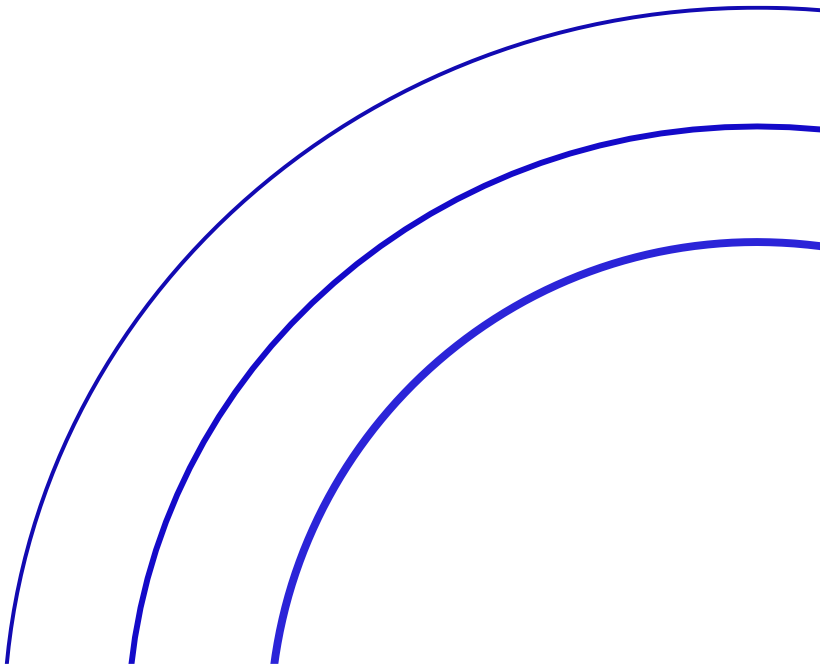
Email Security Services Service Description



Document Control

TITLE:	**Email Security Services Service Description**	**DOCUMENT REF NO:**	QMS REC146
DESCRIPTION:	This document defines the services provided by Calligo's Email Security Services		
OWNER/ AUTHORITY:	VP Cloud Operations	**VERSION NO:**	1.1
DOCUMENT CROSS REFERENCE:	N/A	**VERSION DATE:**	20/02/2023
DISTRIBUTION METHOD	Email and Website	**DOCUMENT CLASSIFICATION**	Internal

DOCUMENT OWNER & APPROVAL
The VP, Cloud Operations, is the owner of this document and is responsible for ensuring that this service description is reviewed in line with the review requirements of Calligo's Information Security Management System, Project Management Frameworks as well as the guidance and requirements of the CSSF.
Approved by the Chief Operating Officer, Calligo ("Entity") on 23 January 2023

CHANGE HISTORY RECORD				
VERSION	**DESCRIPTION OF CHANGE**	**AUTHOR**	**APPROVAL**	**DATE OF ISSUE**
1.0	Initial Issue	Director, Operations Management	VP Cloud Operations	23/01/23
1.1	Updating supporting documentation links	Director, Operations Management	VP Cloud Operations	20/02/23

Contents

DOCUMENT CONTROL **1**

1. SERVICE OVERVIEW **4**

2. SERVICE INCLUSIONS **4**

2.1. CO-ITSM-ESS 4

2.2. CO-ITSM-SD 4

3. SERVICE PROVISIONS **4**

3.1. CO-ITSM-ESS 4

3.1.1. Inclusions *4*

3.1.2. Exclusions *5*

3.2. CO-ITSM-SD 5

3.2.1. Inclusions *5*

3.2.2. Exclusions *5*

4. ROLES AND RESPONSIBILITIES **5**

5. REPORTING **6**

6. DATA RESIDENCY **6**

7. SERVICE REQUIREMENTS **7**

8. ACCESS REQUIREMENTS **7**

9. SUPPORT LOCATIONS **7**

10. SERVICE CATALOGUE REQUEST ITEMS **7**

11. STANDARD SLO'S **8**

SERVICE-LEVEL-AGREEMENT.PDF (CALLIGO.IO) **8**

12. RELATED DOCUMENTS **8**

13. OPTIONAL SERVICES **9**

14. AUXILIARY SERVICES **9**

14.1. SERVICE ONBOARDING & TRANSITION 9

14.2. CHANGE REQUEST AND CHANGE CONTROL PROCESS: 10

1. Service Overview

This document defines the services provided by Calligo's Email Security Services service. The Email Security Services service is one of a suite of services within the Calligo Operating Model.

2. Service Inclusions

2.1. CO-ITSM-ESS

This service leverages client specific requirements for Email Security Services.

2.2. CO-ITSM-SD

This service leverages an ITSM platform and trained Level 1 Service Desk Analysts to cover activities that provide a client facing Service Desk.

3. Service Provisions

3.1. CO-ITSM-ESS

3.1.1. Inclusions

CO-ITSM-ESS	
Scope Item	**Description**
Inbound Sender Policies	Rule definition for sender domain, IP, and geolocation whitelisting and blacklisting, SPF/DKIM/DMARC sender verification, AV and reputation-based e-mail scanning
Message categorization actions	Assign filtering actions by detected message type, including Corporate, Transactional, Marketing, Mailing list, social media, and Bulk E-mail
Custom block/quarantine thresholds	Scanned mail is assigned a spam confidence score. Thresholds can be assigned to block or quarantine dependent on message score.
Phishing policies	Detection of phishing or fraudulent mail, typo squatting protection, URL scanning
Message content policies	Rule definition for permitted and denied attachment formats, encrypted documents, message headers and body content, DLP (outbound only)
Rate control policy	Limit X messages sent or received by an IP address within a 30-minute period.
E-mail Quarantine	Release of blocked messages to recipients' mailboxes, quarantine notifications and self-service quarantine management

3.1.2. Exclusions

CO-ITSM-ESS	
Exclusion Item	**Description**
Per-user filtering	Mail policies are assigned globally to the mail domain
DNS	Management of DNS records required for mail delivery (MX, TXT, SRV, etc.)
Client Mail Server	Administration or troubleshooting client mail server
Recipient Mail Server	Administration or troubleshooting for mail routing or delivery issues external to the spam filter
Intra-site messaging	Message filtering cannot apply to internal mail

3.2. CO-ITSM-SD

3.2.1. Inclusions

CO-ITSM-SD	
Scope Item	**Description**
Access to the Calligo ITSM platform	24/7 access to the Calligo ITSM platform that provides capabilities for clients to raise new support tickets and to access open or historic support tickets.
Telephone Support	Access to the Calligo Service Desk via the issued telephone contact numbers during regional Business Hours only.
First Line Fix	Access to the Calligo L1 Service Desk Analysts for first line fix or resolution.

3.2.2. Exclusions

CO-ITSM-SD	
Exclusion Item	**Description**
24/7 Telephone Support	This is a chargeable addition.
Onsite support	All support delivered via the Service Desk offering is remote.

4. Roles and Responsibilities

The table below provides a responsibility matrix for the core Email Security Services elements:

Service Activities – Core Elements	Calligo	Customer
CO-ITSM-ESS		
Mail filter policy changes	R, A	A, C
User Quarantine		R, A
Blocked Message release	R, A	A, C
Client Admin assignment	R, A	A, C, I
CO-ITSM-SD		
Raising support requests	R	R, A
Contacting Calligo Service Desk via telephone for P1 Support Requests	I	R, A
Correctly assigned the right category and priority to all incoming support requests	R, A	C, I
Providing full and detailed information when creating new support requests	I	R, A
Providing detailed and regular ticket updates	R, A	I
Responding to all ticket updates where additional information or testing is requested from Calligo Service Desk	I	R, A
Providing prompt confirmation of ticket closure agreements.	I	R, A

* Subject to having purchased Microsoft SPLA licensing from Calligo

R=Responsible, A=Accountable, C=Consulted, I=Informed

5. Reporting

The table below provides details on the additional Monthly Reporting and Analytics for Email Security Services that are included in the core service:

Service Item	Reporting Item	Description	Frequency
CO-ITSM-ESS	Inbound Traffic	Summary of inbound messages and scan results (Allowed, Blocked: Rate Control, Spam, Virus, etc.	1/month if requested
CO-ITSM-ESS	Outbound Traffic	Summary of outbound messages and scan results (Allowed, Blocked: Rate Control, Spam, Virus, etc.	1/month if requested
CO-ITSM-ESS	Top Senders	Highest frequency senders and their delivery results (Allowed or Blocked: Rate Control, Spam, Virus, etc.)	1/month if requested
CO-ITSM-ESS	Top Recipients	Highest frequency recipients and their delivery results (Allowed or Blocked: Rate Control, Spam, Virus, etc.)	1/month if requested

6. Data Residency

Calligo Data Residency

7. Service Requirements

Service Item	Requirements Item
CO-ITSM-ESS	Mail Exchange (MX) records in DNS must point only to the spam filtering service.
CO-ITSM-ESS	A mail server is necessary for delivery of received mail
CO-ITSM-ESS	The firewall must accept SMTP connections to/from the spam filtering service (TCP ports 25, 587, 465)
CO-ITSM-ESS	Outbound message scanning requires entry of a smart host server address on the client mail server
CO-ITSM-SD	Client is provided information on support access methods
CO-ITSM-SD	All Priority 1 incidents are logged, and the client must follow up with a telephone call into support.

8. Access Requirements

Requirements Item
Not applicable

9. Support Locations

Calligo Support Locations

10. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Sender Whitelist/Blacklist	24BHR	Sender's e-mail address or domain, action (allow or block)	5/week
Block region or language	24BHR	Countries and character sets to block	1/week
Custom Realtime blackhole list	24BHR	Server address or IP	1/week
Authentication exemption	24BHR	Sender's domain or IP address, exemption (SPF, DKIM, DMARC, PTR)	5/week
Release message (within 30 days)	24BHR	Sender, recipient, approximate date and time message was blocked	5/week

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Filtering threshold change	24BHR	Desired spam confidence score to trigger message block or quarantine	1/week
Content policy change	24BHR	Content patterns to allow or deny, e-mail message samples	1/week
Phishing policy change	24BHR	Phishing detection action (Ignore, Quarantine, Block)	1/week
URL scan exemption	24BHR	Domain to exempt from URL protection	1/week
Outbound DLP Policy	24BHR	Data format or category (e.g. HIPAA), allow or deny	1/week
Rate limit change	24BHR	Desired rate limit or sender exemption	1/week
Quarantine notification enablement or schedule change	24BHR	Desired quarantine notification frequency and schedule	1/month
Assign Client Role	24BHR	User, required role (helpdesk or admin)	1/month
Sender Whitelist/Blacklist	24BHR	Sender's e-mail address or domain, action (allow or block)	5/week

11. Standard SLO's

Service-Level-Agreement.pdf (calligo.io)

https://azure.microsoft.com/en-gb/global-infrastructure/geographies/#overview

Service Level Agreements – Home | Microsoft Azure

12. Related Documents

Supporting documents for this service:

Any clients onboarding to Calligo will require the following document as an introduction to service

Calligo – Welcome to Support for Clients

13. Optional Services

In addition to the Email Security Services service, Calligo can provide the following service items as optional add on services for Email Security Services:

Service Item	Service Item Reference	Description
Service Delivery Manager	CO-ITSM-SDM	The Service Delivery Manager will be responsible for the business as usual and account management relationship. This will include service reviews, point of escalation, responsible for Information Technology Infrastructure Library (ITIL) practice adherence, interfacing with third-party suppliers also participating under the customer's Service Integration and Management model and ensuring that Calligo meets or exceeds Service Level Objective (SLO) targets.
Technical Account Manager	CO-ITSM-TAM	The Technical Account Manager will be responsible for the technical collaboration between the customer and Calligo support teams and will play a key role in technical service improvement, managing deployment of new services or configuration changes, ensuring optimal performance and uptime of the application stack, and interfacing with third-party suppliers as required under the customer's support model.

14. Auxiliary Services

14.1. Service Onboarding & Transition

To launch Email Security Services service successfully, service design, onboarding and transition will be required to prepare and test both the environment and the managed services processes. Calligo will undertake several workshops to discuss and confirm each element of the service to ensure all parties are aware of roles and responsibilities in advance of service launch.

Service transition and onboarding covers areas such as ticket management setup, platform readiness with knowledge share, and finalising all ITIL practices. A test and acceptance criteria are captured and signed off, to allow for the Email Security Services service to commence.

After service launch, Calligo uses a formal service transition framework as the basis to carry out acceptance into service procedures, for new services landing into managed services. We typically engage at the initial stages of a project to ensure service operation adoption and readiness is planned and carried out correctly. This materializes as follows:

- To review designs, build and test artefacts to ensure supportability.

- Attend change review boards to gain early sight of changes by way of knowledge acquisition.
- To witness and validate designs and builds are delivered as proposed and intended.
- Complete operational into service documentation, training, and runbook enablement, which is required as part of the service hand-over.

14.2. Change Request and Change Control Process:

All infrastructure changes introducing risk to the environment will require change control which includes, but not limited to, Microsoft Security Patching, Infrastructure Upgrades, Deployments, Configuration Item status change. This can be generated from maintenance or an event such as an upgrade required on the system released by Third Party vendors, requested by the customer, or from a monthly release of security patches.

Where possible Standard Changes will be used with minimal risk, repeatable implementation steps, and prior approval from the customer in the form of an email.

An Emergency, or unplanned, change process will be raised to resolve a Priority 1 or 2 incident or to implement an emergency Security Patch. This accelerates the time to implement and resolve.

All Requests for Change will be reviewed internally, assessed internally, and authorized or rejected through Calligo ITSM tool.