egress

Cloud Security Principles FAQ

April 2020

www.egress.com | info@egress.com | 0844 800 0172 | @EgressSoftware

Contents

What is this?

This document is intended to provide a high-level overview of our Cloud Security Principles, including commonly asked questions. More in-depth documents are available for specific products.

FAQ

How and what data is encrypted?

- Egress utilises identity-based AES 256-bit encryption using FIPS 140-2 approved cryptographic libraries. This provides the highest level of security for complete end to end data exchange. Egress hides the complexity of encryption using a revolutionary patent protected architecture and is the true evolution of PKI based encryption systems.
- See our hosting page for details.

How is user data protected against physical tampering, loss, damage or seizure?

- Our data centres are provided by third party solutions, which detail their own physical security.

Who has access to my data?

- Subcontractors have no direct access to customer data.
- Access is limited to Egress staff on a least privilege basis, so that only the required staff have access. Any staff that must have access, is required to have Security Clearance before access is approved.

Is data segmented and separated?

- Customer data is either logically or physically separated. Where logical separation is used, Egress uses techniques such as specific customer keys to ensure that one customer cannot access another customers data.
- Logical separation is applied at the database layer, maintained with unique client keys

Is data protected in transit and at rest?

Yes, this is managed through the Azure facility where data is stored securely.

What certifications do our partners have? Eg AWS, Azure?

This can be found at https://www.egress.com/security/hosting

What cloud deployments do you provide?

This can be found at https://www.egress.com/security/hosting

Do you have a capability to continuously monitor and report the compliance of your cloud infrastructure against your information security baselines?

Yes, this is provided by our hosting partners.

Do you have controls in place to ensure that information security risks in cloud environments are mitigated?

Yes, Egress performs reviews considering any emerging risks and security best practice, looking to apply them to the platform as soon as available. If this is not possible, for any reason, then we would look to other remedial work to ensure that services were adequately protected.

Is audit logging, monitoring and alerting in real time implemented?

For resources deployed in the cloud (Azure), MS Security Centre provides real time alerting of security events. We also have a third party SIEM than monitors logs for any unusual/suspicious activity who then report this to our internal Security team.

Is protection implemented against malicious attacks, DDoS attacks?

Yes, this is provided by Cloudflare for DDoS protection in addition to other services such as Web Application Firewalls.

Does your cloud service recovery procedure include hardware independent restore and recovery capabilities?

Whilst backups are taken to allow restore to given points in time if needed, backups take place at scheduled times throughout the day to different sites. This therefore allows for site independence with a maximum of 15 mins delay.

Do you have procedures in place to ensure forensics and investigations conducted by other customers do not have negative impact on customer service levels?

Egress Operations staff has undergone forensics training and we have a specialist forensics company on contract should their services be needed.

Is data securely deleted from your data centre storage, contingency sites and backup media when no longer required?

Yes, this is completed in line with our Data Retention Policy. Due to the nature of some of the cloud environments used, we cannot always provide evidence for customer virtual machines.

Can you provide verifiable evidence that customer's expired data can be securely destroyed from environments?

We will work with your security and compliance teams to provide the required evidence based on destruction of physical disks/data or the logical deletion of disks/data for public cloud.

Do you perform penetration testing on your cloud service infrastructure as prescribed by industry best practices and guidance?

Yes - by a 'Check' Provider at least annually (spread across all Egress service lines), or after any major change.

Do you have encryption key management systems in place for your cloud services?

Egress can provide an on-premise infrastructure which gives you the ability to fully manage your own encryption keys, where applicable.

Can you establish and provide the physical location/geography of storage of customer data?

Data would ordinarily be stored in line with the sender's settings, based on where they were located and whether the user was part of a business account that specified data be kept on their business site. This is locked to a specific location and/or region and we would default to UK based storage by default for UK customers.

US customers' data is stored within the US.

Can you restrict the location of data to specific geographies?

Yes, see above.

Egress Software Technologies Ltd

Egress provides human layer security – helping users receive, manage and share sensitive data to meet compliance requirements and drive business productivity.

Egress' award-winning platform makes sure emails and files are delivered to the correct recipient, encrypts and protects sensitive data, and provides compliance auditing and reporting.

www.egress.com

info@egress.com

0844 800 0172

@EgressSoftware