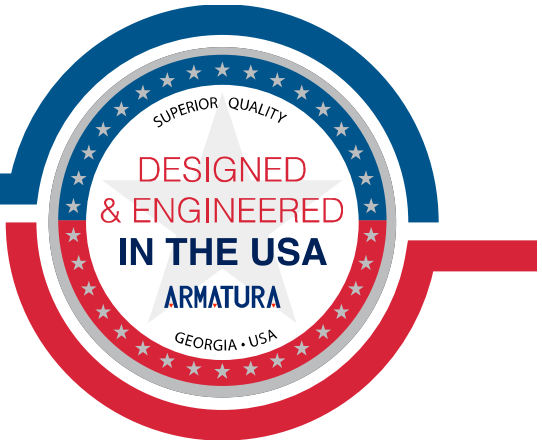
ARMATURA

MADE IN THAILAND




# Armatura Access Control System Data Security Whitepaper

Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

ARMATURA

MADE IN THAILAND

# TABLE OF CONTENTS





Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

## Executive Summary

In the contemporary landscape of security, Armatura has established itself as a leader in delivering robust and sophisticated access control solutions. Our systems are meticulously engineered to provide unparalleled protection, leveraging cutting-edge technology to address the complex security demands of various environments.

At the core of our offerings, you'll find a commitment to both physical and digital security measures. Armatura's hardware components, including multi-technology RFID readers, biometric terminals, and controllers, are designed to meet and exceed the highest standards for durability and tamper resistance. These devices attain IP68 and IP66 ratings for dust and water resistance, IK10 and IK07 ratings for impact resistance, and are constructed with UL94-V0 fire-resistant materials, ensuring they stand strong against environmental challenges and unauthorized access attempts.

In terms of digital security, our secure network design incorporates VLANs, 802.1X authentication, and anti-SYN flood attack mechanisms, creating a fortified barrier against cyber threats. Our approach to data backup and recovery features high-availability systems, regular data backups, disaster recovery plans, and load balancing architectures to ensure continuous operation and data integrity.

A critical aspect of our system is the self-developed biometric technology, including touchless palm recognition, face recognition, and fingerprint identification, all based on advanced computer vision, deep learning, and neural networks. We prioritize user privacy and data security by employing biometric templates protected by AES256 encryption and integrating anti-spoofing measures across software and hardware levels.

Our comprehensive strategy encompasses continuous improvement through security audits, compliance with international standards like ISO 27001, ISO 27701, and ISO 27017, and a proactive incident response and management plan to swiftly address and mitigate security events.

Armatura's Access Control System is not just a product; it is a promise of security, reliability, and innovation. It reflects our deep understanding of the security challenges our clients face and our relentless pursuit of excellence to address them effectively. With our system, clients are equipped to protect their assets and operations against the evolving threats of the digital age.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

## Introduction

In the modern era of ubiquitous connectivity and smart environments, the lines between physical and digital security are increasingly blurred. Access control systems, traditionally focused on physical security, now integrate complex information technology systems to manage access permissions, monitor security protocols, and collect data. Armatura's Access Control System is at the forefront of this integration, offering a sophisticated solution that addresses both the physical and cyber security needs of our clients.

The integration of these domains, while providing enhanced security and convenience, also introduces new challenges. Sensitive data such as personal identification details, access logs, and security configurations are now part of the digital fabric of an organization. Protecting this data from unauthorized access, manipulation, or breaches is paramount to maintaining security, privacy, and trust.

Armatura understands that an effective access control system must not only restrict physical access to authorized individuals but also safeguard the data that underpins the system itself. Our commitment to data security is comprehensive, aiming to protect against both external threats and internal vulnerabilities. We recognize that a security system is only as strong as its weakest link, and in today's threat landscape, data security is often that critical juncture.

This whitepaper provides an in-depth exploration of Armatura's data security strategy. It outlines the rigorous encryption standards we employ, the secure hardware that underpins our systems, our adherence to international compliance protocols, and the proactive measures we take to manage and mitigate threats. As we navigate the complexities of data security in access control, our mission is to deliver a system that clients can rely on without reservation, assured by the knowledge that their data is as secure as the facilities they are protecting.

We invite you to read on and gain insight into the sophisticated security measures that make the Armatura Access Control System a leader in the industry, reflecting our unyielding dedication to innovation, excellence, and the security of our clients.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

## Background

The Armatura Access Control System has been engineered to serve as a robust guardian against unauthorized entry and data breaches. As enterprises evolve and expand in complexity, the need for more sophisticated and integrated access control solutions becomes imperative. Armatura's solution is designed to meet the challenges posed by a diverse array of environments, from corporate offices and government buildings to critical infrastructure and data centers.

### The Need for Integrated Security

In a world where security threats have transcended physical boundaries to include cyber domains, an integrated approach to access control is no longer optional—it is essential. The convergence of cybersecurity and physical security in access control systems is a direct response to this evolving threat landscape. Armatura's systems are engineered to not only control access but also to create an audit trail, monitor real-time events, and provide actionable intelligence for security operations.

### Data-Centric Security Approach

At the core of the Armatura solution is the recognition that data is a valuable asset that requires stringent protection. Our systems handle a multitude of sensitive information, including but not limited to user identities, biometric data, access patterns, and security protocols. The integrity and confidentiality of this data are critical to maintaining operational security and user privacy.

### Commitment to Standards and Compliance

Armatura's systems are developed in alignment with the highest industry standards. Our commitment to excellence is reflected in our attainment of CMMI Level 5 status, demonstrating our dedication to continuous improvement and quality control. Compliance with GDPR, CCPA, and ISO standards such as ISO 27001, ISO 27701, and ISO 27017 exemplifies our approach to ensuring data protection and privacy. Additionally, we align our systems with BS EN 60839-11-1:2013 Grade 3 and Grade 4 standards, signifying our capability to deliver solutions that are suitable for environments where a high level of security is essential.

### System Architecture

The Armatura Access Control System is built on a modular architecture, which allows for scalability and flexibility. Our system is designed to integrate seamlessly with a range of hardware and software components, ensuring compatibility and interoperability across different security ecosystems. This architecture enables our clients to tailor the system to their specific security requirements, whether they are deploying a new system or enhancing an existing one.

In the following sections of this whitepaper, we will delve into the specific data security measures that Armatura implements across its access control solutions—measures that are designed to protect against both current and emerging threats to



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

data security. Our aim is not only to prevent unauthorized physical access but also to ensure the resilience and integrity of the underlying data that powers these advanced security systems.

## Threat Landscape

The threat landscape in the realm of access control systems is a dynamic and evolving space, with new challenges emerging as technology advances. Armatura's Access Control System is designed to anticipate and respond to a broad spectrum of potential threats. Understanding these threats is crucial in developing and maintaining a resilient security posture.

**Cyber Threats**

- Data Breaches:
  Sensitive data stored by access control systems can be a prime target for attackers seeking to exploit personal information, gain unauthorized access, or disrupt operations.
- Advanced Persistent Threats (APTs):
  APTs are sophisticated, stealthy, and continuous hacking processes often orchestrated by nation-states or criminal organizations to extract or destroy data.
- Man-in-the-Middle Attacks (MitM):
  These occur when attackers insert themselves into the communication process to intercept, manipulate, or steal data.
- Ransomware and Malware:
  Malicious software can be used to encrypt data, making it inaccessible until a ransom is paid, or to damage systems and data integrity.
- Phishing Attacks:
  These social engineering attacks are designed to trick users into revealing sensitive information or credentials.
- Insider Threats:
  Disgruntled employees or those with malicious intent can exploit their access to compromise the security of the system.

**Physical Threats**

- Tampering:
  Direct interference with access control hardware can lead to system breaches or data leakage.
- Theft of Devices:
  The theft of devices containing sensitive information can lead to a direct data breach.
- Environmental Damage:
  Natural disasters or environmental factors can damage physical hardware, leading to potential data loss or system compromise.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

- Regulatory Challenges
- Compliance Risks:
  Failure to adhere to data protection regulations can lead to legal repercussions, financial penalties, and reputational damage.
- Cross-Border Data Transfer:
  Different jurisdictions have varying data protection laws, complicating the management and storage of data.

**Emerging Threats**

- IoT Vulnerabilities:
  As access control systems become more connected through the Internet of Things (IoT), they face additional vulnerabilities from poorly secured devices.

**AI-Powered Attacks:**

- Artificial Intelligence (AI) can be used by attackers to automate and adapt attacks at scale, requiring advanced defensive measures.

**Quantum Computing:**

- The potential future use of quantum computing could render current encryption standards obsolete, necessitating pre-emptive planning for quantum-resistant encryption methods.

Armatura's Access Control System is architected to address these threats head-on, with layered security measures, constant monitoring, and adaptive responses. Our approach to threat management involves not only defensive strategies but also predictive analytics and threat intelligence to stay ahead of potential security challenges. The subsequent sections of this whitepaper will detail the specific security controls and practices Armatura employs to mitigate these threats.

## Data Security Fundamentals

Armatura's Access Control System is founded upon rigorous data security fundamentals, ensuring the protection of sensitive data against a myriad of threats. Below we detail the critical security features that fortify our system's integrity, confidentiality, and availability.

**Encryption**

Encryption serves as a critical line of defence for data both at rest and in transit within the Armatura system.

- **Advanced Encryption Standard (AES):** We utilize AES with 128bits and 256-bit keys to encrypt sensitive data, safeguarding against unauthorized access.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

- **Transport Layer Security (TLS) 1.2:** To secure data during transmission, Armatura systems implement TLS1.2 protocols, ensuring robust encryption for network communications.
- **RSA Encryption:** Our system uses the RSA-4096 bits algorithm for secure key exchanges, maintaining the confidentiality of encryption keys even over potentially unsecured channels.
- **Open Supervised Device Protocol (OSDP):** Standard OSDP communications are protected with AES128 encryption, enhancing the security of data exchange between devices.
- **Supervised Inputs:** Our controllers and IO expansion boards come with supervised inputs that alert the system to any unauthorized interference.
- **Magnetic Tamper Systems:** Armatura's readers and standalone terminals are fortified with magnetic tamper systems, which detect and signal any unauthorized tampering attempts.

**Access Management**
Robust access management is crucial for maintaining control over who can access or modify the system and data.

- **Role-Based Access Control (RBAC):** We assign access privileges based on organizational roles, ensuring that users only access data pertinent to their responsibilities.
- **Multi-Factor Authentication (MFA):** Armatura enhances security by requiring multiple verification methods, significantly reducing the risk of compromised credentials leading to unauthorized access.

**Secure Network Design**
Our network security design is comprehensive and aimed at protecting data in transit from various threats.

- **Network Segmentation with VLAN:** Our network design includes the use of Virtual Local Area Networks (VLANs) to segment the network into separate, isolated logical networks. This segmentation improves security by limiting the broadcast domain and restricting the spread of any potential security breaches.
- **802.1X Authentication:** To further enhance network security, Armatura supports the implementation of 802.1X, an access control protocol that provides an authentication mechanism for devices attempting to connect to a wired or wireless network. This ensures that only authenticated and authorized devices can access network resources.
- **Anti-SYN Flood Attack Mechanisms:** To safeguard against SYN flood attacks, which can overwhelm a network with a flood of TCP/SYN packets, our network infrastructure is equipped with anti-SYN flood mechanisms.


Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us
Version 1.0
FEB 20, 2024

These mechanisms detect and mitigate the effects of such attacks, preserving network availability and performance.

**Secure Hardware**
Armatura's hardware solutions are engineered to provide comprehensive protection against a spectrum of digital and physical security threats. Our commitment to robust security is embodied in the design and features of our hardware components.

- **EAL6+ Rated Crypto Chips:** At the heart of our secure hardware lie EAL6+ rated crypto chips, which are designed to provide a high-assurance environment necessary for performing critical cryptographic operations. These chips offer robust protection against physical tampering, ensuring the security of cryptographic keys and sensitive data.
- **Supervised Inputs:** Our controllers and IO expansion boards come with supervised inputs, an essential security feature that continuously monitors system sensors and alarms for signs of tampering or malfunction. Any unauthorized attempts to interfere with these components are detected and promptly reported, enabling immediate response and mitigation.
- **Magnetic Tamper Systems:** Readers and standalone terminals in the Armatura lineup are equipped with advanced magnetic tamper detection systems. These systems are designed to sense when a device is being physically tampered with and instantly trigger an alarm, alerting the system to the security breach.
- **Anti-DOP (Data-Oriented Programming) Design:** Armatura hardware incorporates an anti-DOP design to protect against data-oriented attacks, which exploit the layout and access patterns of memory. By implementing strict access controls and memory management techniques, our hardware is resistant to such attacks, ensuring the integrity and security of data processing and storage.

By integrating these advanced security features, Armatura delivers hardware that not only meets the highest standards of resilience but also ensures the ongoing reliability and security of the access control system. Our clients can trust that the physical components of their security infrastructure are safeguarded against both digital breaches and physical intrusions.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

**Data Backup and Recovery**
Armatura understands the importance of data availability and business continuity in maintaining a secure access control environment. Our advanced backup and recovery solutions are designed to ensure that critical security systems remain operational and resilient against data loss.

- **High-Availability Systems:** Armatura's access control ecosystem includes dedicated high-availability (HA) systems. These systems are specifically designed to provide redundancy, minimize downtime, and ensure continuous access to essential security services, even in the event of a system component failure.
- **Regular Data Backups:** To protect against data loss, Armatura performs secure and regular data backups. These backups are integral to our data management strategy, allowing us to quickly restore system data to its last known good state in case of corruption or loss.
- **Disaster Recovery Plans:** Our disaster recovery plans are meticulously drafted and tested to address various emergency scenarios. These comprehensive plans ensure that we can swiftly restore operational functionality and data access following disruptive incidents, with clear protocols to minimize the impact on our client's operations.
- **Load Balancing Architecture—Clustered Deployment:** In addition to the above points, Armatura employs a load-balancing architecture with clustered deployment. This approach distributes workloads across multiple computing resources, enhancing the performance of the system under varying loads. It also contributes to the high-availability framework by ensuring that in the event of a server failure, the load can be redistributed, maintaining service continuity and system responsiveness.

The combination of high-availability systems, regular data backups, robust disaster recovery plans, and a load-balancing architecture with clustered deployment positions Armatura as a leader in data protection and recovery within the access control industry.

**Regular Audits and Compliance Checks**
To maintain the highest level of security and to ensure adherence to regulatory standards, Armatura engages in rigorous ongoing evaluation of our access control systems.

- **Security Audits:** Armatura is committed to a regimen of regular security audits. These audits are crucial in identifying potential vulnerabilities within our systems and processes. By proactively analyzing and addressing these findings, we ensure that our security infrastructure remains resilient and up-to-date with the latest security practices.


Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us
Version 1.0
FEB 20, 2024

- **Compliance with International and Industry Standards:** Our systems are meticulously engineered to align with international security standards. We rigorously adhere to standards such as BS EN 60839-11-1:2013 Grade 3 and Grade 4, which are pivotal for environments demanding robust protection against sophisticated attempts to compromise security systems.
- **Adherence to ISO Standards:** In addition to the aforementioned standards, Armatura's systems are designed to meet the stringent requirements of ISO 27001, ISO 27701, and ISO 27017.

    I. ISO 27001 is the leading international standard focused on information security management systems (ISMS), providing a systematic approach to managing sensitive company information so that it remains secure.
    II. ISO 27701 extends the ISMS framework for privacy protection, helping organizations manage the security of personally identifiable information (PII).
    III. ISO 27017 addresses cloud security, providing guidelines on implementing information security controls for cloud service providers and users.

By complying with these ISO standards, Armatura ensures that our systems are not only secure but also managed according to globally recognized best practices for information security, privacy, and cloud service provision. Armatura's commitment to these data security fundamentals underscores our pledge to deliver a comprehensive, resilient, and secure access control system. Each element, from our encryption protocols to our backup mechanisms, is meticulously crafted to provide our clients with a robust defence against the ever-evolving security threats of the digital age.

## Encryption Standards

In the quest to maintain an impregnable security posture, Armatura Access Control Systems incorporate stringent encryption standards to safeguard data integrity and confidentiality.

**Advanced Encryption Standard (AES)**

- AES Encryption: The system harnesses AES256, the industry benchmark for encryption, to secure data at rest. This robust encryption method is renowned for its resilience against all known practical brute-force attacks.

**Transport Layer Security (TLS)**

- TLS Protocols: Armatura systems employ TLS 1.2 for protecting data in transit. These protocols ensure that data communications over a network are within a secure tunnel, impervious to eavesdropping and man-in-the-middle attacks.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

**Rivest-Shamir-Adleman (RSA)**

- RSA Key Exchange: The RSA4096 bits algorithm facilitates the secure transfer of encryption keys in Armatura systems, ensuring that even if data transmission is intercepted, the encrypted information remains indecipherable.

**Open Supervised Device Protocol (OSDP)**

- OSDP with AES128: Armatura embraces OSDP integrated with AES128 encryption to secure communications between access control components, providing heightened security for device interactions.

**Secure Hardware**

- Armatura's commitment to security extends to the physical realm with the integration of tamper-resistant hardware, fortified by industry-leading cryptographic chips.
- EAL6+ Crypto Chips: Our systems incorporate EAL6+ rated crypto chips, ensuring a secure enclave for cryptographic operations. These high-assurance chips are designed to be resilient to physical tampering and secure against sophisticated attacks.

**Key Management**

- The strength of an encryption system is largely dependent on the security of its key management processes.
- Proprietary Key Management System: Armatura has developed a proprietary key management system that meticulously administers the creation, distribution, storage, and retirement of cryptographic keys, maintaining the integrity of our encryption architecture.

**Authentication and Access Control**

Ensuring that only authorized individuals can access sensitive areas and data is a primary function of the Armatura Access Control System.

- Multi-Factor Authentication (MFA): Armatura systems employ MFA, requiring users to verify their identity using multiple credentials before gaining system access, thus significantly reducing the risk of unauthorized entry.
- Role-Based Access Control (RBAC): RBAC is implemented to define user privileges based on roles within the organization, ensuring users have access only to the data and resources necessary for their job functions.
- Biometric Authentication: Where the highest level of user authentication is required, Armatura systems support biometric verification methods, adding an additional layer of security by using unique physical characteristics as an access credential.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

By implementing these encryption standards and secure hardware features, Armatura assures a comprehensive security strategy that protects against both digital and physical threats. Our system's resilience is further enhanced by rigorous key management protocols and sophisticated access control mechanisms, ensuring that our clients' data remains secure in an increasingly complex threat landscape.

## Network Security

Armatura's Access Control System prioritizes network security as a critical element in safeguarding data across all points of communication. Our comprehensive network security strategy employs state-of-the-art technologies and best practices to mitigate risks and defend against unauthorized access and cyber threats.

**Secure Network Architecture**

- Segmented Network: We implement network segmentation to create discrete zones for system components, minimizing the attack surface and containing potential breaches.
- Demilitarized Zone (DMZ): A DMZ is utilized to separate the internal network from public internet access, offering an additional security layer for exposed services.
- Least Privilege Access: Network access follows the principle of least privilege, ensuring that users and systems have only the permissions essential for their roles.

**Wireless Security**

- Protected Wireless Communications: We employ stringent wireless protocols and encryption standards to safeguard wireless communications from unauthorized interception and access.

**802.1X Support**

- Network Access Control: Armatura Controllers and Standalone Terminals support the 802.1X authentication standard, providing a robust network access control mechanism that enhances the security of network entry points by requiring authentication credentials for devices attempting to connect to the network.

**Regular Network Testing**

- Penetration Testing and Vulnerability Assessments: Through regular testing, we identify and address potential vulnerabilities to maintain the integrity of the network infrastructure.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

**Monitoring and Response**

- Continuous Monitoring: Our systems are under constant surveillance for signs of unusual or unauthorized activity that could be indicative of a security incident.
- Automated Response Mechanisms: The ability to automatically respond to certain security events is built into Armatura's systems, enabling prompt action to mitigate potential threats.

The integration of these network security protocols ensures comprehensive protection throughout the Armatura Access Control System. By safeguarding every network layer, from individual endpoints to the broader infrastructure, Armatura delivers a secure network environment that stands vigilant against a spectrum of cyber threats.

## Biometrics Security

In the realm of access control, the use of biometric systems is on the rise due to their enhanced security and user-specific identification capabilities. Armatura's biometric technologies are at the forefront of this advancement, offering state-of-the-art, touchless identification methods that prioritize user privacy and data security.

**Armatura's Proprietary Biometric Technologies**

- **Touchless Palm Recognition:** Armatura has developed a proprietary touchless palm recognition technology that provides a secure and hygienic solution for identity verification. This system uses advanced computer vision technology to capture and analyses palm features without the need for physical contact.
- **Touchless Face Recognition:** Alongside palm recognition, our touchless face recognition technology utilizes sophisticated algorithms to identify individuals quickly and accurately, even in dynamic environments with varying lighting conditions.
- **Fingerprint Recognition Technology:** Armatura's fingerprint recognition technology remains a cornerstone of our biometric capabilities, providing reliable and precise user identification through detailed analysis of fingerprint patterns.

**Advanced Algorithm Foundations**

- Cutting-Edge Technologies: The foundation of all Armatura biometric algorithms is a combination of advanced **computer vision technology, deep learning, and multi-layer neural networks, alongside infrared scanning**, to ensure the utmost accuracy in biometric recognition.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

**Privacy and Data Security**

- **Biometric Template Protection:** To ensure the privacy and security of users, our biometric algorithms generate and use biometric templates rather than raw photos. These templates are an abstract representation of the user's unique biometric features, which **are mathematically transformed, making them irreversible and impossible to reconstruct into the original image**.
- **AES256 Encryption:** All biometric templates are safeguarded with AES256 encryption, one of the most robust encryption standards available, to prevent unauthorized access or interception of sensitive biometric data.

**Anti-Spoofing Measures**

- **Software-Level Protection:** Armatura's biometrics algorithms are equipped with sophisticated anti-spoofing functions at the software level. The algorithms analyze the characteristics of the biometric object in relation to the background and other entities within the capture frame to detect and prevent spoof attempts.
- **Hardware-Level Protection:** Our modules and standalone terminals are equipped with embedded infrared (IR) sensors that perform **liveness detection**. These sensors are crucial in ensuring that the biometric data captured is from a live subject, not a photograph or a replica.
- **Multi-Layer Neural Network**: The algorithm employs a multi-layer neural network to detect and extract unique palm print features. It also evaluates the liveliness of the subject to ensure authenticity and cross-references the captured biometric data with stored templates to confirm identity with high precision and security.

Armatura's innovation in biometric technology demonstrates our commitment to leading the security industry with solutions that are not only advanced in terms of technology but also unwavering in the protection of user privacy and data security. By integrating these sophisticated biometric systems into our access control solutions, we offer our clients an unparalleled level of security that is designed to meet the challenges of today and adapt to the threats of tomorrow.

## Mobile Credential Security

Armatura's Access Control System ensures robust mobile credential security through a sophisticated, layered strategy that prioritizes the protection of user data and access permissions. This strategy is anchored by our Cloud Platform, the Armatura Cloud Management System (ACMS), which is deployed on AWS Cloud, leveraging its secure and resilient infrastructure.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

**Cloud-Based Credential Management**

- Armatura Cloud Management System (ACMS): ACMS serves as the central command for mobile credential management, seamlessly integrated with "Armatura One" access control management systems. This setup offers a scalable and flexible solution that aligns with real-time credentialing needs.

**AWS Cloud Security Compliance**

- AWS Deployment: ACMS is hosted on AWS Cloud, adhering to all AWS security best practices and procedures. This ensures that the cloud infrastructure benefits from AWS's robust security measures, including network firewalls, encryption in transit, and identity and access management controls.

**Secure Communication Protocols**

- TLS-Protected Communication: The secure transmission of data between ACMS and "Armatura One" is guaranteed through TCP/IP communication protocols, safeguarded by TLS 1.2 encryption, which secures data against potential cyber threats.

**Offline Operation Capability**

- Armatura ID Mobile App: The Armatura ID Mobile App requires minimal interaction with ACMS, limiting communication mainly to the initial account activation phase. Post-activation, the mobile credentials are designed to work effectively in offline mode, enhancing accessibility and dependability.

**Diverse Operational Modes:**

Armatura offers three secure modes of mobile credential operation:

- **Card Mode:** Utilizes BLE or NFC for communication between the user's mobile device and the access control hardware, with AES256 encryption securing the data exchange.
- **Remote Mode:** Facilitates BLE-based interactions between mobile devices and access control hardware, also protected by AES256 encryption.
- **QR Code Mode:** Features a robust encryption framework with dynamically generated, encrypted QR codes using TOTP algorithms, refreshed every few seconds and secured with AES256 encryption, akin to financial industry standards.

**Initial Activation and Encryption**

- RSA4096 for Key Exchange: During the initial phase of account activation, the Armatura ID mobile app employs the RSA4096 encryption standard for key exchange with ACMS, laying a secure groundwork for all future communications.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

- AES256 for Continued Security: Post-activation communications between the mobile app and access control devices such as Smart Readers or Standalone Terminals are encrypted with AES256, ensuring the security of data in transit.

By deploying ACMS on the AWS cloud and adhering to its comprehensive security measures, Armatura guarantees that our cloud infrastructure is as robust as our on-premises security solutions. Our commitment to security is evident in every aspect of mobile credential management, from initial deployment and activation to daily operation and user access management.

## Compliance Standards

Armatura's Access Control System is designed to uphold the highest levels of compliance with international and industry-specific standards, reflecting our unwavering commitment to security and quality. Our adherence to these standards ensures that we deliver a secure, reliable, and compliant access control solution to our clients.

### Industry Compliance

- **ISO Standards:** Our systems are crafted in line with prestigious industry benchmarks including ISO/IEC 27001 for information security management, ISO/IEC 27701 for privacy information management, and ISO/IEC 27017 for securing cloud environments.
- **BS EN 60839-11-1:2013:** Compliance with BS EN 60839-11-1:2013 is integral to our operation, as it sets forth the necessary electronic access control operational requirements to safeguard against unauthorized access.
- **CMMI Level 5:** Armatura has achieved the Capability Maturity Model Integration (CMMI) Level 5 rating, which signifies our dedication to continuous improvement and the highest level of process maturity in providing quality services.

### Data Protection Regulations

- **GDPR:** Our systems are engineered with the GDPR in mind, ensuring the protection and confidentiality of personal data for EU citizens.
- **AWS Cloud Compliance:** The ACMS within AWS Cloud adheres to AWS's stringent security practices and complies with a broad array of privacy and security standards, echoing our commitment to maintaining secure cloud infrastructure.

### Regular Audits and Assessments

- Security Audits: To ensure compliance and to identify potential vulnerabilities, Armatura conducts regular security audits, a practice that helps us to maintain and enhance our security measures.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

- Vulnerability Assessments: We perform thorough vulnerability assessments aimed at detecting and mitigating security weaknesses, thereby strengthening our defense against evolving cyber threats.

**Training and Awareness**

- Employee Training: Our team receives continuous training in compliance standards and data protection practices, an approach that underscores the importance of human factors in maintaining security.
- Client Education: Armatura believes in empowering clients with knowledge, offering them insights into the compliance aspects of our access control systems and their contribution to overall system security.

By sustaining these rigorous compliance standards and achieving CMMI Level 5, Armatura ensures not only legal compliance but also operational excellence. This comprehensive adherence to standards builds a foundation of trust with our clients, assuring them that their access control system is backed by a commitment to quality, security, and continuous improvement.

## Physical Security

The Armatura Access Control System is designed with a strong focus on physical security to ensure that the hardware components are safeguarded against both digital and environmental threats.

**Multi-tech RFID Readers and Enrollers:**

- **IP68 Certification:** Our RFID readers and enrollers are certified up to IP68 standards, offering full protection against ingress of dust and the effects of immersion in water, ensuring functionality in all weather conditions.
- **IK10 Vandal Proof**: The devices are also up to IK10 rated, indicating the highest level of protection against vandalism, resistant to impact and tampering.
- **Safety and Regulatory Compliance:** These components have successfully passed **CE, FCC, and UL294 standards**, which speak to their safety, reliability, and quality.
- **Fire Resistance:** Built with **UL94-V0 fire resistance materials**, our readers and enrollers are designed to retard the spread of fire, providing an additional layer of safety.

**Biometric Standalone Terminals:**

- **IP66 Rating:** The terminals are IP66 rated, protecting against heavy seas or powerful jets of water, as well as dust ingress, making them suitable for both indoor and outdoor environments.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

- **IK07 Vandal Resistant:** With up to IK07 rating, they are safeguarded against a high level of impact and are robust enough to withstand physical tampering.
- **Compliance with Standards:** These terminals have also passed **CE, FCC, and UL294 standards**, ensuring they meet international safety and performance requirements.

**Controllers:**

- **Safety Compliance:** Armatura controllers conform to **CE, FCC, and UL294 standards**, meeting strict safety and operational guidelines.
- **Fire-Resistant Build:** Constructed from **UL94-V0 fire resistance materials**, these controllers contribute to the overall safety of the environment by mitigating fire propagation risks.

**IO Expansion Boards:**

- **Regulatory Conformance:** Our IO expansion boards are compliant with **CE, FCC, and UL294 standards**, demonstrating our commitment to maintaining high safety and quality standards across all components.

**Physical Security Enhancements:**

- **EAL6+ Rated Crypto Chips:** For secure cryptographic operations and to prevent physical tampering, our devices are equipped with EAL6+ rated crypto chips.
- **Supervised Inputs:** Controllers and IO expansion boards feature supervised inputs to detect and report any unauthorized attempts to interfere with system sensors and alarms.
- **Magnetic Tamper Systems:** Readers and standalone terminals are outfitted with magnetic tamper systems that alert the system to any unauthorized physical tampering attempts.
- **Anti-DOP (Data-Oriented Programming) attacks Design:** Our hardware incorporates an anti-DOP design to prevent attacks that manipulate the memory layout or access patterns, ensuring the integrity of processed and stored data.

Armatura's commitment to physical security is evident in the resilience of our hardware, the rigorous standards they meet, and the advanced features they boast. We ensure that our clients' security infrastructure is not only secure from intrusion but also reliable in the face of environmental challenges and resistant to physical tampering.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

## Incident Response and Management

In the event of a security incident, the ability to respond swiftly and effectively is crucial. Armatura's Incident Response and Management protocols are designed to minimize impact and restore operations as quickly as possible.

**Incident Detection**

- Proactive Monitoring: Armatura's systems are continuously monitored for signs of unusual activity. This proactive approach ensures that potential incidents are detected early, allowing for immediate response.
- Alert Systems: When an incident is detected, our alert systems are designed to notify the appropriate personnel instantly. This enables a rapid initiation of our incident response procedures.

**Incident Assessment**

- Initial Evaluation: Upon detection of a potential incident, our team conducts an initial evaluation to determine the scope and impact. This assessment is critical in guiding the subsequent steps of the response.
- Prioritization: Incidents are prioritized based on their severity, impact on operations, and potential risk to data integrity and privacy. This ensures that resources are allocated effectively to address the most critical issues first.

**Incident Containment**

- Immediate Action: Quick containment actions are taken to prevent further spread or escalation of the incident. This may involve isolating affected systems, revoking access, or implementing additional security controls.
- Communication: Clear and timely communication is maintained with all stakeholders, including management, IT staff, and, if necessary, affected customers.

**Incident Eradication**

- Root Cause Analysis: A thorough investigation is conducted to identify the root cause of the incident. Understanding the underlying vulnerabilities or threats is key to preventing recurrence.
- Remediation: Once the root cause is identified, Armatura's team works to eradicate the threat. This may involve patching vulnerabilities, updating policies, or enhancing security measures.

**Recovery**

- System Restoration: After the threat is neutralized, efforts focus on safely restoring affected systems and services to full functionality.
- Data Recovery: Utilizing our robust backup and recovery solutions, data affected by the incident is restored from the most recent secure backup.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

**Lessons Learned**

- Post-Incident Review: Following the resolution of an incident, a comprehensive review is conducted to assess the response effectiveness and identify areas for improvement.
- Policy Update: The insights gained from the incident are used to refine our incident response policies and procedures, ensuring a more effective response to any future incidents.
- Training: Staff training is updated to include new protocols and information derived from the incident review, bolstering the overall security posture.

Armatura's Incident Response and Management protocols are integral to our security strategy, ensuring that we can handle incidents with the urgency and effectiveness required to protect our clients' interests and maintain their trust.

## Continuous Improvement

Armatura is dedicated to the principle of continuous improvement in all aspects of our Access Control System. We recognize that the security landscape is ever-changing, and staying ahead requires an ongoing commitment to enhancement and evolution.

**Feedback Loops**

- User Feedback: Regular feedback from our clients is a cornerstone of our improvement process. We actively seek and incorporate this input to refine our products and services.
- Performance Metrics: By analyzing performance data, we identify areas that can be optimized, ensuring our systems not only meet but exceed expectations.

**Technology Upgrades**

- Hardware and Software Updates: We continuously monitor advancements in technology to upgrade our hardware and software solutions. This ensures that our systems leverage the latest security features and performance enhancements.
- Integration of New Features: As new threats emerge, we respond by integrating cutting-edge features and capabilities into our system to bolster security and improve functionality.

**Training and Development**

- Employee Training: Our staff undergo regular training to stay updated on the latest industry trends, technologies, and security practices.
- Professional Development: We invest in the professional development of our team, encouraging certifications and advanced education in security and technology fields.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

**Process Optimization**

- Efficiency Reviews: Our internal processes are regularly reviewed for efficiency and effectiveness, enabling us to streamline operations and reduce the potential for errors.
- Quality Assurance: We implement rigorous quality assurance practices to ensure that every aspect of our system, from software coding to hardware manufacturing, meets the highest standards.

**Security Research and Collaboration**

- Threat Intelligence Sharing: Armatura collaborates with other industry leaders and participates in threat intelligence sharing initiatives. By understanding the broader threat landscape, we can proactively address potential vulnerabilities.
- Research Partnerships: We engage in partnerships with academic and research institutions to stay at the forefront of security research and emerging technologies.

**Regulatory Compliance Updates**

- Adherence to Standards: We continually monitor changes in regulatory standards and compliance requirements to ensure that our systems are up to date with the latest legal mandates.

- Policy Adjustments: As standards evolve, we adjust our policies and protocols to maintain compliance and to lead the industry in best practices.

Armatura's commitment to continuous improvement means that our Access Control System is a dynamic and evolving solution, consistently strengthened by new insights, technologies, and practices. Our proactive approach ensures that we are prepared to meet the challenges of the future, providing our clients with a secure, reliable, and forward-looking access control solution.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

## Conclusion

In the rapidly evolving landscape of security technology, Armatura's Access Control System stands as a beacon of reliability, innovation, and comprehensive protection. Our multi-faceted approach to security — encompassing robust physical defences, advanced cyber protection, rigorous compliance standards, and a strategic incident response framework — ensures that our clients' facilities and data remain secure against both current and emerging threats. The integration of high-assurance crypto chips, vigilant network security measures, and resilient hardware design demonstrates our unwavering commitment to safeguarding access points and sensitive information. Our systems are not only designed to resist environmental challenges and physical tampering but are also constantly updated to stay ahead of the sophisticated tactics employed by modern adversaries.

Through regular audits, continuous monitoring, and adherence to international standards, we maintain a posture of rigorous compliance and operational excellence. Our dedication to continuous improvement is reflected in every aspect of our operation, from proactive threat intelligence sharing and research partnerships to ongoing employee training and technology upgrades.

Armatura's Access Control System is more than a security solution; it's a partnership with our clients, offering them peace of mind and the freedom to focus on their core business objectives, knowing their security is in expert hands. As we look to the future, Armatura will continue to pioneer advancements in access control technology, driving the industry forward and setting new benchmarks for safety and reliability.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

## References


- International Organization for Standardization (ISO). (n.d.). ISO/IEC 27001 Information security management. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html
- International Organization for Standardization (ISO). (n.d.). ISO/IEC 27701 Privacy information management. [Online]. Available: https://www.iso.org/isoiec-27701-privacy-information.html
- International Organization for Standardization (ISO). (n.d.). ISO/IEC 27017 Cloud security. [Online]. Available: https://www.iso.org/isoiec-27017-cloud-security.html
- British Standards Institution (BSI). (2013). BS EN 60839-11-1:2013 Alarm systems. Part 11-1: Electronic access control systems. System and components requirements. [Online]. Available: https://shop.bsigroup.com/ProductDetail?pid=000000000030320089
- Underwriters Laboratories (UL). (n.d.). UL 294 Standard for Access Control System Units. [Online]. Available: https://standardscatalog.ul.com/standards/en/standard_294_5
- Federal Communications Commission (FCC). (n.d.). Equipment Authorization - Radio Frequency Devices. [Online]. Available: https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization
- European Union Agency for Network and Information Security (ENISA). (n.d.). Threat Landscape and Good Practice Guide for Internet Infrastructure. [Online]. Available: https://www.enisa.europa.eu/publications/threat-landscape-for-internet-infrastructure
- Fire Safety Advice Centre. (n.d.). Understanding the UL94-V0 Fire Resistance Rating. [Online]. Available: https://www.firesafetyadvicecentre.org.uk/ul94-v0-rating.html
- Security Industry Association (SIA). (n.d.). Vandal Resistance - IK10 Rating. [Online]. Available: https://www.securityindustry.org/report/ik10-vandal-resistance-rating/
- International Electrotechnical Commission (IEC). (n.d.). Degrees of protection provided by enclosures (IP Code). [Online]. Available: https://www.iec.ch/ip-ratings




Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

## Glossary

The glossary section of a whitepaper serves to clarify terminology and acronyms that are used throughout the document. It ensures that readers from various backgrounds can understand the specialized or technical language pertaining to the subject matter. Here is an example of what a glossary in the Armatura whitepaper might include:

- Access Control System (ACS): A system that grants or denies access to resources within a computing environment by identifying entities and assigning user rights and restrictions.
- Biometric Terminals: Devices that use unique biological traits, such as fingerprints or facial recognition, for determining and verifying individual identity.
- Crypto Chips (EAL6+ Rated): Hardware chips evaluated to an EAL6+ (Evaluation Assurance Level 6+) standard that perform secure cryptographic operations and are resistant to physical tampering.
- Disaster Recovery Plan (DRP): A strategic plan for how an organization will recover and restore its IT operations following a disaster.
- Firewall: A network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies.
- High Availability (HA): Systems or components that are continuously operational for a desirably long length of time.
- Intrusion Detection System (IDS): A device or software application that monitors network or system activities for malicious activities or policy violations.
- IP Rating (Ingress Protection Rating): A two-digit grading system defined by international standard IEC 60529 which rates the degree of protection provided against the intrusion of solid objects (including body parts like hands and fingers), dust, accidental contact, and water in electrical enclosures.
- IK Rating (Impact Protection Rating): A code that classifies the degree of protection provided by enclosures for electrical equipment against external mechanical impacts, as defined by international standard IEC 62262.
- Load Balancing: The process of distributing network traffic across multiple servers to ensure no single server becomes overwhelmed, optimizing resource use, maximizing throughput, minimizing response time, and avoiding overload.
- Magnetic Tamper System: A security feature in devices that detects and signals an alert when a tamper attempt is made.
- Supervised Input: An input on a security device that is monitored for specific conditions, such as being shorted or cut, to provide an indication of tampering or fault conditions.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024

- UL94-V0 Fire Resistance: A fire resistance standard that indicates that the material will stop burning within 10 seconds on a vertical specimen; drips of particles allowed as long as they are not inflamed.
- VLAN (Virtual Local Area Network): A logical subgroup within a local area network that is created via software rather than hardware, which can group a set of devices across multiple physical LAN segments.
- VPN (Virtual Private Network): A secured private network connection built on top of a public network, such as the Internet, to secure and encrypt communication.



Address: 190 Bluegrass Valley Parkway Alpharetta, GA 30005
Email: sales@armatura.us

Version 1.0
FEB 20, 2024