GenVis

See Good. Do Good.

GenVis Security Program

Document Number: IT018

Date:
13th of July 2020

GenVis
See Good. Do Good.

Contents

The team at GenVis understand that the security of your data is paramount. You trust us to keep it safe and we take that seriously.

We take care to ensure the latest security processes and protocols are adopted and embedded within our solutions, aligning to industry standards and our own best practices. The GenVis Security Program adheres to the ISO 27001 standard and is guided by the NIST[1] Special Publication 800-53.

Whether a customer opts to use our products on the Cloud or Self-Hosted, they can rest assured knowing that GenVis has built the highest-level of security into our applications and security practices.

Secure by Design

GenVis embeds a culture of security within its Engineering team whereby security is considered throughout the software development lifecycle. Security analysis tooling is integrated into the GenVis build pipeline to ensure security quality assurance.

GenVis products are developed by in house GenVis engineers and where third party technology is leveraged, GenVis initially assesses and then reviews the risk posed by the third party to provide assurance across the software supply chain.

The GenVis patch management cycle routinely patches all GenVis assets to optimal levels. Software patch levels at all levels of the technology stack are monitored and maintained.

GenVis ensures that any emerging vulnerabilities are dealt with swiftly. GenVis subscribes to a threat intelligence service to gain early sight of vulnerabilities impacting the industry. GenVis is able to deploy vulnerability remediation at short notice to any part of its technology stack.

Data Encryption and Segregation

All data is encrypted in transit and at rest. We align our processes to industry best practices and adjust/upgrade them as required.

GenVis ensures that customer data is always segregated such that no customer organisation is ever able to access the data of another customer organisation and no user is able to access unauthorised data.

Customers seeking a GenVis hosted solution with the highest level of infrastructure segregation are able to opt for a dedicated cloud service account, thus ensuring complete isolation of all resources at the infrastructure level.

[1] The National Institute of Standards and Technology

Access Control

GenVis has built granular access control within its products to help customers grant the permissions needed by teams and individual team members, and control who within their organisation has access to what information.

Network Protection and Monitoring

GenVis products comprise network level firewalls to protect the perimeter and segregate the network appropriately, and web application firewalls to enhance the protection of the web application. Vulnerability scanning and intrusion detection systems constantly monitor and alert whenever anomalies are detected. All security information events are stored and GenVis is able to search this information for investigation purposes. This ensures we can rapidly respond to any issues that arise. In the event of a security breach, we will promptly notify you of any unauthorized access to your data.

Secure and Reliable Infrastructure

GenVis products are cloud-agnostic solutions that can be hosted with leading cloud service providers, AWS and Azure, or deployed in your on-premises environment.

National cyber security agencies across a range of territories have awarded AWS and Azure PROTECTED certification for the cloud services used by GenVis.

AWS data centres are monitored by 24/7 security, biometric scanning and video surveillance, and both AWS and Azure are SOC 1, SOC 2 and SOC 3 certified.

GenVis products are backed up at the application and data level ensuring that, in the worst case, customers are always able to recover from an incident.

Where customers deploy to, and manage their Self-Hosted cloud account they are responsible for ensuring the security of their content and data.

Cloud Service Provider Compliance

AWS and Azure Cloud infrastructure have been designed and managed in alignment with many regulations, standards and industry best practices. Here are just some of the accreditation certifications standards that both have:

- Australian Signals Directorate Certified Cloud Services Member
- General Data Protection Regulation (GDPR)
- International Standards Organisation (ISO) 27001
- ISO 27017
- ISO 27018
- ISO 9001
- ISO 20000
- Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS)
- Federal Information Processing Standard (FIPS) 140-2
- Federal Information Security Management Act (FISMA)
- Federal Risk and Authorization Management Program (FedRAMP)

- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 9001
- CSA STAR Attestation
- CSA STAR Certification
- CSA STAR Self-Assessment
- System and Organization Controls (SOC) 1, SOC 2, and SOC 3
- Payment Card Industry Data Security Standard (PCI DSS) version 3.2
- Cloud Infrastructure Services Providers in Europe (CISPE)
- EU Data Protection Directive (Directive 95/46/EC) Model Clauses
- Information Security Registered Assessors Program (IRAP) (Australia)
- International Computer Room Experts Association (ICREA)
- International Traffic in Arms Regulations (ITAR)
- National Institute of Standards and Technology (NIST) 800-171
- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Singapore Multi-Tier Cloud Security (MTCS) Level 3
- UK Cyber Essentials Plus
- UK Data Protection Act 1998
- UK National Cyber Security Centre (NCSC) Cloud Security Principles

Physical Security and Geo Resilience

Both AWS and Azure provide the highest levels of physical resilience within data centers and GenVis products always provide resilience across at least two availability zones so that a failure limited to one availability zone does not degrade service delivery.

Data Privacy

When using GenVis products, your data and information always remains yours. GenVis contractually commits that customers control and own all rights, title and interest in and to the customer content. GenVis does not claim any ownership of customer content. Customers can download and/or have their content permanently removed at any time by submitting a written request to GenVis.

By accessing GenVis products, customers may provide us with or create, data and content, including text, photos, images, audio, video, other materials and personal information. GenVis personnel cannot access customer data without the explicit permission of the customer. Where GenVis customers require support or assistance, GenVis administrators are only able to access customer data with the explicit permission of the customer for a limited period of time.

GenVis will only access and use customer content, with the customer's explicit permission, for the limited purposes of providing GenVis products to them, improving GenVis products, developing new AI capabilities, and as otherwise set out in our Terms of Service and in our Privacy Policy. The only exception to this is in the case of a system emergency where access may be required to ensure the operability of GenVis products. Only a small team of GenVis system administrators have the ability to access the system. Their access is authenticated using 2 factor authentication and data access is logged.

Neither AWS nor Azure accesses or uses customer data for any purpose other than as legally required for maintaining their respective services. You can read more about AWS's privacy policy here and Azure's privacy policy here.

Data Sovereignty and Residency

The team at GenVis understand that ensuring your data remains in and never leaves your local region is likely to be a requirement for you. GenVis products only use your local region to store and process your data ensuring that your data remains localised and is never moved outside of that region.