ArrowSphere Security Posture
Secure Cloud Aggregation and Management Platform

November 2021
Table of Contents

Introduction
Information Security Management System
Physical Security
Account Management
Platform Security Controls
Data Security and Privacy
Email Security
Logging and Monitoring
Security Operation Center and Incident Response
Secure Vendor Integration
Security Awareness Training
Security Risk Management
Business Continuity and Disaster Recovery
Backup and Recovery
ArrowSphere

The cloud delivery and management platform for powering digital growth.

Disclaimer
This document is intended for ArrowSphere partners, ArrowSphere employees and prospective customers. Approved for limited release only to this audience.
ArrowSphere

ArrowSphere is a cloud aggregation and management platform offered by Arrow Electronics Inc. to partners, which utilize it to act as a reseller by using standard APIs provided by third-party vendors to offer subscriptions to their services.

Arrow Electronics Inc. has defined a set of corporate rules and policies which are applicable to the ArrowSphere Platform with overall goal to protect customer data.

This document describes a high-level summary of security controls, which are aligned and certified to ISO 27001 requirements, to protect ArrowSphere web application, its infrastructure, data, and accounts.
Information Security Management System

ISO 27001:2013 Certified

Information Security Management System covering the ArrowSphere Platform is ISO27001:2013 certified.

Arrow Electronics Security Program

Arrow Electronics Inc. maintains a written information security program consisting of policies, standards, procedures, and guidelines which establish operational security controls to govern security for processing, storage, and transmission of customer data. Arrow's security program is developed using best practices based on industry standard frameworks (NIST CSF, NIST 800-171, ISO 27001, CIS, and SANS CSC) to protect customers’ data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Arrow periodically tests the effectiveness of its security program via independent internal and external assessments.

Arrow’s information security organization is led by a Chief Security Officer with the following security pillars: IT Risk & Governance, Security Operations, Security Architecture, Security Training & Awareness, Business Continuity, Fraud and Physical Security. Arrow’s operational security staff hold numerous cybersecurity degrees and industry recognized certifications.
Arrow has implemented accepted industry standards to prevent unauthorized persons from gaining access to offices and data centers where customer data may be processed.

- High-definition/IP Network Video Cameras/Monitors
- Integrated Surveillance Networking
- Leading Operating Systems/Video Management Software
- Access controls
- Surveillance Services
ArrowSphere platform security includes Identity and Access Management controls to protect the confidentiality, integrity, and availability of user accounts of our partners. Below a high-level summary of the controls available on our platform:

- Multi-Factor Authentication on ArrowSphere web application and infrastructure.
- Single Sign On (SSO) to ArrowSphere web application.
- Enforcement of Password complexity.
- Role-Based Access Control (RBAC) with a formal end-user onboarding process.
ArrowSphere web application, its source code and infrastructure are continually assessed, monitored, and enhanced to detect and fix vulnerabilities that could be exploited by attackers. Risks are identified, managed, prioritized, and monitored.

- ArrowSphere platform is monitored 24x7 by Arrow’s Security Operation Center to identify possible attacks and manage incidents if required.
- Internal web application and API assessments.
- Regular and on-demand penetration testing.
- Dynamic and Static (DAST and SAST) security assessments.
- Recurring database risk reviews.
- Internal security audits.
- Continuous vulnerability management and patching process on production and non-production environments.
- Denial of Service (DDOS) and layer 7 protection in place to protect website and APIs.
- Protection and access control to source code repository.
- CI/CD software development lifecycle utilizing secure development principles with security impact assessments for platform changes.
ArrowSphere is GDPR compliant and has controls to guarantee the privacy of the data of our users. Encryption is being used to protect the data.

- ArrowSphere data is hosted in a SOC 2 and ISO 27001 certified providers.
- Encryption controls implemented for at-rest, in use, and in-transit data.
- Data hosted in Europe and compliant with GDPR requirements.
- Data anonymization features implemented as per GDPR.
Arrow utilizes commercially available email security gateway systems to scan both inbound and outbound email for viruses and other malicious content (links, etc.).

There are strict anti-phishing controls through Arrow cloud email & collaboration platform including commercial anti-phishing protections.

Data Loss Protection (DLP) Policies are configured to detect and alert on sensitive data exfiltration through email.

ArrowSphere platform emails are sent securely, encrypted, and validated using DKIM, SPF, and DMARC. Access to the ArrowSphere emails platforms is controlled by an enterprise Identity and Access Management (IAM) solution with security policies based on security best practices.
Audit logs and events are collected from the infrastructure environments which contain sensitive data using a Security Information and Event Management platform (SIEM) to ensure there is a non-repudiation trail regarding system events, mitigation of log tampering opportunities and to provide the ability to conduct correlation and forensics to detect and/or research anomalous activity.

The SIEM platform is configured with advanced analytics that apply threat intelligence with account and sensitive data access attempts as well as exfiltration signatures. Access to the centralized logging system is restricted to select members of the Arrow Security Operations Team.
Arrow has a 24/7 managed Security Operations Center (SOC) that provides monitoring, detections, and response services globally to handle Level 1, 2 & 3 security events. Arrow’s SOC utilizes Security Operation Automation and Response (SOAR) for faster resolution times on phishing attacks and potentially compromised accounts.

Arrow’s SOC also maintains an ever-evolving Incident Response Program which includes advanced forensic capabilities, global readiness plans and exercises, matured KPIs and a third-party retainer for global incident response within 72 hours. This also includes a threat hunting program applicable to both internal and third-party services.
Arrow monitors, analyzes, responds to, and reports security incidents in a timely manner in accordance with Arrow’s standard operating procedures. Arrow’s Security Operations team escalates and engages teams as necessary to address an incident.

Breach notification: Unless notification is delayed by the actions or demands of a law enforcement agency, Arrow will report to the Customer and relevant Data Protection Agency (DPA), any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, customer data (a “Breach”) in accordance with applicable legal requirements following determination by Arrow that a breach has occurred.
Arrow maintains a vendor risk management program that assesses all vendors who access, store, process, or transmit customer data for appropriate security and IT operational controls along with business disciplines. The Arrow's IT Risk team works closely with Arrow's Global Sourcing and Procurement team to ensure assessments are conducted up front for all contracts that have a known element of data transfer or access to Arrow systems. External cybersecurity companies are also used in delivering an objective rating score during the vendor IT risk assessment process. Applicable contractual language regarding legal compliance, onward transfer, and audit rights is also included when applicable. In addition, high risk and enterprise critical vendors are continually monitored.
Arrow maintains a security awareness program that includes appropriate and relevant training of Arrow’s personnel on the security program, current threats, and vulnerabilities facing Arrow and the industry. Training is conducted in the Human Resources Information System (HRIS) during new hire onboarding and, periodically throughout employment at Arrow.
Arrow has implemented an IT Risk Program on the industry standard NIST CSF to evaluate security risks related to the confidentiality, integrity, and availability. Then, based on such evaluation, implement appropriate technical and organizational measures to ensure a level of security which is appropriate to the risk of the specific personal data type and purposes being processed by Arrow which may include, but not limited to:

- The pseudonymization and encryption of personal data where applicable and using systems capable of providing these features.
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- The ability to restore the availability and access of customer’s data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.
Arrow Electronics Inc. has formally documented and implemented Business Continuity and Disaster Recovery plans for the ArrowSphere Platform. These plans are tested on a regular basis and improvements are made as necessary.
ArrowSphere has a high availability architecture with a designated disaster recovery site, which is distributed across multiple geographic locations in Europe. This architecture allows ArrowSphere to mitigate potential customer impact from outages.
Infrastructure configurations and relevant data are continually backed up for recovery purposes. Backups are monitored and tested on a regular basis.
ArrowSphere values the security and privacy of your data and has made significant investments in people, processes and technology to instill confidence and trust in our customers and partners.

Please direct any questions you might have on ArrowSphere's offerings or security via [https://xsp.arrow.com/index.php/site/contact](https://xsp.arrow.com/index.php/site/contact)
Thank You