egress

Egress Security Measures and Controls

April 2020

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

Contents

Security Measures and Controls

Information Security Policies

Egress have an information security policy that:

- Provides management direction and support for Egress' information security;
- Does so in accordance with the various business requirements as well as the relevant laws and regulations that Egress is subject to;
- Is reviewed annually, or earlier if there are significant changes to the scope of Information Security within Egress or change in strategic business direction;
- Is approved by management and is published and communicated to all employees along with relevant external parties through our own internal Secure Workspace;
- Is an overarching document supported by various subject specific security policies.

Security Policies

In addition to Information Security related policies, we also have security policies that include, but are not limited to:

- Firewall Management Procedures;
- Remote Access;
- Change Control;
- Penetration Testing;
- Control of Records;
- Data Sanitisation;
- Incident Management; and
- Lost Stolen Assets.

Organisation of Information Security

Egress have a certified Information Security Management System (ISMS) that follows the ISO27001:2013 standard. The scope of the ISMS encompasses all Egress offices.

The ISMS is managed by a cross organisation Information Security team that includes Senior Management, Security, Operations, Technical Operations, Technical Development and Human Resources representatives. It meets monthly and minutes of each meeting are maintained.

Egress has an in-house security team who manage the ISMS on a day to day basis, supplemented as necessary by specialist external resources and 3rd party suppliers.

Human Resources Security

Prior to Employment

- All UK staff are subject to UK Government Baseline Personnel Security Standard (BPSS) checks and a basic criminal record check;

- All personal references are checked; and
- Commensurate checks are undertaken on staff recruited in North America, Canada and Amsterdam. This includes:
    - SSN Traces;
    - Sex Offender Search;
    - Global Watchlist Search;
    - National and Country Search; and
    - Terrorism checks.

During Employment

- Where necessary (based on client requirements), staff may be subject to enhanced Government national security or policing personnel vetting processes;
- All new staff are given security training by the Information Security team. Current staff are given annual security awareness training and mandatory Cyber Security Awareness programs monthly; and
- Staff are provided with appropriate guidance in the form of our Acceptable Use Policy and specific subject policies and procedures. Each month staff are informed of new policies through our internal 'Policy of the Month' update.

Post-Employment

Staff are reminded of their legal, regulatory and contractual obligations in their exit letter when they leave Egress. All access and permissions are removed and revoked when leaving Egress.

Asset Management

Responsibility for Assets

Egress assets are:

- Listed in a maintained inventory;
- Assigned owners (designated departments/employees); and
- Operated with under the scope of the Acceptable Use Policy.

Information Classification

Egress information is:

- Classified in accordance with our Information Classification and Labelling Policy. The Policy lists the tiers of classification that Egress use, which are designed to categorise the information in the documents based on the value, legal requirements, sensitivity and criticality of that information to Egress;
- Classified using Egress Protect; and
- Where required by Government clients, national classifications schemes are adopted and implemented for projects/services.

Access Control

Access to all Egress services is based on the principle of least privilege, and users are only granted the minimum permissions to conduct their role.

Cryptography

Egress utilise commercial grade encryption to protect all traffic both externally and internally within our platforms.

Egress uses identity-based AES 256-bit encryption using FIPS 140-2 approved cryptographic libraries as default on our endpoints. 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 which is the true evolution of PKI based encryption systems.

Physical and Environmental Security

Egress platforms operate from secure Data Centres across the UK. Security requirements are included in the contracts with Data Centre providers. As part of due diligence, Egress review their compliance with various International Security standards (such as ISO27001:2013) to ensure client commercial data and personally identifiable information (PII) is adequately protected in-line with accepted International Standards.

Physical Security

UK Building Security

Egress offices have swipe card access to enter the office space. An additional unique pin is also required after working hours or on weekends to enter the office space, and logs of all access is recorded. Egress have 24/7 CCTV footage watching over the entrances and exits of the office space.

UK Building Access

The Egress London and Sheffield offices require an access card in order to go beyond the reception on the ground floor.

Egress Staff

Staff have individual access cards that allow them past the turnstiles (if applicable) on the ground floor and onto the correct floor only. They use the same card to enter the Egress reception, and then need to use it again to enter the office space.

The Toronto, Boston and Amsterdam offices do not have reception areas, but office space is secured with access controls. Floors require key cards/codes to enter any Egress office space.

Egress Guests

Guests receive a temporary pass once reception has contacted the respective Egress office to confirm the visitor is expected. Once on the correct floor, they must be "buzzed" into the Egress reception where they must sign in and receive an Egress specific visitor pass. It is mandatory that this pass is worn and visible when present in Egress offices. The member of staff expecting them can then collect their guest. All visitors are always accompanied.

Server Rooms Access

Server rooms require a unique access card and pin which is only given to those that require it.

Operations Security

Egress maintain event logs to support incident investigations. Egress uses a 3rd party Security Operations Centre (SOC) and managed Security Incident Event Management (SIEM) solution to support the monitoring of security incidents/events.

Communications Security

Egress utilise commercial grade encryption to protect all traffic both externally and internally within our platforms. Egress also have network services supporting Egress platforms which are segregated in-line with good industry practices.

Information Systems Acquisition, Development and Maintenance

Development of Egress products follows industry standard processes and is undertaken by Egress personnel. Security testing of services is undertaken in line with business and contractual requirements.

Supplier Relationships

Egress has a small supplier footprint in respect of Egress platforms, they include Data Centre providers, a 3rd party SOC provider and a Digital Forensic supplier for digital forensic investigations.

Each contract with an external supplier meets the requirements of the GDPR.

Information Security Incident Management

Reporting Information Security Events and Weaknesses

Egress have a documented incident management process which:

- Displays avenues for incident, vulnerability and weakness reporting; and
- Provides guidance for incident classification.

Egress employees, contractors and third-party users are:

- Aware of their responsibility in reporting incidents, vulnerabilities and weaknesses through the Roles and Responsibilities Policy;
- Given bespoke Information Security training, which highlights the importance of reporting security incidents, vulnerabilities and weaknesses; and
- Provided with the appropriate means to report and communicate incidents, vulnerabilities and weaknesses.

Management of Information Security Incidents and Improvements

Egress has:

- Established policies to ensure swift, effective and orderly Incident Response and Management. These are listed in our master Incident Management process;
- Established Incident Management roles within the roles and responsibilities of all Egress employees, so that the response is structured, orderly and most importantly, efficient;
- Monthly ISMS cross organisation management meetings (including at least one C-Level member of staff), which reviews Security Incidents from across the Group; and
- Support and guidance in place regarding evidence collection i.e. a digital forensic capability.

Incident Management

Crisis Management

Egress maintains realistic Incident Management and Crisis Management plans that recognise the importance of having high-level executive backing and understanding to ensure we can manage and resolve incidents or crises.

Business Continuity Management

Egress have a Business Continuity Plan which includes, but is not limited to:

- Business risks identified through our Risk Assessment Methodology;
- A Business Impact Analysis; and

- Plans for events that may cause disruption to various services/products/locations and how Egress will respond.

Disaster Recovery

The Egress Disaster Recovery plan covers disruption to key products, services and locations. It details how the Egress IT capability will return to a suitable level of functioning following an IT related crisis.

Compliance

Legal

Egress comply with all relevant legislation in relation to the operation of Egress services and platforms. Egress have an in-house Legal Counsel who leads on all legislative matters.

In the USA, Canada and the Netherlands, local legislation applies.

Legal guidance for users of Egress platforms can be found here.

Audit

Egress' Information Security team manage audit schedules that support the Egress ISMS.

Audits are carefully planned to prevent disruption to business processes whilst making sure that Egress can demonstrate our adherence to the ISO/IEC 27001 standard and the efficacy of our ISMS.

Access to audit tools are limited to the relevant teams that require access to them. Egress operates on the principle of least privilege.

Certifications

Egress perform a variety of audits and assessments to provide ourselves and our customers with independent, third-party assurance that we are adhering to our commitment to protect our systems and customer's data. We hold:

- ISO 27001:2013 Certification;
- SOC II Type 1 (current assessment);
- FIPS 140-2;
- EU-Approved cryptographic product to EU RESTRICTED classification;
- NATO IACD;
- Cyber Security to Government Scheme;
- PGA;
- Trustwave PCI DSS Certification;
- Skyhigh CloudTrust;
- Commercial Product Assurance;
- Cyber Essentials and Cyber Essentials Plus Certification; and
- Common Criteria.

Further information can be found at: https://www.egress.com/certifications.

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