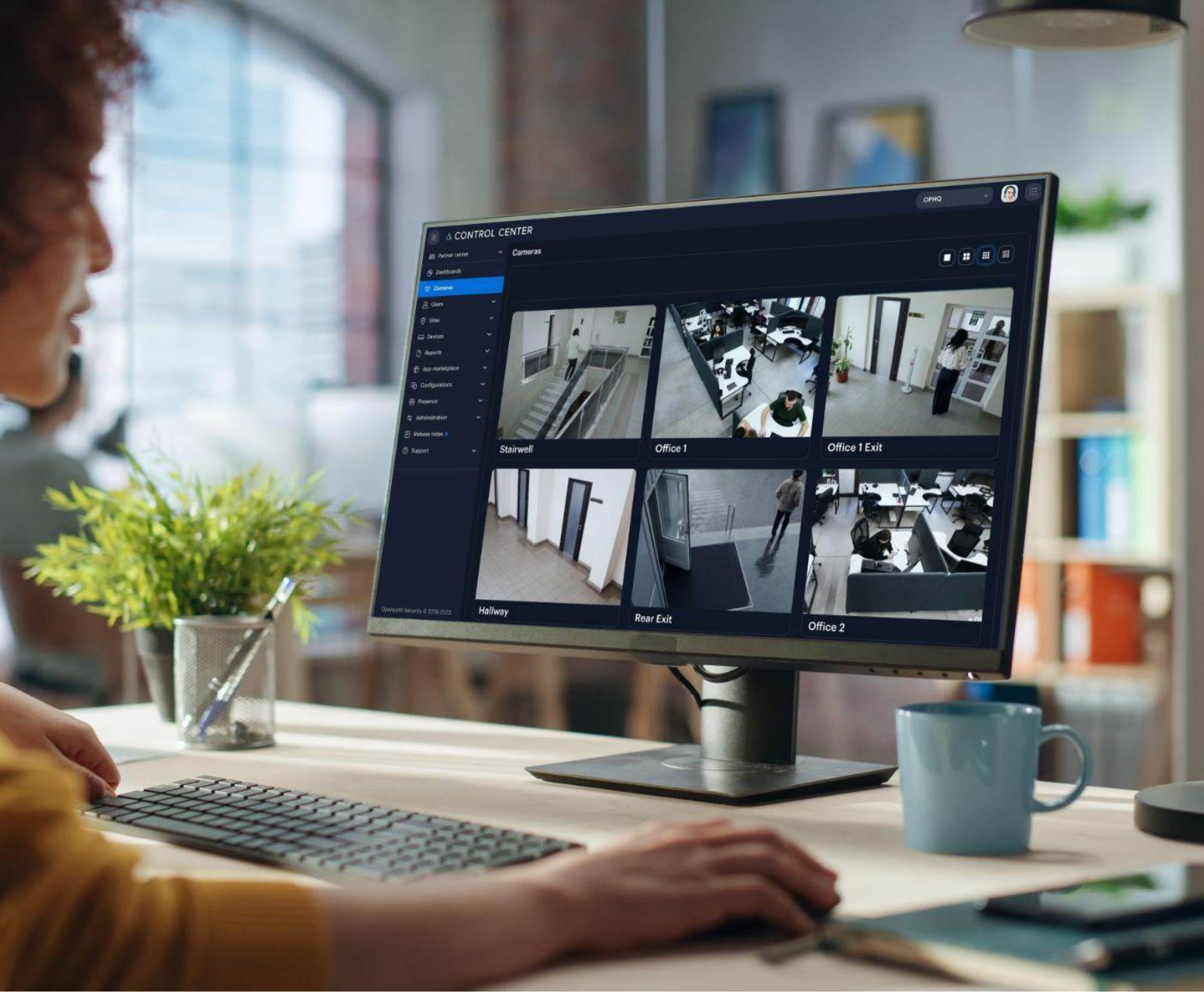


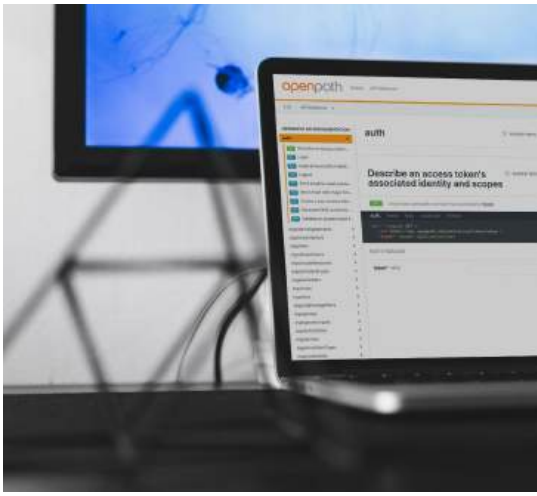
AVIGILON™

Openpath Access Control System Physical & Cyber Security Overview

MOTOROLA SOLUTIONS

Openpath Access Control System Physical & Cyber Security Overview

Openpath System Architecture



Openpath understands security is challenging and that new systems are often constructed on top of imperfect, existing infrastructure that is difficult to change. With this in mind, we've built our architecture with the assumption that our technology will be deployed into hostile network environments and locations with pre-existing threats. We expect that all communication channels will be unreliable and insecure, vulnerable to both passive and active attackers. Despite these factors, we've designed our system to provide secure and reliable access and communication.

In a nutshell, we've built Openpath technology under the following assumptions:

- Communication channels are unreliable
  - Internet/cloud communication is not always available
  - Wiring (Wiegand/22-6, CAT5/6) may have interference or be low-bandwidth
  - WiFi is unreliable or may be non-existent
  - Bluetooth Low Energy (BLE) connections may be unreliable
  - Cellular data is unreliable or may not be available in some locations

- Communication channels are insecure
  - New attacks may compromise existing security premises, including which communication methods are resistant against attacks
  - Wiring (22-6, RS-485, CAT5/6), wireless protocols (BLE, WiFi, cellular), and Internet connectivity may have passive eavesdroppers monitoring all communication
  - All wiring, wireless protocols, and Internet connectivity may have active attackers intercepting, collecting, modifying, and interfering with all data and traffic
  - BLE implementations have security weaknesses or are missing critical security features

- Hardware is physically accessible and vulnerable to tampering
  - Openpath Readers are on the unsecured side of entries and attackers may attempt physical tampering, data exfiltration, and even alteration of hardware components
  - Openpath Cards may be accessed by attackers
  - Mobile devices may be shared by users

Anticipating these scenarios, our technology is designed to meet the following objectives:

- Multiple paths of communication should be available in case of unreliable or unavailable paths
- Authenticating information should be stored offline in case of Internet, wireless, or mobile network outages
- Private data should only be communicated with confidentiality (encryption)

- All private and trusted communication should provide integrity to protect against tampering
- All trusted or encrypted communication should be mutually authenticated (i.e. both sides verify the identity of the other) before sharing privileged data or requests, preventing passive eavesdropping or active man-in-the-middle attacks from succeeding
- In addition to strong cryptography, ephemeral (temporary) keys, validated against an associated long-term key, should be generated when possible and be used for short-term communication; ephemeral keys reduce the ciphertexts generated with long-term keys and reduce the threat of a temporary side-channel attack revealing master keys
- Physical hardware that is accessible by attackers should not store private keys or secret material; any physical tampering should not reveal confidential information
- Physical tampering of any wiring should not reveal confidential information
- Eavesdropping or recording of any communication should not allow any type of replay attack
- All authentication must be challenge-response based and require short timeouts
- All cryptographic algorithms must be open, well-vetted, and available for public scrutiny

This document further outlines some of our design considerations to satisfy the above requirements under many worst-case scenarios.

Overview

Openpath is a cloud-based physical access control solution consisting of on-premise hardware (Smart Readers and Smart Hubs), user credentials (mobile, key cards, fobs, and cloud keys), and a cloud-based administrative web portal (see Figure 1).

Most communication within the Openpath ecosystem is based on Public Key Infrastructure, is mutually authenticated, and is end-to-end encrypted via TLS 1.2. Openpath's architecture is designed to provide secure communication over insecure channels and to resist both passive and active

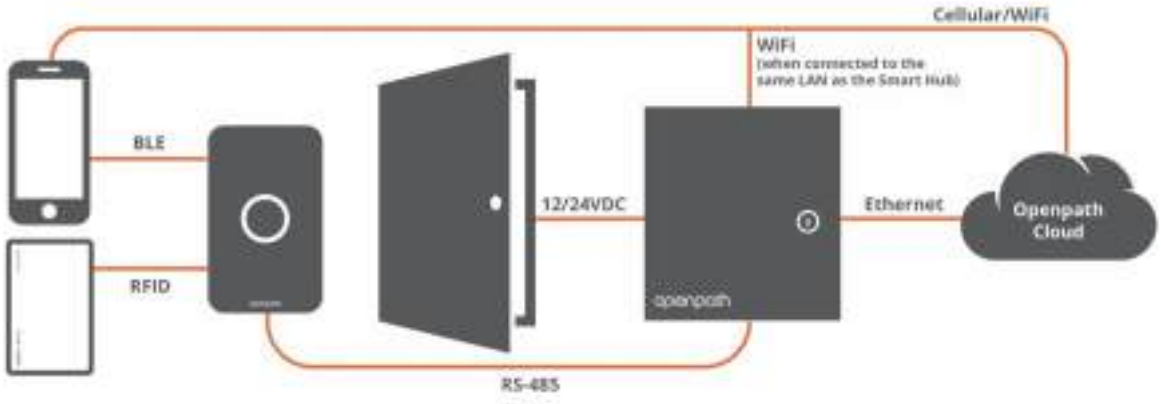


Figure 1: High Level Openpath System Architecture

Wiring

Openpath uses RS-485 wiring between Openpath Readers and Smart Hubs. Any mobile communication to a reader is end-to-end encrypted to the Smart Hub. Traditional access control systems use unencrypted Wiegand wiring that sends cleartext data across the wire, from the reader to the control panel. That being said, Openpath can use legacy Wiegand (22 gauge wire, often 22-6) wiring to run our RS-485 communication, making it easier to retrofit existing systems, without using the insecure Wiegand protocol.

TLS encryption

Openpath uses TLS 1.2, enforced with NSA Suite B Cryptography algorithms (preventing downgrade and similar attacks) for most communication. This is the same technology you use to log into online banking, but more secure as both sides authenticate each other, unlike a banking website where only the client authenticates the bank, not vice versa. We only allow well-vetted, open, and modern cryptographic algorithms for all communication.

Openpath is unique among cloud-based systems in regards to how we handle communications over BLE. Instead of relying solely on the security of BLE, which by itself is susceptible to downgrade and man-in-the-middle attacks, Openpath leverages TLS encryption on top of BLE. This ensures secure, encrypted communication despite attacks to Bluetooth's security features. Communication between the mobile device and Smart Hub is encrypted end-to-end, leaving wireless eavesdroppers unable to gain any useful details as all data is encrypted, and preventing active man-in-the-middle-attackers from performing successful attacks by the use of signed certificates.

Mobile security

Openpath mobile credentials are a more secure alternative to traditional PIN codes, key cards, and fobs. PIN codes can be shared, and key cards and fobs lost, stolen, or potentially cloned. Our mobile credentials support strong cryptography and allow additional security features such as multi-factor (MFA) and biometric authentication. While many cloud-based access control systems offer mobile credentials, Openpath differs in the level of effort we put into making our mobile solution secure: multiple layers of security, well-vetted cryptographic technologies, and third-party security auditing and penetration testing.

Setting up a mobile credential

When a user sets up a mobile credential for the first time, they receive a temporary, one-time-use, digitally signed token in their email. By clicking the token, their mobile device generates a public/private key pair for authentication. The private key never leaves the mobile device. To securely assign the user's email address to their certificate, the phone sends the signed token and certificate signing request (CSR) to Openpath. We then sign the certificate with information from the token and return it to the mobile device. When the user attempts to authenticate in the future, their

device digitally signs data using their private key which authenticates them to their original email address.

A user can regenerate this key pair by requesting a new signed token from Openpath by email and then reprovisioning the mobile app with that token. This ties the authenticity of the user to their email address, which is how Openpath uniquely identifies users.

Using a mobile credential

When a user presents a mobile credential to an Openpath Smart Reader, the Openpath app may send up to three signals simultaneously over BLE, WiFi, and cellular. This is our patented triple unlock technology and it ensures that the fastest signal is the one that is used to unlock your entry. All signals are end-to-end encrypted between the mobile device and Smart Hub, as is all communication between the Smart Hub and Openpath Cloud.

BLE

The mobile device sends the BLE signal directly to the reader with no requirement for Internet or network connectivity. The reader then sends the communication over RS-485 to the Smart Hub. This communication between the mobile device, reader, and Smart Hub is end-to-end encrypted where the reader acts as a proxy between the mobile device and Smart Hub and is unable to decrypt any communication.

WiFi

If the mobile device is on the same network as the Smart Hub, the mobile device creates an encrypted connection directly to the Smart Hub over WiFi. If the mobile device is on a different network, it will create an encrypted connection over WiFi to the Openpath Cloud, which will then communicate with the Smart Hub.

Cellular

If the mobile device has a cellular data connection, it will create an encrypted connection by first connecting to the Openpath Cloud, which will then communicate with the Smart Hub.

Key card security

Openpath uses MIFARE DESFire EV3 key cards for our Openpath Cards, but our readers also support DESFire EV2 and EV1. Openpath Cards support mutual authentication and use AES for encryption. We use unique cryptographic keys per card that are generated by the Smart Hub. At the time of writing, there are no publicly known attacks against DESFire EV3. If somehow a key were ever extracted for a card, we additionally use asymmetric cryptography and store signed data within each card with alternative keys, validating that the card was issued by Openpath after the card is authenticated with the (potentially compromised) key.

Most competitive access control systems do not use encrypted cards by default. Systems that do support cryptographic cards often use the same key for each card, meaning if one is compromised then all other cards in the system are at risk. Additionally, if a key is compromised on the Openpath system, an attacker would need physical access to the card to obtain the embedded signed data to emulate the card, whereas traditional systems don't perform any other validation.

The communication between the Smart Hub and Openpath Card is also end-to-end encrypted and mutually authenticated. Unlike traditional badge readers, the Openpath Smart Reader has no knowledge of encrypted keys or other secret material. Instead, the Smart Hub and Openpath Card negotiate a temporary session key to communicate. The session key is derived from both the Openpath Card and Smart Hub and both are randomized per session, as well as encrypted with the shared key unique to the card. The communication is designed to be resistant to passive (snooping) attacks, active (man-in-the-middle) attacks, and replay attacks.

Reader security

Openpath Smart Readers do not store credential data or any other secret material. This is critical as readers are installed on the unsecured side of the door and are often the weakest point in any access control system. Rather, our Smart Reader acts as a proxy, securely sending sensitive material over end-to-end encrypted communication to the Smart Hub, which is located in a secured network closet. Legacy systems often don't provide any cryptography on their readers. For readers that do use cryptography, they typically store keys on the reader itself, making it especially vulnerable to tampering. Storing this kind of information on the reader gives attackers the ability to extract cryptographic keys by simply having physical access to the reader. Additionally, traditional readers, whether they use encryption or not, typically use unencrypted Wiegand communication which can allow sniffing and replay attacks by simply tapping the wires on the back side of the reader.

Smart Hub security

Like our mobile credentials, each Smart Hub generates its own public/private key pair for authentication. The private key never leaves the Smart Hub. The Openpath Cloud signs the public key when provisioning the Smart Hub for the first time. It does this by generating and sending a signed token to the administrator provisioning the system through an authenticated and encrypted TLS session with the Openpath Cloud. The administrator sends this temporary, one-time-use signed token to the Smart Hub over the local network or BLE. The administrator then must demonstrate physical access to the hardware by pressing the Admin Button on the Smart Hub, which then sends the token along with its CSR to the Openpath Cloud over TLS. The Openpath Cloud signs the CSR with the Smart Hub identity in the token and returns it to the Smart Hub.

Offline capabilities

Our Smart Hubs support backup batteries ensuring that your system works in the event of power and Internet outages. All necessary credential data is stored locally on the Smart Hub to ensure proper operation at all times. Even if your mobile device has no WiFi or cell service, and even if the Smart Hub is offline, your mobile credentials and access control system continue to communicate encrypted over BLE.

Additionally, if changes to user permissions occur during the time that a Smart Hub is offline and unable to receive updates, the updates are sent by

Openpath vs other cloud-based systems

Openpath differs from other cloud-based access control systems in several ways:

- Our convenience of Touch to Unlock on the reader with no requirement to pull out or unlock your phone (unless required by the entry using Openpath MFA)
- Our enhanced TLS-over-BLE communication protocol
- Our Triple Unlock feature utilizing BLE, WiFi and cellular data simultaneously for fast authentication and reliability
- Our readers do not store secret data or keys
- Our mobile credentials are passwordless and tied to users' email
- Our key cards use modern cryptography and include the addition of signed data within each card, future-proofing against attacks on the card cryptography itself, which has traditionally been a weak point in access control systems

Openpath vs legacy systems

Openpath's security is a vast improvement over legacy access control systems:

- Mobile credentials provide greater security features like MFA and biometric authentication, unlike legacy key cards, fobs, and PIN codes
- Openpath uses cryptographic key cards, unlike legacy proximity cards that offer no encryption or integrity
- Openpath wired communication is encrypted end-to-end, rather than using the unencrypted and unauthenticated Wiegand protocol
- Our cloud software updates automatically in real time to protect against security threats, unlike traditional onsite servers that require costly maintenance and a considerable time lag for critical updates

Openpath Cybersecurity

Openpath employs many security measures to ensure our system and customers' data are protected. These measures include items like mandatory multi-factor authentication, complex password requirements, enforced encryption of data in transit and at rest, strong and modern cryptographic protocols, daily internal vulnerability and network scanning, periodic third-party penetration testing, external security and compliance auditing (SOC2 Type II), environmental isolation, and the principle of least privilege, to name a few.

1. When it comes to customer data, we ensure that the customer is in control of their data and system. By default, our support team does not have the ability to control or unlock any customer systems, and customers have the capability to enable or disable our support team's ability to even have read access to their system. For example, this could be enabled temporarily to allow a representative to support the system or answer specific questions, and then disabled immediately after by the customer. Additionally, all changes performed from these accounts are stored in an immutable audit log and accessible by the customer.
2. Internally, we maintain a vulnerability management and information security program to test for and remediate any potential system vulnerabilities. As part of this program, the Security team performs recurring internal vulnerability and network scans in addition to endpoint antivirus and malware scanning tools.
3. In addition to internal scans, the Security and Technology teams engage objective third party companies to perform annual penetration testing over our system and products. Our team prioritizes any potential risks and works towards swift resolution of potential concerns while maintaining a high level of security.

AICPA SOC 2 Type II

In 2023, Openpath underwent a nine-month audit for SOC 2 Type II and may share the attestation report produced by Armanino, Openpath Security's Service Auditor, with a signed NDA.

Security Policies

Openpath Security Inc. by Motorola Solutions Inc. maintains security policies that are audited in conjunction with annual SOC 2 Type II. These policies follow our standard policy review process which includes, evaluation for updates, required policy owner sign-off, and annual policy testing. Motorola Solutions Inc. does not share internal policies but does attest to uphold and maintain these policies.

Information Security Policy

The Motorola Solutions Inc. InfoSec Policy, which has been adopted by Openpath, is designed to educate employees about information technology and security measures in use by the organization to keep information and personal data secure.

Disaster Recovery

Items covered in the policy are the following:

- Openpath Leadership is responsible for maintaining, updating, and testing the plan
- Notification list
- Disaster Recovery Objectives
- Non-Critical vs Critical Systems
- Notification Phase
- Recovery Phase
- Reconstitution Phase
- Forensics Phase
- Retrospective Phase
- Reenactment Phase
- RTO/RPO

Business Continuity Plan

Items covered in the policy are the following:

- Testing the plan
- Lessons Learned Report
- Business Impact Assessments (BIAs)
- Alternate Business Location
- Key Vendors- Communications/SSO, Infrastructure/AWS, Customer Support Ticketing, IP Phone System, Customer Billing, Domain Registrar
- Responsibility
- Insurance
- Disciplinary Action

Backup Policy

Openpath's Backup Policy describes how often service and customer data is backed up. All original (non-derived) customer data on infrastructure operated by Openpath should be backed up.

Openpath has the ability to completely restore and replace the production database cluster in the unlikely event that it becomes necessary. Openpath also has the ability to restore an earlier backup into a separate cluster in order to facilitate the examination of earlier data without completely restoring it into the production database. Backups are encrypted with AES-256 bit encryption and stored in AWS, which includes all logs, backups, and snapshots.

Acceptable Use Plan

Our customers trust us, and they expect us to protect the data and resources they've shared with us. Part of how we uphold that trust is through pre-established policies so we make the best decisions for our business and our customers in critical moments. This IS Policy should be read and acknowledged by everyone in the organization and a record kept of this, with updates as appropriate for every revision.

Asset Management Policy

This Asset Management Policy is designed to protect customers' data stored on endpoints, including laptops and mobile devices. It details how Openpath accounts for endpoint information technology assets (e.g. employee computers) and outlines what should be done if assets are lost, destroyed, or otherwise damaged.

Incident Response Plan

Openpath has an Incident Response Plan that offers guidance for the security team, employees, and incident responders who believe they have discovered or are responding to a security incident. The plan outlines the following:

- Escalation Process
- Classification of Severity and Prioritization
- Response Steps (including response time of 72 hours)
- Response Meeting Agenda
- Response Team Members
- Lessons Learned
- Disciplinary Action
- Responsibility

Change Management Policy

Openpath's Change Management Policy describes how and why changes to the Openpath system are proposed, reviewed, deployed, and managed. This policy covers all changes made to Openpath software, regardless of their size, scope, or potential impact.

Cryptography Policy

This policy document provides Openpath encryption standards and best practices to ensure that Openpath consistently follows industry standards for encryption and key management.

Data Classification, Deletion, and Protection Policy

The Openpath Data Management Policy covers data classification, data protection, and data deletion. Openpath employees must follow this policy. Contractors, consultants, partners, and any other external entities are also required to follow these policies. Generally, our policy refers to anyone we collaborate with or who acts on our behalf and may need access to Openpath data.

Privacy Policy

Please refer to the Openpath Privacy Policy.

Penetration testing

Openpath conducts annual and ongoing third-party penetration testing to detect and resolve potential security vulnerabilities or weaknesses.

Openpath Security Inc. by Motorola Solutions Inc. completed a full product and system penetration test including hardware, software, mobile, and cloud services with Tevora in 2023. For security purposes, we do not share penetration test results but will attest to the findings and our remediation plan. An executive summary is available, upon request.

Safety and Compliance

Openpath hardware is rigorously tested to comply with the required and relevant standards provided by national and international regulatory bodies, including the FCC, ISED, CE Directives, and more. In addition to complying with the necessary radiofrequency and electromagnetic limits, we also certify for UL294, IP65, and other safety and environmental standards to ensure quality and protection. For more information, please refer to the Openpath Compliance Webpage.

GDPR and CCPA

Openpath considers privacy and security its highest priorities, and we are committed to ensuring the protection of our customers' data, and providing transparency around our policies. Openpath is CCPA compliant. For more information about GDPR compliance, please refer to our International Data Transfers and GDPR Statement.

- UK Data Processing Addendum
- EU Data Processing Addendum

Data Residency

Openpath now offers to selectively store data in a server in the European Union which will help with strict data privacy laws. Note that this data residency is not designed to help meet any legal, regulatory, or compliance requirements.

For more information, please see below our Frequently Asked Questions to learn how Openpath can help increase your data privacy compliance.

Frequently Asked Questions

Compliance and certifications we help our customers meet

- PCI Requirements for Physical Security (Requirement 9), and Track and Monitor All Access to Systems (Requirement 10)
- ISO 27001 requirements for Physical entry controls (A.11.1.2) as well as Securing offices, rooms and facilities (A.11.1.3)
- MPAA Best-Practices Requirements for Entry/Exit Points (PS1.0), Visitor Entry/Exit (PS2.0), Perimeter Security (PS4.0), Authorization PS-6.0, Electronic Access (PS-7.0), and Logging and Monitoring (PS-10.0)
- CJIS Requirements for Auditing and Accountability (5.4), Access Control (5.5), Identification and Authentication (5.6), Physical Protection (5.7), and Media Protection (5.8)
- HIPAA Requirements for Workforce Security, Information Access Management, Facility Access Controls, Access Controls, Audit Controls, and Person or Entity Authentication