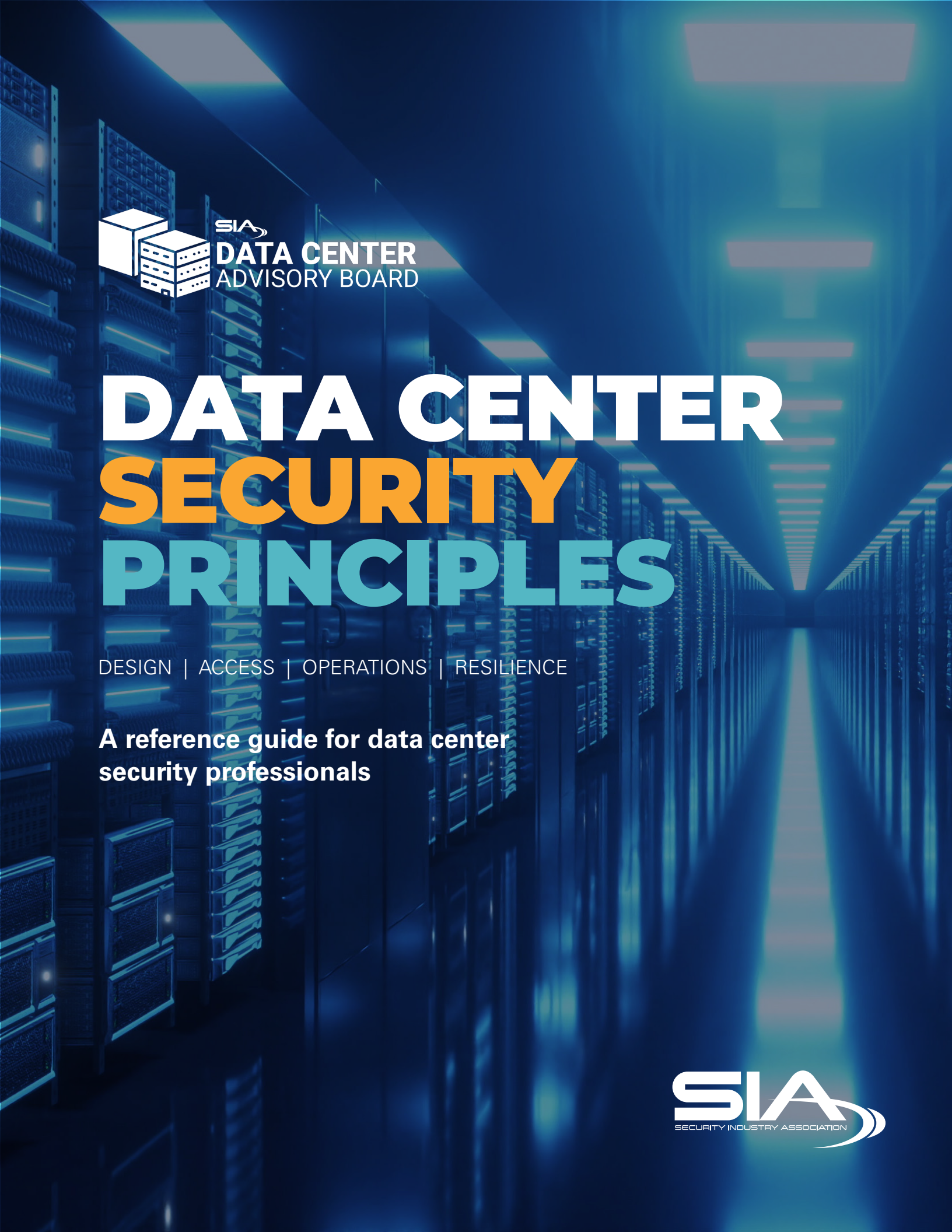

SIA DATA CENTER ADVISORY BOARD

DATA CENTER SECURITY PRINCIPLES

DESIGN | ACCESS | OPERATIONS | RESILIENCE

A reference guide for data center security professionals

SIA
SECURITY INDUSTRY ASSOCIATION

Introduction to Data Center Security Principles

> **“Data centers are foundational to the operation, resilience and long-term sustainability of nearly every other critical infrastructure sector.”**

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 becomes ever more central to modern life, the need for practical, credible and broadly applicable security guidance has never been greater.

Data centers are foundational to the operation, resilience and long-term sustainability of nearly every other critical infrastructure sector. They support the digital systems behind communications, finance, health care, transportation, government services, energy and many other essential functions that communities and economies rely on every day. As this dependence continues to grow, so does the need for clear and enduring physical security principles for the facilities that make it possible.

As chair of the Data Center Advisory Board, I am pleased to introduce these Principles for Data Center Security. 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.

Many of the principles presented here will be familiar. In some cases, they align closely with principles already used across other critical infrastructure sectors, and in others they are identical. That consistency is intentional: it reflects the reality that data centers share many of the same security priorities and risk considerations as other mission-critical facilities. It also means these principles may be useful to stakeholders beyond the data center sector who face similar risks and physical security challenges.

Most importantly, these principles are intended to serve as the cornerstone for the Data Center Advisory Board’s upcoming work on physical security best practices for data centers. By establishing a common foundation now, we build toward more detailed and actionable guidance that helps organizations strengthen protection, improve consistency and adapt to evolving threats with confidence.

I would like to close by expressing my sincere appreciation to 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

DATA CENTER SECURITY

12 PRINCIPLES AT A GLANCE

Design & Architecture

1. **Early Security Engagement**
   Security stake-holders at the table before land is acquired or leases signed.
2. **Secure by Design**
   Security built in from the very start not added later.
3. **Defense in Depth**
   Multiple overlapping layers of security so no single control is a single point of failure.
4. **Secure by Default**
   Protections are on by default, no extra steps, no opt-in.

Access & Trust

5. **Least Privilege**
   Grant only the minimum access required, nothing more.
6. **Proportionate Security Friction**
   Right-sized friction, enough to mitigate risk, not enough to impede operations.
7. **Zero Trust**
   No entity, user, system or device is trusted by default.

Operations & Management

8. **Secure Operations**
   Continuous improvement of controls and monitoring to meet evolving threats.
9. **Streamlining**
   Fewer systems, fewer vendors, fewer vulnerabilities.
10. **Risk-Based Controls**
    Security investments guided by formal risk assessments, not assumptions.

Resilience & Adaptability

11. **Resilience**
    Recover fast, maintain dependability, design for failure from the start.
12. **Adaptability**
    Scale and flex as demands change, without compromising baseline security.

DESIGN & ARCHITECURE

1 Early Security Engagement

Security stakeholders at the table before land is acquired or leases signed.

Security stakeholders shall participate in site selection activities prior to land acquisition, development or lease execution to assess risk and positively influence decision-making. Data center locations must be selected with full consideration of threat exposure, current/future adjacencies, jurisdictional factors and the ability to meet required physical security standards without undue reliance on excessive or cost prohibitive compensating measures.

2 Secure by Design

Security built in from the very start not added later.

The secure by design principle emphasizes incorporating security measures from the outset of the development process. Owners must consider security requirements during the initial design stages, ensuring that security is an integral part of the system's development and implementation rather than an afterthought.

DESIGN & ARCHITECURE

3 Defense in Depth

Multiple overlapping layers of security so no single control is a single point of failure.

This principle advocates multiple layers of security controls to protect from various physical and cyber threats. By implementing a combination of preventive, detective and corrective measures, owners can create a robust defense mechanism that minimizes the risk of attacks. Successive and complementary layers of protection ensure that no single measure is exclusively relied upon for protection, and that subsequent layers support (or compensate for) weaknesses, inefficiencies, failures or the defeat of other layers.

4 Secure by Default

Protections are on by default, no extra steps, no opt-in.

Security protections are enabled and enforced by default, require no extra effort and are not optional. Every product must have security features enabled and active by default. Privacy settings should always be turned on, rather than requiring users to opt in.

ACCESS & TRUST

5 Least Privilege

Grant only the minimum access required, nothing more.

The principle of least privilege ensures that individuals, processes and devices have only the minimum level of access necessary to perform their tasks/functions. By restricting access rights to the minimum necessary (both physical and logical), owners can reduce the attack surface and limit the potential impact of security breaches. Implementing role-based access ensures tighter control over who can enter critical areas or modify systems.

6 Proportionate Security Friction

Right-sized friction, enough to mitigate risk but not impede operations.

Security controls shall introduce only the level of user friction necessary to effectively mitigate identified risks, ensuring a balance between protection and usability. Customer experience should remain as seamless as possible while still meeting defined security requirements, avoiding unnecessary measures that do not materially reduce risk. When choosing between measures of equal protection capabilities and total cost of ownership, favor those with the least impact to operations.

7 Zero Trust

No entity, user, system or device is trusted by default.

Zero Trust is a security model that assumes no inherent trust in any entity (user, system or device), regardless of location. It requires continuous verification of identities and strict access controls based on contextual factors. By adopting zero trust, owners enhance security by eliminating implicit trust and enforcing stringent authentication, authorization and monitoring.

OPERATIONS & MANAGEMENT

8 Secure Operations

Continuous improvement of controls and monitoring to meet evolving threats.

Security controls and monitoring will continuously be improved to meet current and future threats. Incorporate security logs and monitor them. Default credentials must be removed and replaced by robust controls.

9 Streamlining

Fewer systems, fewer vendors, fewer vulnerabilities.

Streamlining embodies both simplicity and serviceability. Reducing technology choices to fewer brands of products simplifies service and maintenance processes, making it easier to manage changes, including firmware and software updates. Leveraging streamlined technologies optimizes operational efficiency, lowers maintenance costs, enhances security and reduces risks. Fewer technologies and product models mean fewer potential points of failure and fewer variables that could introduce unpredictability. Streamlined systems are more resilient to threats, with fewer vulnerabilities and easier implementation of security updates. Additionally, supply chain risks are minimized, making inventory management and potential disruption prediction more manageable.

10 Risk-Based Controls

Security investments guided by formal risk assessments, not assumptions.

Security investments and operational decisions are guided by formal risk assessments, ensuring that protections are applied commensurate with the likelihood and impact of threats. Higher-risk scenarios receive stronger, layered controls, while lower-risk locations/areas are managed with appropriately scaled measures to optimize effectiveness and resource utilization.

RESILIENCE & ADAPTABILITY

11 Resilience

Recover fast, maintain dependability, design for failure from the start.

Resilience refers to technology's ability to recover from a fault or change and maintain service dependability. Redundancy (e.g., the intentional duplication of technology components to increase a system's dependability) is one method of enhancing resilience. Physical and logical network redundancy prevents a single failure from causing downtime. Backup power sources and multiple independent utility feeds prevent temporary or permanent disruptions from causing technologies to fail. Owners should also evaluate disaster recovery scenarios and plan for near-immediate fallback to alternate sites. Ensure backup systems are isolated from primary environments to avoid compromise. Critical security functions, technology and infrastructure must be designed with resilience in mind.

12 Adaptability

Scale and flex as demands change, without compromising baseline security.

This includes both scalability—the capability of a system and technology to handle increased workload or expand its capacity without compromising performance—and flexibility—the ease with which systems and technologies can be modified or adjusted to meet new or unforeseen circumstances. Owners must plan for future growth and technology evolution without compromising baseline security. Use modular designs that can adapt to new capacity demands, device types or additional security controls.