

5 BEST PRACTICES FOR A MORE SECURE DATA CENTER

In 2024, the U.S. data center market size by investment was valued at USD \$208.38 billion, and is projected to reach \$308.83 billion by 2030.

This industry is growing at a rapid pace, but are data center operators prepared to implement the high level of security required to protect their facilities?

1. Implement multi-layered access control:

With a large portion of data breaches happening due to unauthorized physical access into data centers, combining physical and digital layers of access control that accurately authenticate an individual's identity can help reduce, or even eliminate, this risk.

2. Audit rigorously and regularly:

Schedule and maintain regular audits of access activity and conduct periodic vulnerability assessments of your security hardware, software, and infrastructure, as well as your security policies and procedures. Consider hiring professional "hackers" for penetration testing to identify faults and unknown vulnerabilities.

3. Train your most important asset:

Your employees can serve as your most powerful security tool. Train them on security awareness with regular training on phishing, social engineering, and physical security protocols so they can identify potential vulnerabilities. Establish and publish anonymous reporting procedures to make it easy for them to call out bad actors and threats.

4. Establish an access control data backup:

If your data center goes down or you experience a hack, you'll want to be sure ONLY the right people gain access while issues are resolved. Implement automated, encrypted access control data backups, stored in secure, geographically diverse locations.

5. Isolate important systems:

Isolating physical security systems on a dedicated network helps protect it in the instance of a hack, while also protecting client data in the instance there is a breach to your security system. Consider using VLANs (virtual local area network) and firewalls to isolate these systems and reduce the attack surface.

When choosing an access control platform, ensure that it meets the following criteria:

- Multimodal identity authentication, like Iris/Face fusion
- Support for Multifactor Authentication (MFA)
- Compatibility with MIFARE®/DESfire® Proximity Cards
- Supports Presentation Attack Detection (PAD)
- High User Capacity – up to 100k users
- Rapid Match Speeds of less than 1 second

Secure your data center with the only proven iris and facial recognition fusion technology designed for high-security data centers and environments that demand secure access control.

For more information
visit [IrisID.com](https://www.irisid.com)

