Azlo.app

Azlo Security

At Azlo, we see our relationship with Umpqua Bank not as a typical vendor engagement but as a true partnership built on trust, collaboration, and shared success.

We fully understand the importance of maintaining the highest security and compliance standards. As part of our commitment to supporting Umpqua's goals, we are prepared to adjust and strengthen our security protocols as needed to align with your internal policies and regulatory expectations.

Our priority is to work closely with your team to ensure our platform integrates seamlessly, securely, and in a way that supports Umpqua's operational excellence. We believe that through this collaboration, we can help position Umpqua as a leader in secure, efficient, and human-centered banking.

The next few pages outline Azlo's existing security architecture and compliance measures.

Azlo.app

Azlo Security

Phase One & Two

No Access to Sensitive Data

Customer & Employee Data

- Isolated from all customer-facing systems and data stores. No personal data is processed or retained.

Use Case Boundary

- Smart automation systems use only internal, non-sensitive data (e.g., summarizing reports, scheduling tasks, assisting in documentation).

Hosting & Infrastructure Security

Cloud Platform

- Built on AWS, using top-tier security infrastructure.

Data Encryption

- Data at rest is encrypted with AES-256 in S3, RDS, and other services, compliant with FIPS 140-2.

In Transit

- All communication between components and services utilizes TLS 1.2 or higher for secure, encrypted transport.

Networking

- Hosted in a VPC with strict security groups and ACLs.
- Private subnets isolate LLM processing from public.

IAM & Access Control

- Role-based access is managed via AWS IAM.
- Access is limited by least privilege across all services.

Azlo.app

Azlo Security

Machine Learning Layer (AWS BEDROCK)

- Amazon Bedrock securely runs LLMs without storing or training on your data.
- The LLM provider does not log or fine-tune the data, and it remains private.
- Request data is processed in-memory and never stored.

Compliance & Standards

Designed around leading industry frameworks

- SOC 2 Type II readiness (platform and practices).
- ISO/IEC 27001-aligned policies for data management.
- NIST 800-53 principles are followed in system design.
- GDPR & CCPA conscious architecture (though the system does not handle PII).

Monitoring & Incident Response

- CloudTrail and CloudWatch are used for logging and anomaly detection.
- 24/7 automated monitoring for unauthorized access, failed login attempts, and network anomalies.
- Our Incident response plan includes audit logs, rollback strategies, and alert escalation procedures.

Azlo.app

Azlo Security

Machine Learning Layer (AWS BEDROCK)

- Amazon Bedrock securely runs LLMs without storing or training on your data.
- The LLM provider does not log or fine-tune the data, and it remains private.
- Request data is processed in-memory and never stored.

Compliance & Standards

Designed around leading industry frameworks

- SOC 2 Type II readiness (platform and practices).
- ISO/IEC 27001-aligned policies for data management.
- NIST 800-53 principles are followed in system design.
- GDPR & CCPA conscious architecture (though the system does not handle PII).

Monitoring & Incident Response

- CloudTrail and CloudWatch are used for logging and anomaly detection.
- 24/7 automated monitoring for unauthorized access, failed login attempts, and network anomalies.
- Our Incident response plan includes audit logs, rollback strategies, and alert escalation procedures.

Azlo.app

AWS bedrock

Azlo Security

Regulatory Compliance

Amazon Bedrock and the AWS infrastructure comply with major frameworks, including:

- SOC 1, 2, 3
- ISO/IEC 27001, 27017, 27018
- FedRAMP and HIPAA eligible

Data Privacy in API Calls

Customer & Employee Data

- Your data is never used for model training or fine-tuning.
- Each API call is stateless; the model processes the request in-memory and does not persist input or output.
- You own your data, and the AWS Service Terms and Data Privacy Addendum govern its usage.

From AWS documentation
Input and output data from Bedrock are not used to train any of the foundation models on Bedrock, and they are not stored or seen by model providers.

Logging and Storage

- By default, AWS does not retain or log payloads of your Bedrock API calls.
- You can opt in to CloudWatch logging for troubleshooting, but this is off unless explicitly configured.
- All data in transit is encrypted using TLS 1.2 or higher.

Azlo.app

AWS bedrock Cont.

Model Providers

- Third-party models (e.g., from Anthropic or Cohere) are deployed and hosted within the AWS environment.
- They do not receive your raw data; the interaction is fully contained within AWS's secure infrastructure.

Bottom-line

Using Amazon Bedrock ensures that:

- Your data stays private and within your control
- No training or data retention happens without your consent
- All interactions are secured within a trusted cloud environment

Azlo Security