Security
You Can Trust

Asure Data Security

Asure has a full time information Security Team, led by a Director of Information Security, Joshua Gohman, CISSP, who is a former information security auditor and cybersecurity expert.

Asure has an Information Security Committee that includes several members of senior management that meet on a weekly basis.

We maintain several documented security-related policies that are reviewed on a regular basis and audited annually including:

· Information Security Policy

· Information Security Governance Policy

· Business Continuity Plan

· Change Management Policy

· Risk Management Policy

· Incident Response Policy

· Information Classification and Handling Policy

Eight Reasons to Choose Asure:

01 Data Hosting on Amazon Web Services (AWS) to leverage their infrastructure for greater security, confidentiality, and availability of our client's environment

02 Annual audit of SOC2 Type 2 by a licensed 3rd party auditing firm

03 Publicly held company and conducts SOX audits, which include an IT/Security component

04 Compliant with the strictest privacy standards, including CCPA, HIPAA, NY SHIELD Act, and GDPR

05 Defense in-depth approach to cyber information security including monthly vulnerability management scans of our environments, antivirus software installed on all endpoints and production environments, encryption of client data at rest and in transit

06 Various technical and administrative controls limit access to sensitive data to only those that need it for their daily jobs

07 Performance monitoring tools placed across our environments to alert us on incidents and activity

08 Individual databases and micro-pods in AWS for each Service Bureau

Asure Software employees are required to undergo annual information security awareness training, which covers topics including CCPA, HIPPA, phishing, etc.

DATA
Secure, Safe, & Compliant

As a business, how secure is the data for you and your clients? At Asure, we take cyber security seriously.

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations

SOC1 & SOC2 Certified

Controls that directly relate to the security, availability, processing, integrity, confidentiality, and privacy at a service organization.

| Infrastructure Security	DDoS Mitigation	Data Encryption	Inventory & Configuration	Monitoring & Logging	Identity & Access Control
AWS provides several security capabilities and services to increase privacy and control network access.	AWS customers benefit from AWS services and technologies built from the ground up to provide resilience in the face of DDoS attacks.	AWS offers you the ability to add an additional layer of security to your data at rest in the cloud, providing scalable and efficient encryption features.	AWS offers a range of tools to allow you to move fast while still ensuring that your cloud resources comply with organizational standards and best practices.	AWS provides tools and features that enable you to see exactly what's happening in your AWS environment.	AWS offers you capabilities to define, enforce, and manage user access policies across AWS services.

AWS Global Infrastructure

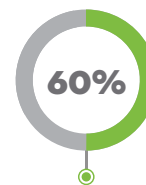The AWS Cloud Spans 61 Availability Zones within 20 geographic regions around the world.

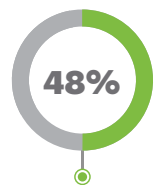## General Small Business Cyber Security Statistics

The AWS Cloud Spans 61 Availability Zones within 20 geographic regions around the world.

45%
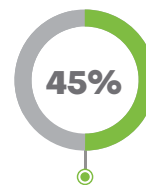
45% percent of cyber attacks target small business

60%

60% percent of companies go out of business within 6 months of a cyber attack

48%

48% percent of data security breaches are caused by acts of maicius intent.