G-Cloud 10 Service Definition Document

Egress Email and File Protection

Egress Software Technologies
18.05.18

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

Confidentiality Statement

This document contains information confidential and proprietary to Egress Software Technologies. It shall not be disclosed in whole or part by the recipient to any third party or to any employees other than those who have a need to know such information. It shall not be duplicated or used by the recipient for any purpose other than to evaluate Egress Software Technologies products and services.

No part of this document may be reproduced, distributed, stored in a database or retrieval system, or transmitted in any form or by any means, without the exclusive and written permission of Egress Software Technologies. No liability is assumed for damages resulting from the use of the information contained herein.

Copyright Notice

Executive Summary

Service users and customers have a reasonable expectation that their sensitive personal information will be shared securely and efficiently between Government organisations and third parties. However, it is commonly accepted that there is currently no pan Government solution for communication of confidential data outside of Government accredited networks.

Current local solutions are either designed to meet specific service needs, installed as local implementations, or simply not practical for day to day use (e.g. Winzip, PGP).

Existing national investment is targeted at improving secure communications within different parts of the public sector, for example Central Government to Local Government or within the NHS. However, there already exists a daily need to communicate with a large number of voluntary, community sector, private sector partners, and service providers which are not currently supported by these initiatives.

Egress Software fully acknowledges the role of secure Government networks in addressing many of the issues with regards internal communication between local and central Government, health, and criminal justice organisations. Designed to complement these projects, Egress offers encryption services that addresses a key gap identified across Government where is there is no coherent or widely recognised way of communicating sensitive personal/business information with partners and service providers in the third sector, private sector, or even small Government agencies.

Service Overview

1.0 Introduction

1.1 This part of the Service Schedule describes the Egress Service, the Service Types, Service Dependencies and forms part of our Agreement with you.

2.0 Service Overview

2.1 The Egress Email and File Protection service enables users to encrypt, share, and remotely manage secure information up to Impact Level 3 (IL3)/OFFICIAL/OFFICIAL-SENSITIVE under the current Government Classification Policy, as certified and accredited by NCSC: https://www.ncsc.gov.uk/products/egress-switch

2.2 Offered as a fully managed service, a hybrid cloud service, or private cloud on premise installation, Egress enables small or large organisations in the Public and Private sector to share information securely by enforcing policy centrally and integrating information security into existing workflow processes. Additionally, comprehensive real-time auditing ensures that information owners know precisely who, when, and where confidential data is being accessed. This new approach to secure information sharing enables users to maintain visibility and control wherever the data resides.

2.3 Egress Email and File Protection service is a client-server solution that consists of two principal components:

2.3.1 Egress Server Infrastructure (ESI)

A number of server components externally visible as a web-service that communicates with its clients over SOAP 1.1-based protocol on top of an SSL/TLS encrypted channel.

2.3.2 Egress Client

An application that makes requests to ESI to download policy information, register secure packages and retrieve keys for packages created by other users. Multiple Egress Clients are available as MS Windows, OS X and mobile applications, as well as web-based applications.

3.0 Service Types

3.1 There are three Service Types. The Customer's applicable Service Type shall be as stated in the Order Confirmation.

3.1.1 Fully Hosted Cloud Service: leverages the Egress Service Infrastructure for complete delivery of encryption services, key management, and user management.

3.1.2 Hybrid Hosted Cloud Service: leverages core elements of the Egress Service Infrastructure for key management and user management while installing Client Side Software to deliver encryption services.

3.1.3 Private Cloud Service: leverages Client Side Software for complete delivery of encryption services, key management, and user management.

4.0 Egress Server Infrastructure (ESI)

4.1 Egress Server Infrastructure (ESI) is responsible for the following:

4.1.1 Storing, distributing and controlling access to secure package properties, keys and detailed audit data.

4.1.2. Managing access restrictions applying to groups of packages based on their properties.

4.1.3 Assigning and resolving policies to users, groups of users and organisational units

4.1.4 Providing a basic user web interface for self-help or accessing packages.

4.1.5 Encryption and decryption of packages.

4.1.6 Storage of encrypted packages.

5.1 Core Components

5.2 Egress Server Infrastructure (ESI) is made up of several core components, which can be grouped together or distributed between multiple servers depending on security and resiliency requirements.

5.2.1 Authentication Service

5.2.2 Key Management Server

5.2.3 Web Interface

5.2.4 Egress Gateway

5.2.5 Web Access

5.2.6 Secure Storage

5.2.7 (Optional) Vetting Database and Web Service

6.0 System Requirements

6.1 Authentication Service:

- Physical or virtual server
- MS Windows Server 2012 R2 / MS Windows Server 2016
- Windows Server Roles
    - IIS with Metabase Compatibility
    - ASP.NET
    - .NET 4.5 Framework
    - SMTP server
    - WCF Activation
    - Active Directory Lightweight Directory Services
    - Windows Identity Foundation

6.2 Key Management Server (Connection Point):

- Physical or virtual server
- MS Windows Server 2012 R2 / MS Windows Server 2016
- Windows Server Roles
    - IIS with Metabase Compatibility
    - ASP.NET
    - .NET 4.5 Framework
    - SMTP server
    - WCF Activation
    - Active Directory Lightweight Directory Services
    - Windows Identity Foundation

      Database:

        - Physical or virtual server
        - MS Windows Server 2008 R2/MS Windows Server 2012 R2
        - Microsoft SQL 2008 Advanced Express or higher

6.3 Web Interface:

- Physical or virtual server
- MS Windows Server 2012 R2 / MS Windows Server 2016
- Windows Server Roles
    - IIS with Metabase Compatibility
    - ASP.NET
    - .NET 4.5 Framework
    - SMTP server
    - WCF Activation

6.4 Egress Gateway:

- Physical or virtual server
- MS Windows Server 2012 R2 / MS Windows Server 2016
- Windows Server Roles
    - IIS with Metabase Compatibility
    - ASP.NET
    - .NET 4.5 Framework
    - SMTP server

6.5 Web Access:

- Physical or virtual server
- MS Windows Server 2012 R2 / MS Windows Server 2016
- Windows Server Roles
    - IIS with Metabase Compatibility
    - ASP.NET
    - .NET 4.5 Framework
    - SMTP server

6.6 Secure Storage:

- Physical or virtual server
- MS Windows Server 2012 R2 / MS Windows Server 2016
- Windows Server Roles
    - IIS with Metabase Compatibility
    - ASP.NET / ASP.net 4.5

- .NET 4.5 Framework

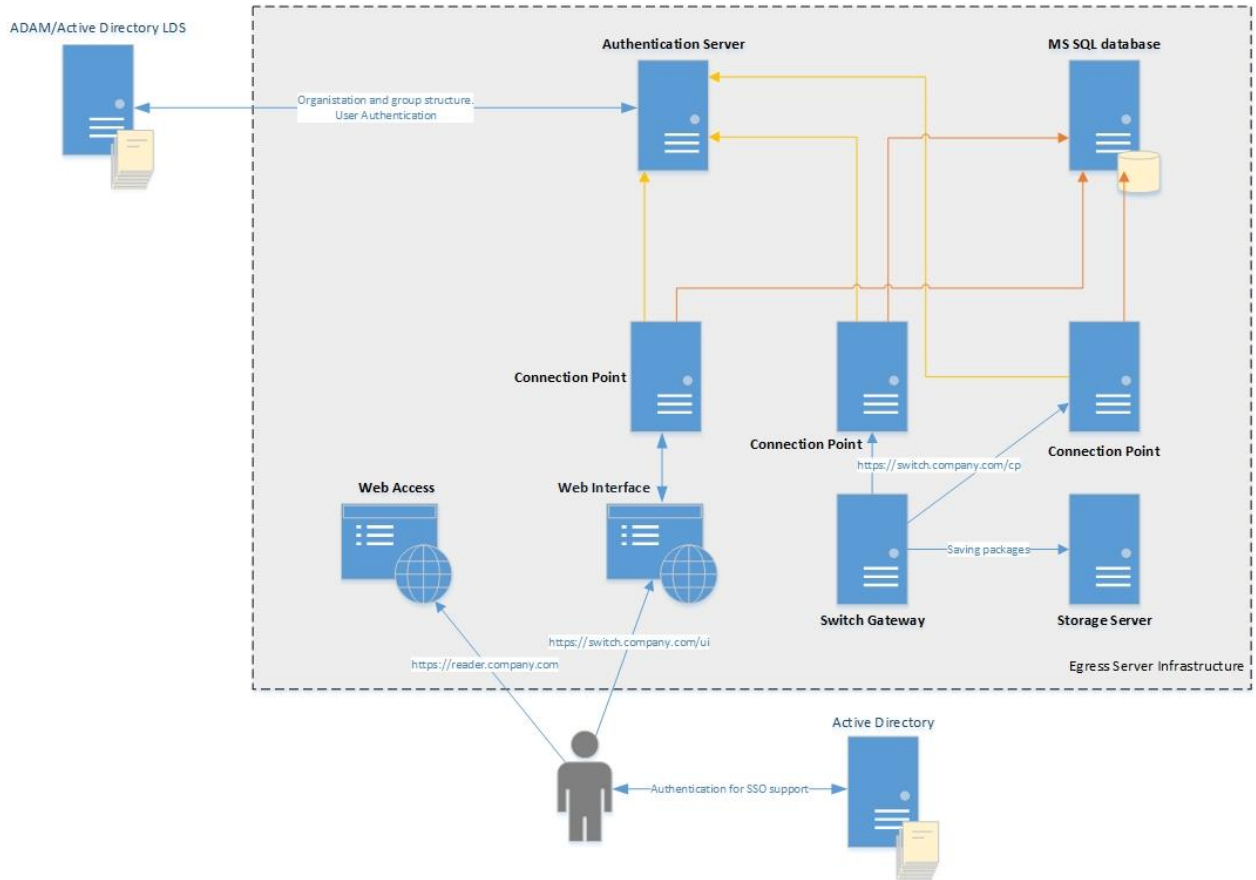
6.7 (Optional) Vetting Database and Web Service:

- Physical or virtual server
- MS Windows Server 2008 R2/MS Windows Server 2012 R2
- Windows Server Roles
  - IIS with Metabase Compatibility
  - ASP.NET
  - .NET 4.5 Framework
  - SMTP server
  - WCF Activation
  - Active Directory Lightweight Directory Services
  - Windows Identity Foundation

  Database:

  - Physical or virtual server
  - MS Windows Server 2008 R2/MS Windows Server 2012 R2
  - Microsoft SQL 2008 Advanced Express or higher

Fig.1 below shows the components of ESI in a distributed set up (excluding optional Vetting Database and Web Service).



7.0 Service Dependencies

7.1 The following Service Dependencies are specific to the Hybrid Hosted Infrastructure and the On-Premise Hosted Infrastructure:

7.1.1 Microsoft Windows operating system (Windows 2012 R2 x64 for server components, Windows 7 x32 + Outlook 2010x32 for client components)
7.1.2 Microsoft .NET framework (version 4.5)
7.1.3 Microsoft Internet Information Server version 7.5+ (part of Windows 2008 R2 x64)

7.2 For all new configurations of the Egress Services, Egress will produce a Service Design Document which will include details of the proposed solution, policy design and architectural overview.

7.3 In order for Egress to produce the Service Design Document and to provide the Services, Customer shall provide the following information:

7.3.1 Customer site access and contact details;
7.3.2 Encryption policy requirements;
7.3.3 System integration requirements (such as integration with AV, content scanning, archiving, etc.);
7.3.4 Details of operating systems and mobile platforms used within Customer's organisation; and
7.3.5 Details of deployment software currently used within Customer's organisation;

7.4 To enable the deployment by Egress of the required Client Side Software, Customer shall provide the following information:

7.4.1 Mail-flow Topology;
7.4.2 What email servers are currently in use in Customer's organisation;
7.4.3 What Anti-virus software is used within Customer's organisation;
7.4.4 What gateway scanning software is used within Customer's organisation;
7.4.5 Whether email archiving and/or journaling used within Customer's organisation; and
7.4.6 What file size limitation is applied to email messages (if any);

7.5 IN ADDITION, CUSTOMER SHALL COMPLY WITH THE FOLLOWING OBLIGATIONS:

7.5.1 Providing the necessary hardware/virtual infrastructure, environmental conditions, and security measures at the Customer sites in accordance with the Services system requirements;
7.5.2 Giving Egress (and any third party engaged by Egress in connection with the Services) reasonable access to equipment that is covered by, or required for, the Services at reasonable times during Working Hours and in accordance with Customer's normal security procedures;

7.5.3 Ensuring that all permissions of any kind needed for the installation and operation of Client Side Software are in place at all times and can be verified by Egress upon request;

7.5.4 Any other obligations reasonably notified to Customer by Egress from time to time.

8.0 Term and Termination

8.1 The subscription to the Services starts on the date that Egress tells the Customer that its account is active. The Customer agrees to maintain its subscription to the Services for the agreed initial subscription period, and thereafter for each renewed subscription period.

8.2 This Agreement shall continue for the Call-Off Contract term.

8.3 Either party may terminate this Agreement in accordance with the terms of the G-Cloud 10 Framework Agreement and the Call-Off Contract.

8.4 If the Customer terminates this Agreement during the initial subscription or any renewed subscription for any reason other than Egress material breach, it shall remain responsible for the payment of all charges (whether non-recurring or annual recurring charges) due for that initial subscription or renewed subscription period (as applicable). If these sums have been paid in advance, Egress shall be entitled to retain them in full. If these sums have been contracted for but are being paid by the Customer in instalments, any unpaid instalments shall become immediately due and payable.

8.5 Upon termination of this Agreement for any reason (a) generally: (i) all licences and rights granted by one of us to the other under this Agreement will immediately cease (except as provided in this section 8.5); (ii) Egress will stop permitting access to the Services, and Customer will stop (and will ensure its users stop) trying to access them; (iii) both parties will return, or if instructed destroy, equipment, property and other items and copies that we have belonging to the other (except that either party may retain confidential information where required by law); (iv) either Egress or the Customer (whoever is most appropriate) will delete any and all copies of any software provided by Egress from the Customer's systems. If the Customer does so, it will confirm to Egress in writing that it has done so. Where Egress does it, the Customer hereby grants to Egress all necessary physical or remote access to its sites and systems to do so; (v) any unpaid fees relating to either a period prior to the date of termination or expiry or an unexpired period of the Initial Subscription or any renewed subscription shall be immediately due and payable; and (vi) any rights, remedies, obligations or liabilities that accrued prior to termination or expiry won't be affected or prejudiced. (b)Post termination or expiry:(i) the Customer will have 30 calendar days from termination or expiry to request a copy of its Content. Egress reserves the right to charge for this at its then current rates. If a Customer doesn't request it, Egress will destroy or otherwise securely dispose of the Content after that period and will have no obligation to store it. The Customer may request that Egress continues to store it subject to: (A) paying any applicable fees; and (B) providing Egress with a written statement outlining the lawful basis for Egress to do so on the Customer's behalf signed by an authorised signatory of the Customer. (ii) Egress may retain copies of the Content where required to do so for legal or regulatory reasons, and it may continue to be stored and processed by Egress where it forms part of another user's Content."**Content**" means the files, data, text, audio, video and images that are

transferred, stored, shared or hosted on or through the Services by the Customer, its users and third parties, including any personal data in it

9.0 Incident Management

"Fault" means the Services are not performing in accordance with the current description at www.egress.com.

"Incident" means an event (including a suspected Fault) caused in relation to issues that are Egress' responsibility that is unplanned, causes an interruption to the Services, or a deterioration in its quality and requires a support ticket to be logged.

9.1 The Customer must appoint primary and secondary contacts who will be responsible for reporting and progressing Incidents.

9.2 Egress will carry out Incident management during the applicable support hours to attempt to: (i) restore the Services; and (ii) minimise any adverse impact of the Incident on the Customer.

9.3 Prior to reporting a suspected Incident, the Customer must complete initial troubleshooting and use all reasonable endeavours to ensure that it has arisen from issues that are Egress' responsibility.

9.4 Egress will have the right to charge the Customer for any reasonable costs Egress incurs in investigating suspected Incidents that are caused by issues that Egress is not responsible for (including, failures at the Customer's sites, the Customer's or a third-party's hardware or software).

9.5 Having completed its investigation if the Customer suspects there is an Incident the Customer must report it to Egress using the reporting methods that Egress notifies to it. The Customer must provide adequate information to enable Egress to replicate, diagnose and resolve the Incident and procure, at the Customer's own cost, such co-operation from users and third-party providers as is reasonably requested by Egress to assist in managing the Incident.

9.6 Egress will: (a) raise support tickets to separately identify Incidents and track their resolution to closure of the ticket. Incidents will be deemed to have commenced at the time Egress raises the ticket; (b) categorise Incidents in accordance with the severity levels in section 13; (c) maintain and update records of Incidents; and(d) investigate, carry out diagnostic activities, and resolve Incidents where such activities are included as part of the Customer's support services (subject to the terms of this section).

9.7 Incidents will be deemed resolved at the time that Egress notifies the Customer. A support ticket may be re-opened if it subsequently becomes apparent that the Incident hasn't been resolved.

9.8 Whenever possible the Customer must give Egress a minimum of 14 calendar days' notice of any event which the Customer is aware of which may disrupt the Services or Egress' provision of them to the Customer.

10.0 Changes

10.1 The Customer acknowledges that the Services are a 'software-as-a-service' solution (meaning changes for one customer can affect all Egress customers) and Egress reserves the right to change the details of them such as organisation, procedural and functionality charges over time and without prior notice (including to Incident reporting, management processes, service levels and descriptions). If these changes result in a material degradation to performance, accessibility or available functionality, the Customer may write to Egress and/or raise a dispute.

11.0 Maintenance Schedule

11.1 Egress will maintain a rolling maintenance schedule with regards to the Services and planned downtime (**Permitted Maintenance**). Egress will let the Customer know when it is going to carry out Permitted Maintenance and will try to do so with minimum disruption during normal working hours.

11.2 Egress can book up to a maximum of 24 hours for Permitted Maintenance in each calendar month which shall be notified to the Customer in advance.

11.3 Egress will not be liable for any losses, charges, damages, costs, liabilities or expenses incurred by the Customer or its users as a result of Permitted Maintenance.

11.4 Outages arising due to Permitted Maintenance that is carried out by Egress will be subtracted from the total number of hours in the relevant service period when calculating Service Availability.

11.5 The Customer will be responsible for notifying its users of any Permitted Maintenance.

12.0 Emergency Changes and Outages

12.1 Unplanned outages to the Services may occur from time to time due to a change requiring immediate action to either: (i) restore the Services; or (ii) prevent an outage, and which may be documented retrospectively with reduced (or in extreme cases, eliminated) testing if necessary to deliver it immediately (**Emergency Changes**) and will take priority.

12.2 If the Emergency Change is being made as a result of information provided by the Customer, Egress will use reasonable endeavours to process it within 2 hours of receiving notification and sufficient information from the Customer (subject to the Customer's support hours).

12.3 Egress will: (i) use reasonable endeavours to give the Customer as much notice as reasonably possible of any Emergency Changes; (ii) use reasonable endeavours to attempt to minimise any disruption to the Customer; and (iii) not be liable for any losses, charges, damages, costs, liabilities or expenses incurred by the Customer or its users as a result of an Emergency Change

12.4 The Customer will be responsible for notifying its users of any Permitted Maintenance.

13.0 Severity Levels

13.1 Severity Levels for Incidents are defined as follows:

Incident Severity Classification	
The following classifications link to the Incident Response and Incident Resolution time for each Incident, and drive the Incident management process.	
Incident Severity Level	**Definition**
Incident Severity Level 1 (P1)	A Service Failure where: a) The number of Permitted Users not able to utilise the Egress Service is greater than 10% of the total number of Permitted Users.
Incident Severity Level 2 (P2)	A Service Failure where: a) The number of Permitted Users not able to utilise the Egress Service is greater than 5% but not more than 10% of the total number of Permitted Users.

Incident Severity Level 3 (P3)	A Service Failure where: a) Permitted Users are reporting issues with the Egress Service, however the number of Permitted Users affected by the Incident does not exceed 5% of the total number of Permitted Users
Incident Severity Level 4 (P4)	A Service Failure where: a) A single Permitted User reports any issue with the Egress Service.

14.0 Service Levels and Measurement

14.1 Egress shall be responsible for measuring the Availability of the Services.

14.2 Where the Services are wholly or partially hosted by Us, its Actual Availability will be measured as the percentage of time that it's available in each calendar month. The target availability is 99.9% (**Target Availability**).

Actual Availability is calculated as follows:

$$P = \frac{A-B}{A} X\ 100$$

Where:

P	=	percentage availability in that calendar month
A	=	number of hours in the relevant calendar month
B	=	number of hours in the relevant calendar month during which the Services were not available **excluding time** where they're not available due to: • outages arising due to Permitted Maintenance; • agreed changes; • an Excluded Event; and/or • an Emergency Change.

An "**Excluded Event**" includes any of the following: (a) a Fault or Incident in, or problem associated with, software, hardware, connectivity, networks or other telecommunications systems not operated or provided by Egress; (b) the Customer's or a user's fault, negligence, act or omission, or that of any third-party not within Egress direct contractual control; (c) the Customer's non-performance of, or delay in performing, any of its responsibilities under the G-Cloud 10 Framework Agreement or Call-Off Contract; (d) any request for Egress to modify or test a Customer site even though no Fault has been detected or reported; (e) service suspension or a force majeure event; (f) an Emergency Change, Fault or Incident resulting from the Customer's or a user's acts or omissions or those of any third-party on the Customer's behalf; or (g) any other circumstances caused by events for which Egress is not liable in accordance with the terms of the G-Cloud 10 Framework Agreement or Call-Off Contract

15.0 Service Credits

15.1 Subscription Charges invoice in full and final settlement of any and all liability that Egress may have for the relevant issue. No other Services Credit shall be payable.

15.2 Service Credits are not available, and Egress is not obliged to pay them, where the Customer has not upgraded its subscription (or any relevant part of its software, services, system or infrastructure) within 12 months of any upgrade, new release or new version being made available by Egress or the relevant owner (as applicable).

15.3 Service Credits accumulate up to a maximum of 14% of the ARCs paid by the Customer during the relevant subscription period.

15.4 Service Availability: Where the availability of the Egress Switch Service does not meet the Target Availability, Customer shall be entitled to a following Service Credits. Service Credits are only payable if the Actual Availability is below the Target Availability during the relevant period **and either**: (a) Egress notifies the Customer that a Service Credit is payable; or (b) the Customer notifies Egress in writing that it believes a Service Credit is payable within thirty (30) calendar days of the end of the relevant month. Following receipt of any notice from the Customer, Egress will investigate the Customer's claim and confirm if a credit is due:

Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Credit
Availability of the Service	Availability %	99.90%	99.8% – 99.9% (2% Service Credit gained) 99.7% - 99.8% (3% Service Credit gained)

Service Level Performance Criterion	Key Indicator	Service Level Performance Measure	Service Credit
			99.6% - 99.7% (4% Service Credit gained) 99.5% - 99.6% (5% Service Credit gained) <99.5% total Service Credit of 14% in any Service Period

The Service Credit for Service Availability is calculated by using the following formula:

Service Credit £ = ((a-x)*c)*d)

Where:

- a is the Service Level Performance Measure (%) below which Service Credits become payable;
- x is the Achieved Service Level (%) for a Service Period;
- c is the Service Credit (%) payable if the Achieved Service Level falls below the Service Level Target; and
- d is the amount payable in respect of the Services during the Service Period, not including VAT

15.5 Incident Response: Where Severity Level 1 incidents are not resolved within the target Incident Resolution Time, Customers shall be entitled to the following Service Credit. Service Credits are only payable if the Actual Availability is below the Target Availability during the relevant period **and either**: (a) Egress notifies the Customer that a Service Credit is payable; or (b) the Customer notifies Egress in writing that it believes a Service Credit is payable within thirty (30) calendar days of the end of the relevant month. Following receipt of any notice from the Customer, Egress will investigate the Customer's claim and confirm if a credit is due:

Service Levels				Service Credits
Incident Severity Level	**Key Indicator**	**Incident Response Time**	**Incident Resolution Time**	
Incident Severity Level 1 (P1)	Incident Response Time and Incident Resolution Time	Within 15 minutes	Within 4 hours	1.5% Service Credit gained for each incident not resolved under the specified Service Level Performance Measure
Incident Severity Level 2 (P2)	Incident Response Time and Incident Resolution Time	Within 30 minutes	Within 8 hours	0.75% Service Credit gained for each incident not resolved under the specified Service Level Performance Measure
Incident Severity Level 3 (P3)	Incident Response Time and Incident Resolution Time	Within 3 hours	Within 72 hours	n/a
Incident Severity Level 4 (P4)	Incident Response Time and Incident Resolution Time	Within 6 hours	Within 72 hours but not exceeding 5 business days	n/a

The Service Credits for Incident Resolution are calculated using the following formula:

Service Credit £ = ((a*c)*d)

Where:

- a is the number of Incidents not resolved within the Service Level Performance Measure during a Service Period;
- c is the Service Credit (%) payable in each instance where the Achieved Service Level falls below the Service Level Performance Measure; and
- d is the amount payable in respect of the Services during the Service Period, not including VAT

16.0 Charges

16.1 The charges for the Egress Service consist of one or more of the following components:

16.1.1 Initial non-recurring charges (NRC) in return for system installation and initial set up;

16.1.2 Other non-recurring charges (ONRC) raised periodically during the term of the Agreement in return for policy customisation; or

16.1.3 Annual Recurring Charges (ARC);

17.0 Billing

17.1 We will bill you:

17.1.1 Monthly in advance for all NRCs;

17.1.2 Monthly in advance for all ONRCs; and

17.1.3 Annually in advance for all ARCs.

18.0 Additional Charging

18.1 Egress may charge in accordance with its then current rates for any support required in respect of:

18.1.1 any maintenance, alterations, modification or adjustments by or on behalf of the Customer made to the Services without Egress' prior written consent or approval.

18.1.2 any use by the Customer of the Services in conjunction with other software or hardware not supplied or approved in writing by Egress; and

18.1.3 any Excluded Events.

18.2 Egress' right to charge under section 18.1 above is without prejudice to its other rights under the Framework Agreement and Call-Off Contract, including any right to terminate the provision of support services.

18.3 Egress reserves the right to charge for non-standard elements of the Services requested by the Customer (and for any and all design work or service customisation involved in the scoping, design, delivery or support of such elements).