

SECURITY WHITEPAPER



This whitepaper outlines how Unmand keeps its cloud systems secure, the steps we take to build security into our products, and the role your organization plays in keeping your work environment secure.

Our security approach focuses on security governance, risk management and compliance. This includes encryption at transit, IP restrictions, role-based access control, system monitoring, logging and alerting, and more.

We apply security best practices and manage the platform security so customers can focus on their business. Our products are designed to protect customers from threats by applying security controls at every layer from the physical to application, while keeping the ability to rapidly deploy security updates without customer interaction or service interruption.

PRODUCT SECURITY

We constantly strive to achieve the right balance between releasing features that matter to you and deploying secure products. The following features and activities help our products, and your data, safe.

ROLE & PROJECT ACCESS CONTROLS

Access to data within Unmand's portal is governed by role and project-based controls and can be configured to define granular access privileges. There are permission levels for read, write and administrator.

IP RESTRICTIONS

Unmand products can be configured to only allow access from specific IP address ranges you define. This access is configurable at an organisation level directly within the Unmand portal.

2-FACTOR AUTHENTICATION

Unmand secures your account with enforced two-factor authentication. Anyone accessing their account must have both a password and a one-time access code generated on their mobile device.

DATA RETENTION

You can set the retention period for your data directly in the portal. This can be set from no data retention, and up to 30 days.

ENCRYPTION AT REST

All data sent is encrypted in transit and customer data encrypted at rest. We use Transport Layer Security (TLS) 1.0, 1.1, 1.2 to protect data from unauthorized disclosure or modification. Our implementation of TLS enforces the use of ciphers & key lengths.

AUDIT AND LOGGING

We maintain comprehensive logs of all activities and actions for each product. These logs can be used for your audit purposes or internally for troubleshooting and support.

SECURE CREDENTIAL STORAGE

Unmand follows secure credential storage best practices by never storing passwords in a plain text format. Passwords are salted and repeatedly hashed before being stored.

DATA OWNERSHIP

Your data 100% belongs to you. Unmand does not use, or sell your data to third party providers.

PHYSICAL SECURITY

DATA CENTERS

Unmand's physical infrastructure is hosted and managed within Amazon Web Services (AWS). Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data centre operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402
- PCI Level 1
- FISMA Moderate

ON SITE PREMISE

Access to Unmand's offices is restricted to authorised personnel. We deploy several security features such as individualised swipe card access, security video feeds, intrusion detection technology, and other security measures.

PEOPLE SECURITY

BACKGROUND CHECKS AND ACCESS

Each team member has an extensive background check and undergoes comprehensive training on data security protocols. Only a limited number of staff members can access customer data.

CONFIDENTIALITY AGREEMENT

All employees are bound by non-disclosures and confidentiality agreements.

CONTINUOUS EDUCATION CAMPAIGN

Unmand provides staff with continuous communication on emerging threats, performs phishing awareness campaigns, and communicates with staff regularly.

QUALITY CONTROL

PEER CODE REVIEWS

Whether it's a new feature or a bug fix, every line of code is reviewed by peers before being released to production. Security reviews are performed as appropriate for the work.

CONTINUOUS INTEGRATION AND DELIVERY

Every code release is automatically subjected to a pipeline of rigorous tests and analysis before it is merged. Our continuous deployment system and development process allow us to rapidly update and patch our system whenever needed.

SEPARATE ENVIRONMENTS

The development and testing environments are logically separated from the Production environment.

DISASTER RECOVERY

GLOBAL RESILIENCY

We maintain multiple geographically separated data replicas and hosting environments to minimise the risk of data loss or outages. Using AWS gives Unmand the ability to remain resilient globally even if one location goes down.

CUSTOMER DATA BACKUPS

Unmand performs regular backups of account information, and other critical data using Amazon S3 cloud storage. All backups are encrypted in transit using strong encryption. Backup files are stored redundantly across multiple availability zones.

SECURITY COMPLIANCE

Unmand is committed to mitigating risk and ensuring services meet regulatory and security compliance requirements.

PRIVACY

We've developed and implemented comprehensive processes, privacy safeguards, and ongoing training for our teams to ensure we are following industry best practices. Across the organization, our teams are regularly trained and updated on essential privacy and security practices.

GDPR

We're committed to compliance with the EU General Data Protection Regulation (GDPR) and have implemented a wide range of technical and organisational measures. This includes the ability for customers to delete provided information, such as names and email addresses, and any data uploaded to any product. Customers may also access, and export their data using our platform.

SUMMARY

Unmand's cloud platform enables businesses to deliver superior customer experiences by automating mundane tasks, reducing errors and streamlining existing processes. Security mechanisms to protect physical, network and application components of the platform, coupled with transparency about security practices and compliance best practices, give customers the confidence they need to move automation to the cloud.