salto

INSPIRED ACCESS

Version 1 (November, 2025)

Cybersecurity Framework, Compliance, and Best Practices.

SALTO WECOSYSTEM

Cybersecurity Framework,
Compliance,
and Best Practices.

Index

INTRODUCTION

Why Is Cybersecurity Important?

In an increasingly interconnected world, cybersecurity has become a cornerstone of trust, resilience, and operational continuity. For companies like **Salto**, which specialize in advanced access control solutions, the stakes are particularly high. The integrity of digital infrastructure directly impacts physical security, customer confidence, and regulatory compliance.

The Expanding Threat Landscape

Cyber threats are evolving rapidly. From ransomware and phishing to supply chain attacks and insider threats, organizations face a wide array of risks that can disrupt operations, compromise sensitive data, and damage reputations. The convergence of IT and OT (Operational Technology) in smart building environments further amplifies these risks, making cybersecurity not just an IT issue, but a business-critical priority.

Why It Matters for Salto

As a trusted provider of advanced electronic locking solutions and cloud-based access platforms, Salto plays a key role in safeguarding physical and digital environments. By securely managing sensitive data such as user credentials, access logs, and system configurations, Salto ensures seamless and reliable access control for its clients. Demonstrating compliance with leading security standards and regulations like ISO 27001, GDPR, and NIS 2 not only reinforces our commitment to data protection but also strengthens customer confidence. In today's market, clients actively seek partners who prioritize security and transparency making our robust approach a clear competitive advantage.

Cybersecurity is not just about defense, it's about **enabling secure innovation**. It allows Salto to confidently expand its digital offerings, integrate with third-party platforms, and support remote management capabilities without compromising safety.

A Strategic Imperative

Cybersecurity must be embedded into the DNA of the organization, from product design and development to deployment and support. It requires a proactive, layered approach that includes governance, technical controls, employee awareness, and continuous monitoring.

This white paper outlines Salto's cybersecurity strategy, its alignment with industry best practices, and its roadmap for building a resilient, secure future.

CHAPTER 1: Cybersecurity Framework

At Salto, cybersecurity is not just a technical requirement—it's a strategic pillar that supports our mission to deliver secure, smart access solutions to clients worldwide.

Our cybersecurity framework is built upon a robust Information **Security Management System (ISMS)**, which provides the foundation for all our security practices. This ISMS is **certified to ISO/IEC 27001**, the globally recognized standard for information security, demonstrating our commitment to continuous improvement, risk management, and regulatory compliance.

This framework enables Salto to deliver secure, scalable, and resilient access control solutions while meeting the expectations of clients across industries. By aligning with international standards and embedding security into every layer of our operations, we help our clients meet their own compliance goals, reduce risk, and build trust with their stakeholders.

The following sections outline the key components of our cybersecurity framework, designed to protect sensitive data, ensure system integrity, and support business continuity.

1. Security Policies and Standards

Salto maintains a comprehensive set of security policies and standards that guide our operations, development, and service delivery.

To ensure comprehensive coverage and global relevance, our policy framework is informed by:

> **ISO 27001 / 27002:** Provides detailed guidance on implementing security controls across domains such as access control, cryptography, physical security, and operations management.
> **NIST Cybersecurity Framework (CSF):** Offers a structured, risk-based approach built around five core functions **(Identify, Protect, Detect, Respond, and Recover)** which guides our strategic and operational decisions.
> **ETSI EN 303 645:** A key standard for cybersecurity in IoT devices, ETSI 303 645 helps ensure our connected products meet security requirements, including secure default settings, software update mechanisms, and data protection.

By aligning these frameworks, Salto ensures that our security posture meets the expectations of clients across regulated industries, including hospitality, healthcare, education, and critical infrastructure.

The following sections detail the key policies and standards that underpin Salto's cybersecurity program.

2. Roles and Responsibilities

Clear roles and responsibilities are defined across the organization to ensure accountability in cybersecurity. From executive leadership to technical teams, every employee understands their part in maintaining a secure environment.

3. Backup and Recovery

We implement automated, encrypted backups across critical systems, with regular testing of recovery procedures. This ensures data integrity and availability in case of system failures or incidents.

4. Business Continuity Plan (BCP)

Our BCP framework ensures operational resilience. It includes risk assessments, continuity strategies, and recovery plans to minimize downtime and maintain service delivery during disruptions.

5. Cryptography

Salto uses strong encryption protocols to protect data in transit and at rest. Our cryptographic standards align with industry best practices, ensuring confidentiality and integrity across our platforms.

6. Identity and Access Management (IAM)

We enforce strict IAM controls, including Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and periodic access reviews. These measures ensure that only authorized users can access sensitive systems and data.

7. Detection and Response (SOC)

At Salto our **Security Operations Center (SOC)** is a cornerstone of our proactive cybersecurity strategy. It enables us to detect, analyze, and respond to threats in real time, ensuring the continuous protection of our infrastructure, services, and customer data. Our SOC operates 24/7 around the clock leveraging advanced **Security Information and Event Management (SIEM)** tools to monitor logs, network traffic, and system activity across our cloud and on-premises environments.

8. IT Security Operations

We maintain a proactive IT security posture through:

> Endpoint Detection and Response (EDR)
> Regular patch management
> Vulnerability scanning and remediation

These practices help us stay ahead of emerging threats and maintain system integrity.

9. Network Security

Our network architecture includes firewalls, intrusion detection systems, segmentation, and secure VPNs. These controls protect against unauthorized access and ensure secure communication across environments.

10. Personnel Security

All employees sign confidentiality agreements and receive ongoing training. We foster a culture of security awareness and accountability.

11. Physical Security

Salto facilities are protected by access controls, surveillance systems, and visitor management protocols. Physical assets are safeguarded to prevent unauthorized access or tampering.

12. Data Protection and Privacy

We adhere to GDPR and other global privacy regulations. Our data handling practices ensure transparency, user control, and lawful processing of personal information.

Further information on the privacy chapter of this document is provided.

13. Remote Working

Secure remote access is enabled through mandatory use of our corporate encrypted connections, MFA, and endpoint protection. Our policies ensure that remote work does not compromise security.

14. Secure Development & Security by Design

Security by design is a core principle embedded through our software development lifecycle through secure coding practices, automated testing, and code reviews.

Salto complements internal efforts with regular **penetration tests** through external security partners to simulate real world attacks.

Salto has a bug **bounty program** to engage ethical hackers and security researchers in identifying vulnerabilities before they can be exploited.

Salto's vulnerability management process ensures that vulnerabilities are identified, prioritized, and addressed promptly.

15. Risk Management

Salto conducts regular risk assessments to identify, evaluate, and mitigate cybersecurity risks. Our risk register is actively maintained and informs strategic decisions.

16. Security Awareness and Training

Employees receive tailored training on cybersecurity, phishing, data protection, and incident response. Awareness campaigns and simulations reinforce best practices across the organization.

17. Vendor Management

Third-party vendors are assessed for security posture and compliance. Contracts include security clauses, and we monitor vendor performance to ensure alignment with Salto's standards.

CHAPTER 2: Security Benefits

Salto integrates robust security controls across its entire technology stack, **hardware, software, and mobile platforms** to deliver secure, scalable, and resilient access control solutions. These measures are designed to protect sensitive data, prevent unauthorized access, and support compliance with international standards.

1. Hardware Security

Salto's electronic locks and IoT devices are built with embedded security features aligned with **ETSI EN 303 645**, the leading standard for IoT cybersecurity. Key controls include:

> **No default passwords:** Devices require strong, unique credentials.
> **Secure firmware updates:** Authenticated updates ensure vulnerabilities are patched safely.
> **Encrypted communication:** Strong cryptographic algorithms protect data in transit.
> **Secure storage:** Sensitive parameters are stored using secure elements or encrypted memory.
> **Minimized attack surface:** Unused interfaces are disabled; regular pentests are conducted.
> **Physical security:** Tamper-resistant design and default-enabled security features.
> **Resilience:** Devices are designed to operate securely during network or power outages.

2. Software and Cloud Security

Salto's software platforms are developed using secure coding practices and aligned with **OWASP** and **ISO/IEC 27002** standards. Key controls include:

> **Password policies and 2FA:** Enforced authentication mechanisms.
> **Encryption at rest and in transit:** Protects sensitive data throughout its lifecycle.
> **Granular access control:** Role-based permissions and app-level management.
> **Secure development lifecycle:** Includes code reviews, threat modeling, and regular penetration testing.
> **High availability and continuity:** Resilient infrastructure ensures uptime even during data center failures.

In addition, Salto's cloud-based services are hosted on **trusted cloud providers**, which provide a secure and compliant foundation certified under internationally recognized standards including **ISO/IEC 27001** and **SOC 2 audit attestation.**

While the cloud provider ensures the infrastructure meets these standards, **Salto implements and manages additional security layers** to protect customer environments, including:

> **Continuous monitoring and threat detection** via Salto's Security Operations Center (SOC)
> **Automated backups and tested recovery procedures**
> **Secure identity and access management**
> **Automated vulnerability scanning**
> **Configuration hardening and vulnerability management** across cloud workloads

This shared responsibility model ensures that Salto's cloud architecture is not only compliant and scalable, but also actively managed and monitored to meet the highest standards of cybersecurity.

3. Mobile App Security

Salto's mobile applications are designed with multiple layers of security and aligned with **OWASP MASVS** standards. Key features include:

> **Secure architecture and design:** Vulnerabilities are addressed before deployment.
> **Encrypted data storage and transmission:** Protects personal information from unauthorized access.
> **Authentication and session management:** Secure login and session controls.
> **Secure communication protocols:** Ensures safe interaction with backend systems.
> **Privacy controls:** Users have control over personal data usage.
> **Google MASA certification:** Independent validation by Google Authorized Labs of security for several of our apps.

4. Client Benefits

By implementing these security measures, Salto delivers:

> **End-to-end protection** across physical, digital, and mobile environments
> **Compliance-ready infrastructure** for regulated industries
> **Operational resilience** through secure design and recovery capabilities
> **User trust and transparency** via certified apps and secure data handling
> **Scalable security** that grows with client needs and integrates with third-party systems

CHAPTER 3: Security Compliance

At Salto, security compliance is a strategic commitment. Our certifications and alignment with international standards reflect our dedication to protecting customer data, supporting regulatory requirements, and delivering secure, reliable access control solutions across industries.

1. ISO/IEC 27001 Certification

Salto operates under a robust **Information Security Management System (ISMS)** certified to **ISO/IEC 27001**, the global benchmark for information security. This certification confirms that Salto applies a structured, risk-based approach to managing sensitive data, protecting digital and physical assets, and continuously improving its security posture.

Importantly, **Salto's solutions are designed and delivered within the scope of this certified ISMS.** Our cloud platforms, software applications, and supporting infrastructure are developed, maintained, and operated in accordance with ISO 27001 principles ensuring consistent protection, accountability, and resilience.

✓ ISO 27001 certification provides clients with confidence that Salto's ISMS are independently validated, aligned with global best practices, and built to support compliance in regulated environments.

For more details, clients can refer to the official certificates Certifications | Salto Systems

2. MASA Certification for Mobile Apps

Salto's mobile applications are developed with security at their core, following industry best practices and secure development standards. Our apps have achieved **MASA (Mobile Application Security Assessment)** certification, confirming compliance with the **OWASP MASVS** standard through a Google Authorized Lab. This ensures they meet rigorous practices in:

> Secure architecture and design
> Data encryption at rest and in transit
> Authentication and session management
> Privacy controls and secure communication protocols

For more details, clients can refer to the official certificates Certifications | Salto Systems

Cybersecurity Framework,
Compliance,
and Best Practices.

3. BSI Kitemark™ for IoT and Secure Applications

Salto has earned two prestigious certifications from the **British Standards Institution (BSI):**

> The **BSI Enhanced Level IoT Kitemark**™, which confirms that selected Salto hardware products meet advanced cybersecurity requirements based on the **ETSI EN 303 645 standard.**
> The **BSI Kitemark™ for Secure Digital Applications**, which certifies that Salto ProAccess Space and Justin mobile app meet the **OWASP ASVS** standard for secure software development.

These certifications demonstrate that Salto's solutions, both physical and digital, are designed to resist cyber threats, support secure updates, and protect user data throughout their lifecycle.

🔒 For more details, clients can refer to the official certificates:

> BSI IoT Kitemark Certificate (KM_723320)

> BSI Secure Applications Kitemark Certificate (KM_731184)

4. NIS 2 and DORA Compliance

Salto not only supports clients in meeting the requirements of the **European NIS 2 Directive** and the **Digital Operational Resilience Act (DORA)**, we also ensure our own operations and solutions are aligned with these regulations.

How Salto Meets NIS 2 Requirements

Salto's internal security practices and product architecture are designed to comply with NIS 2 obligations, including:

> Risk management and governance: Our ISO 27001 certified ISMS includes formal risk assessments, incident response plans, and business continuity strategies.
> Technical and organizational measures: We implement strong access controls, encryption, secure development practices, and vulnerability management across all systems.
> Incident handling and reporting: Salto maintains a structured process for detecting, responding to, and reporting security incidents, supported by our SOC and security advisories.
> Supply chain security: We assess and monitor third-party vendors to ensure they meet Salto's security standards.
> Continuous improvement: Our compliance **program** is regularly reviewed and updated to reflect evolving regulatory requirements and threat landscapes.

How Salto Supports Customer Compliance

Our access control and identity management solutions help clients comply with NIS 2 and DORA by offering:

> Granular access control and multi-factor authentication
> Visitor management with digital registration and real-time alerts
> Comprehensive audit trails for access events
> Secure infrastructure and resilient cloud services

DOWNLOAD ⤓ **NIS 2 & DORA Compliance Overview (PDF)**

5. Privacy and GDPR

At Salto, privacy is a priority. Salto is committed to protecting personal data in accordance with the highest international standards, including the European Union's General Data Protection Regulation (GDPR).

Here's how we safeguard the personal data:

> Responsible Data Use: We collect and process personal data only when necessary to deliver our services, enhance your experience, or meet legal and contractual obligations.
> Global Transparency: We provide clear, accessible information about how data is used, regardless of your location.
> Strong Security: We implement advanced security measures such as encryption, access controls, and continuous monitoring to protect data from unauthorized access, loss, or misuse.
> Respect for Customers' Rights: Customers have rights over their personal data, including access, correction and deletion.
> Trusted Partnerships: When we share data with service providers or partners, we ensure they meet strict privacy and security standards, and only for legitimate business purposes.
> No Data Sales: We never sell customers' personal data. Customer trust is our foundation, and we treat their information with the utmost respect.

Salto is dedicated to building secure and privacy-conscious solutions. For more information about Salto Privacy Policy, clients can refer to to Salto Systems | Salto Systems

6. Additional Standards and Practices

Salto's broader compliance efforts include:

> **Responsible Disclosure Policy:** Encouraging ethical reporting of vulnerabilities
> **Bug Bounty Program:** Engaging external researchers to strengthen our defenses

Client Assurance

By choosing Salto, clients gain access to a security ecosystem that is:

> Certified, transparent, and independently validated
> Aligned with global and regional regulations
> Designed to support compliance and reduce risk exposure
> Continuously monitored and improved

Security compliance is not just a checkbox, it's a strategic advantage that Salto delivers with every solution.

SALTO WECOSYSTEM
INSPIRED ACCESS

saltosystems.com

Version 1 (November, 2025)