Enterprise Business Unit Solutions

Contractual Service Description

Cloud Mail Security

Date	06/09/2018
Sensitivity	**Unrestricted**

Table of contents

Sensitivity: Unrestricted

1. Introduction

Cloud Mail Security (hereafter 'the Service') protects SMTP compliant e-mail systems against internal and external security threats such as described in this document. The Service is offered "in-the-cloud", meaning no heavy hardware or software investments are required by the Customer. All inbound e-mail traffic of mailboxes in the scope of this Agreement is directed towards an Internet based security platform thanks to a change in the MX record of the Customer domain. There it is cleaned according to several predefined parameters before the e-mail traffic arrives on the Customer's infrastructure. Optionally, also outbound e-mail can be directed towards the Internet based security platform, where it can be analyzed if it matches the configured security policy. For this the Service needs to have the sending IP address or hosted e-mail service registered. The basic functionalities of the Service aim to protect the Customer organization against spam and malware, to give the Customer the ability to encrypt its email traffic and to provide the Customer with reporting tools. Depending on the chosen functional options, the Customer can have this complemented with several advanced features.

The Service is available in two Flavors: Reactive Care and Full Care. They differ in terms of number of activities that are performed by Proximus in the areas of on-line administration, configuration and support. The Full Care flavors is available as from 25 mailboxes.

The Service is based on the following infrastructure elements, called Solution elements:

- Platform
- Administration Portal
- Spam Quarantine Portal
- Synchronization Tool

The Service Overview Chapter lists the functionality and support activity types that may be included in the Service and specifies the scope of each support activity provided by Proximus per Solution element.

The functionality of the Service is described more in detail in the 'Functional Service Description' Chapter whereas the support Services ('Assist and Care Services') provided to the Customer during the implementation and the operational phases are described respectively in the Chapters 'Implementation Phase' and 'Operational Phase'.

2. Service Overview

The tables below list the functionality and activity types that may be included in the Service (also called Service components). The Service components are:

- per default included in the Service ('DEF');
- or optional ('OPT') and must be selected by the Customer;
- or subject to a separate contract ('SC').

Once the Service components have been selected through the Order Form, the scope of this Agreement is defined. Adding or changing Service components will lead to a new Agreement.

2.1 Functional Service

In the below table an overview is made of the functionalities which are included in the basic service and in the options. Further explanation of these details is provided in the Functional Service Description Chapter.

Services components	Detail	Reactive care	Full Care
Basic Service	Antimalware Antispam Opportunistic TLS encryption Address Registration Message Tracing Reporting End User Spam Quarantine Portal and notifications Disclaimer management	DEF	DEF
Data Loss Prevention (DLP)	E-Mail Data Protection E-Mail Image Control Enforced TLS Encryption Basic Policy Based encryption E-Mail Impersonation Controls	OPT	OPT
Advanced Threat Protection (ATP)	Cloud-based sandboxing Click-time URL protection Detailed Malware reporting	OPT	OPT
Add-On: Active Directory Integration	Synchronisation of Active Directory users and groups	OPT	OPT

2.2 Assist and Care Services

The support provided by Proximus during the Implementation and Operational phases is applicable to Solution elements listed per type of activity in table below. The Service does not include any activities regarding any other Solution elements.

Service Component	Solution elements in scope	Reactive Care	Full Care
Assist			
Assist service	Platform Spam Quarantine Portal Synchronization tool Administration Portal	DEF	DEF
Optional Assist service	Platform	OPT	
Service Desk Access	All solutions elements	DEF	DEF
Incident Handling			
Remote Diagnostics	All solution elements	DEF	DEF
Remote Intervention	All solution elements	DEF	DEF
Configuration Restore	Administration Portal Spam Quarantine Portal	DEF	N/A
Configuration Handling			
Configuration handling with Customer Read Access	Administration Portal	N/A	DEF
Configuration handling with Specific Access Rights	Spam Quarantine Portal/ Synchronization Tool	N/A	OPT
Configuration Handling without Access Rights	Platform	N/A	DEF / OPT
Configuration back-up	Administration Portal Spam Quarantine Portal	DEF	DEF
Change Handling			

Standard Changes	Administration Portal Spam Quarantine Portal	N/A	SC
Custom Changes	Administration Portal Spam Quarantine Portal	N/A	SC
Updates and Upgrades	All solution elements	DEF	DEF
Monitoring			
Service Availability Monitoring	All solution elements	N/A	DEF
Reporting			
Service Availability Reporting	Platform Administration Portal Spam Quarantine Portal	N/A	DEF

3. Functional Service Description

The Service relies on a hosted security platform (also called 'Platform') which aims to filter inbound and optionally outbound e-mail messages of the email addresses in the scope of the Agreement (meaning the email addresses mentioned in the Validation list- see below) to help to protect Customer's infrastructure from security threats such as described in this document.

The parameters of the functionalities of the Service are configured via the Administration portal placed at the Customer's disposal. In case of Reactive Care Flavor, the Customer configures himself these parameters in the Administration Portal whereas in case of Full Care Flavor, Proximus configures these parameters in the Administration portal for the Customer based on the Technical Configuration Requirements Form and the subsequent Customer's requests. The Customer acknowledges and agrees that it is solely responsible for selecting the configuration and assuring that the selection conforms to its policies and procedures.

The Service supports e-mail services from multiple vendors, such as Microsoft Exchange, Office 365, Google Apps, etc. The list of compatibilities is available upon request.

This Chapter describes the different functionalities which may be included in the Service, regardless the selected Flavor.

3.1 Basic Service

3.1.1 Antimalware

This functionality aims to provide the Customer with a protection against known and unknown malware distributed via URLs or files to and optionally from the mailboxes of the Validation list. The protection is a combination of various technologies, such as heuristics, reputation and signature based engines.

The Administration Portal is used to configure the parameters of this functionality which includes, but is not limited to:

- Drop infected e-mails
- Quarantine suspected viruses proactively until a signature/solution is released.
- Send automatic alarms to administrator and/or End users for notification
- Release e-mails to the first address of the original recipient list, to a pre-defined e-mail address or to an alternative address requested by the Customer
- Create virus banners to inform End users about the e-mail scanning
- Set maximum e-mail sizes

Emails suspected being malware by default are put in quarantine and maintained there during 30 Calendar days. At the expiration of this period, the e-mail is automatically deleted.

3.1.2 Antispam

This functionality aims to provide the Customer with a protection against spam meaning unsolicited commercial mail by scanning inbound and optionally outbound e-mail traffic of the mailboxes of the Validation list.

A multi-layered approach is applied, meaning the following techniques are used, such as:

- A private approved senders list compiled by the Customer or (with the Customer's approval) his individual End users.
- A private blocked senders list compiled by the Customer or (with the Customer's approval) his individual End users.
- A number of public blocked sender lists.
- A signature based system.
- Symantec.clouds' SkepticTM heuristic detection.

E-mails that are suspected of being spam can be subject to multiple actions, according to what has been configured in the Administration portal. Actions defined as a result of a signature based or heuristic detection hereby supersede any less severe action previously allocated by one of the preceding methods. Possible actions are:

- Drop e-mails from suspected senders using reputation filters
- Quarantine e-mails from suspected senders using reputation filters
- Drop e-mails from identified spam
- Quarantine e-mails from identified spam
- Tag suspected e-mails within the subject line
- Tag suspected e-mails within the header
- Release e-mail from spam quarantine by administrators
- Release e-mail from spam quarantine by End-users

E-mails suspected being spam maintained in quarantine are deleted as described in the End User Spam Quarantine Portal and notification section below.

3.1.3 Opportunistic TLS Encryption

This functionality aims to allow the Customer to securely exchange emails outside its organization using the encryption protocol SMTP over TLS, hence over an encrypted channel. The partner organization(s) with which the Customer wants to exchange e-mails over an encrypted channel are identified in the Administration Portal. A secure private e-mail network is setup with those partner organisations, using authentication certificates that are fully managed for the Customer. This is only possible if the partner organisation's mail server support TLS. In other cases, the e-mail will be delivered in clear text.

Additionally, the Customer can receive encrypted e-mail communication sent opportunistically by organizations that have TLS-capable mail servers.

Proximus draws the attention of the Customer on the fact that with this functionality   the e-mail itself is not encrypted, only the channel is encrypted. This as opposed to the Basic Policy Based Encryption functionality.

3.1.4 Address Registration

Thanks to this functionality, the Customer can upload in the Administration portal a list of valid e-mail addresses of End users in the organisation. E-mails sent to non-registered End users are blocked. The sender will receive a 550 invalid recipient error message in case the e-mail was legitimate but the address was incorrectly formed or misspelled.

Customer agrees to provide and maintain a list of valid e-mail addresses to receive the Service (the "Validation List"). It is Customer's responsibility to verify the Validation List prior to the Service being made available and throughout the term of Agreement.

Customer accepts that Service Levels will not apply to e-mails sent to invalid addresses or not mentioned in the Validation list.

For the avoidance of doubt, Customers using the Spam Quarantine system must maintain a Validation List and have the Address Registration capability enabled. If Customer is unable to provide such Validation List and requests that the Address Registration capability is disabled, Proximus will review each such request on a case-by-case basis and reserves the right to decline requests, in Proximus' sole discretion.

3.1.5 Message Tracing

The Track and Trace search functionality of the Administration portal enables the Customer to check how specific e-mails have been processed by the Platform. It reveals details on the different processing steps such as the reception of the e-mail by the Platform, the actions taken on the e-mail, the delivery of the e-mail, etc. No copies of the e-mails are stored.

The Track and Trace search facility is ideally suited for searching individual e-mails as it allows the Customer to avoid browsing through large numbers of e-mails to find a specific e-mail. The e-mails that have been processed within the last 30 Calendar days only are traceable.

The Track and Trace functionality is accessible for the Administrator, this is Proximus in case of Full Care Flavour and the Customer in case of Reactive Care Flavour. If needed, additional End users can be given read permissions on Track and Trace functionality.

3.1.6 Reporting

Reporting dashboards are available in the Administration Portal. The Dashboards displays a selection of key statistics, such as, but not limited to:

- Number of e-mails scanned
- Number of e-mails identified as spam
- Number of times a data protection policy was triggered (in case the option DLP is ordered).

The statistics in these dashboards can be shown per domain or for all domains.

Next to that, the Administration Portal enables the Customer to retrieve reports in the form of documents. The reports in document format can be generated for all Customer domains or per individual domain, but not per individual mailbox. The reports are available in different formats and can be scheduled to be mailed to a number of predefined recipients as well. Specifically following formats are available:

- Graphical dashboards
- Summary reports in .pdf, comprising charts, graphs, and tables, for the last year maximum.
- Detailed reports in .csv, with a limit of 500.000 rows. These provide a detailed log listing of all service activity for all domains. The reporting data is only for the last 30 Calendar days maximum.

The reporting data is available for 12 months.

3.1.7 End User Spam Quarantine Portal and Notifications

The Spam Quarantine Portal is a portal where intercepted e-mails that have been identified by the Service as spam or e-mails that contain data or images that violate Customer's compliance rules are kept in quarantine.

In this End User Spam Quarantine portal, the Administrator of the Customer organisation can view, release, and delete quarantined mail, manage blocked and allowed senders, and specify settings and preferences. The Administrator can also give this right to (some of the) End users for the e-mails sent to the e-mail address of the concerned End user.

Depending on the configuration, End users can receive a notification when an e-mail has been quarantined.

E-mails are kept in Quarantine Portal for 14 Calendar days, unless they are deleted sooner.

3.1.8 Disclaimer management

An e-mail disclaimer is the text in the footer of an inbound or outbound e-mail that passes through the Service. Thanks to this functionality, disclaimers can be configured using a combination of default and custom e-mail disclaimers, for inbound and optionally outbound e-mails of the email addresses of the Validation list, at global, domain, and group level.

Proximus reserves the right to scan all outbound Emails if the Customer configures to the Service for outbound emails. A default disclaimer message will be applied to e-mails that are scanned by the Service from the time of provisioning the Service.

Proximus reserves the right to update the default disclaimer message at any time. This shall not be deemed as an amendment to the Agreement.

3.2 Data Loss Prevention

When selected, the Data Loss Prevention option provides the Customer with the following functionalities aiming to reduce the risk of data loss:

3.2.1 E-mail Data Protection

This functionality allows the Customer to create a set of rules according to which incoming and optionally outgoing e-mail is filtered on basis of the email content. Each rule identifies a particular format of e-mails (or attachments: Microsoft Office Documents, PDF documents or text files) for which a prescribed course of action has to be taken.

The Administration portal is used to configure or review the applicable rules and corresponding actions to be taken on inbound and optionally outbound e-mails. Possible actions are:

- block and delete suspected e-mail;
- tag (the header of) suspected inbound e-mail
- redirect or copy suspected e-mail to a specified administrator;
- compress e-mail attachments;
- log in only to the management portal's statistics;
- Tag the subject line.

3.2.2 E-Mail Image Control

This functionality allows the Customer to identify, control and block inappropriate images embedded in e-mails or attachments (in Word, Excel and PowerPoint attachments, with exception of content under the sole control of the sender, such as password-protected or encrypted files). It scans inbound and optionally outbound e-mail using methods such as:

- Approved senders and recipients lists.
- Approved image signatures in a Customer database.
- The global Image Control community database.
- The Image Composition Analysis (ICA) engine.

The Administration portal is used to configure actions to be taken on inbound and optionally outbound e-mail upon detection of inappropriate images. Possible actions are:

- log suspected e-mail;

- tag suspected inbound e-mail within the header;
- redirect or copy suspected e-mail to a pre-defined e-mail address;
- delete suspected e-mail;
- tag suspected e-mail in the subject line;
- send alert notifications to sender / intended recipient

The goal of this functionality is to detect inappropriate images, especially pornographic images. Please note a 100% detection rate of pornographic images is not guaranteed and that the definition of what does and what does not constitute a pornographic image is subjective.

3.2.3 Enforced TLS Encryption

This functionality allows organizations to create secure links with their business partners and/or with the Service, enabling all e-mail traffic in between to be encrypted without any additional action by the sender. The message content remains transparent to both sender and recipient**.**

Please note, unlike opportunistic TLS encryption, E-mail is not delivered when a business partner's mail server does not support TLS, or if the Service fails to authenticate the certificate that the third-party recipient mail server presents when the domain uses Strong Validation. Undelivered mail is bounced back.

3.2.4 Basic Policy Based Encryption

This functionality aims to scan e-mails and attachments and is designed to automatically encrypt the messages itself which are identified as containing sensitive information. The encryption happens as from the moment it passes through the Service.

The Service allows the recipients to receive their e-mail via their mailbox or via a dedicated secure web portal (which is not a part of the Administration portal). This secure web portal can be used by the recipients to send their answers or (optionally) to send new e-mails to the End users.

The functionality is subject to the following limitations:

• The maximum amount of secured outbound e-mails per End User per month is 300 for this functionality. When sending to multiple recipients, each unique address will be counted as a separated secured outbound email. If Customer exceeds the number of permitted secure outbound e-mails in any calendar month, Proximus reserves the right to invoice Customer for actual usage.

• E-mails routed through this functionality are limited to a maximum size of fifty megabytes (50 MB), otherwise they are not encrypted.

• If using Pull encryption with Policy Based Encryption (Z) functionality, by default, e-mails will be stored for 90 Calendar days in the dedicated, secure web portal before deletion . These e-mails can be exported to save locally by the End user.

• The Availability and Latency Service Levels do not apply to Policy Based Encryption.

3.2.4.1 E-Mail Impersonation Control (EIC)

This functionality aims to protect the Customer against scams and spear phishing e-mail messages. EIC checks e-mail that is inbound to email addresses of the Validation list for username impersonation, commonly known as spoofing. Specifically, EIC checks the legitimacy of inbound e-mail that appears to be sent from the Customer organization's domains or End users.

The Administration portal is used to configure the actions to be taken on e-mail upon detection of suspected impersonation. Possible actions are:

- log
- tag the subject line
- quarantine
- redirect to Admin
- block and delete

3.3 Advanced Threat Protection (ATP)

When selected, the Advanced Threat Protection option provides the Customer with the functionalities described below:

3.3.1 Cloud-based sandboxing

To aim to detect characteristics of potential malware in an unknown file, a copy of the file is launched in a cloud-based sandbox. Then typical End-User behaviors within various operating system environments are mimicked. When necessary, the sandbox moves the execution from a virtual to a physical environment to uncover malware that is "virtual-machine-aware”. If the suspected malware remains inactive in the sandbox environment, the sandbox continues to monitor it. This way, it can later be detected if the malware later attempts to move within the environment or communicate with a control server or other computer. The sandbox correlates the data with data from the Symantec Global Intelligence Network to determine if the files are malicious. The Administrator Portal is used to determine how long the e-mail is held before it is sent, with a maximum of 20 minutes. If further analysis determines that a downloaded file contained malware, up to five specified e-mail addresses can be notified. Specifically for Customers using Office 365 it t has the ability to pullback e-mails that are determined to be malicious post-delivery.

3.3.2 Click-Time URL Protection

This functionality aims to "rewrite" and perform checks on certain URLs in e-mails that are delivered to emails addresses of the Validation list. The process of rewriting allows the Service to manage access to the URL to ensure the destination is innocuous.

Any URL that is rewritten by Click-time URL Protection is checked every time an End-user clicks on it, to ensure the URL destination is not hosting malware, phishing, or spam threats. For instance, many rewritten URLs can be checked and deemed to be free from threats. At a later date, a URL that was previously allowed might start hosting malware, phishing, or spam. At that point the Click-time URL Protection functionality blocks access to the URL and a notification is made in the Administration portal.

3.3.3 Detailed Malware Reporting

This functionality provides the Customer with granular reporting on clean and malicious e-mail entering in the Customer organization. These reports are available via the Administration Portal.

The provided reports include 60+ data points, such as:

- source URLs of an attack
- targeted attack information
- malware categorization
- sender & recipient information
- method of detection
- detailed information about file hashes
- threat category
- severity level

The reporting data is available for 12 months

3.4 Active Directory Synchronization

When selected, the Synchronization option provides the Customer with a tool to assist him in keeping his directory sources synchronized with the Platform. The tool allows a combination of the following synchronization types:

- Mail synchronization to synchronize e-mail addresses
- End User synchronization to synchronize End User identities, e-mail addresses and group memberships
- Group synchronization to synchronize group identities

The synchronization tool guides the Customer through a configuration process to extract the required data from his directory system. Once correctly configured, the synchronization process can be run either from the synchronization tool interface or from the command line. The process can be scheduled to operate automatically. The synchronization tool can also send e-mail notifications reporting its outcome at each invocation.

4. Implementation Phase

4.1 Ordering

The Customer orders the Service by submitting the relevant Order Form, duly completed and signed, to Proximus. In this Order Form, the Customer should specify the following, among other things:

- The selected Flavor
- The selected options
- The number of mailboxes to be protected
- Technical information (e.g. IP address of mail servers, mail domain)
- Information about requested quarantine model

The Technical configuration requirements document, applicable for Full Care Flavor, is annexed to the Order Form.

Any change involving a change of Service fee shall be subject to a new Order Form/Addendum.

4.2 Activation and Assist Services for Reactive Care Flavor

4.2.1 Activation

As soon as it receives the duly completed and signed Order Form (including the annexes), Proximus will start the implementation of the Service.

Only Proximus or its subcontractors are allowed to carry out the implementation activities below. All implementation activities are performed during Business Hours, after the activation has been done and according to the best practice policy. Proximus carries out the following activities when implementing the Service:

Per default the implementation of the Service consists of:

- The activation of the Platform for the ordered domains with a maximum of 5, the anti-virus and anti-spam environments are activated by default.
- Configuration of the inbound and, if ordered, outbound mail routes on the Platform;
- The creation of 1 account on the Administration Portal and providing the Customer with relevant credentials.
- The hand-over of the Service documentation and manuals.
- The creation of 1 administrator account on the Spam Quarantine Portal (if selected on the Order Form). Relevant credentials are provided.
- Backup of the configuration of the Platform
- Activation of the Service and provision of the Portal(s)

Once the Service is activated and the Customer is provisioned with the Portals linked to the Service on the Platform for the e-mail domains that were requested by the Customer, the Service will be deemed as having been made available to the Customer.
In order to avoid any misunderstandings, Proximus draws the Customer's attention to the fact that the following activities are not included in Proximus' implementation the Service, except if expressly agreed and specified in the Order Form:

- Activation of the Platform for more than 5 domain names
- Configuration of the Platform. The Customer is responsible for the configuration of the Platform via the Administration Portal. Proximus draws the attention of the Customer on the fact that the Service Level is only applicable when the following best practices settings have been configured by the Customer :
    - enable both approved sender options and keep entries on the list to a minimum where possible
    - enable spoofed sender detection with SPF – For incoming and outgoing e-mails
    - enable DMARC - for incoming and outbound emails
    - enable both blocked senders lists
    - utilize the dynamic IP block list
    - enable the signature system
    - enable skeptic heuristics - predictive spam detection
    - enable the newsletter filter extension
    - enable spoofed sender detection with SPF – for outgoing e-mails
    - enable DMARC – for outgoing emails

- The administrator can create himself other accounts for his organization and attribute fine-grained roles to these other accounts in the Administration Portal.
- Training
- Creation of security policy for the Customer
- Once the administrator account has been handed over to the technical contact of the Customer, it is the responsibility of the Customer to change the password.
- Installation and configuration of the Active Directory Synchronization tool, if ordered

4.2.2 Assist Services

In case the Customer has ordered the Assist option, the following implementation activities will be performed by Proximus in addition to the implementation activities included per default in the Reactive Care Flavor:

- Configuration of the Administration Portal of the Customer, including, if applicable, the DLP, ATP and/or AD synchronization policy, Spam Manager, according to the security policy of the Customer;
- Proximus configures the Platform not only in compliancy with the security policy of the Customer communicated by the Customer, but also with the following best practice settings:
    - enable both approved sender options and keep entries on the list to a minimum where possible
    - enable DMARC- Only for incoming mails
    - enable both blocked senders lists
    - utilize the dynamic IP block list
    - enable the signature system
    - enable skeptic heuristics - predictive spam detection
    - enable the newsletter filter extension

For the sake of clarity, even if the Customer has subscribed to this option, he stays responsible to configure the following best practice settings on his end (the Service Level is not applicable if they are not configured by the Customer):

- enable spoofed sender detection with SPF – for outgoing e-mails
- enable DMARC – for outgoing emails

4.3 Activation and Assist Services for Full Care Flavor

As soon as it receives the duly completed and signed Order Form (including the annexes), Proximus will start the implementation of the Service.

Only Proximus or its subcontractors can carry out the implementation activities below. All implementation activities are performed during Business Hours, after the activation has been done and according to the best practice policy. Proximus carries out the following activities when implementing the Service:

The implementation of the Service consists of:

- The activation of the Platform for the ordered domains with a maximum of 5. Proximus configures the Platform in compliancy with the Technical Configuration Requirements enclosed to the Order Form, the security policy of the Customer communicated to Proximus in due time, and the following best practice settings:
    - enable both approved sender options and keep entries on the list to a minimum where possible
    - enable DMARC- Only for incoming mails
    - enable both blocked senders lists
    - utilize the dynamic IP block list
    - enable the signature system
    - enable skeptic heuristics - predictive spam detection
    - enable the newsletter filter extension
    - Configuration of the inbound and, if ordered, outbound mail routes on the Platform
- The creation of 1 read-only account on the Administration Portal and providing the Customer with relevant credentials.
- The configuration of the Administration Portal of the Customer, including, if applicable, the DLP, ATP and/or AD synchronization policy, Spam Manager, according to the security policy of the Customer.
- The hand-over of the Service documentation and manuals.
- The creation of 1 administrator account on the Spam Quarantine Portal (if selected on the Order Form). Relevant credentials are provided.
- Backup of the configuration of the Platform
- Activation of the Service and provision of Portal(s)

Once the Service is activated and the Customer is provisioned with the Portals linked to the Service on the Platform for the e-mail domains that were requested by the Customer, the Service will be deemed as having been made available to the Customer.

In order to avoid any misunderstandings, Proximus draws the Customer's attention to the fact that the following activities are not included in Proximus' implementation the Service, except if expressly agreed and specified in the Order Form:

- Activation of the Platform for more than 5 domain names. The activation and configuration of additional domains can be requested via change credits.
- Configuration of the following best practices settings parameters on the Platform (the Service Level is only applicable when they are configured by the Customer):
  - ➢ enable spoofed sender detection with SPF – For incoming and outgoing e-mails
  - ➢ enable DMARC - outbound emails
- Training
- Creation of security policy for the Customer
- Once the administrator account has been handed over to the technical contact of the Customer, it is the responsibility of the Customer to change the password.

4.4 Acceptance

At the end of implementation phase, Proximus will invite the Customer to do an acceptance of the configuration of the Platform. In this regard, the Customer can check the configuration of implemented via the Administration Portal.

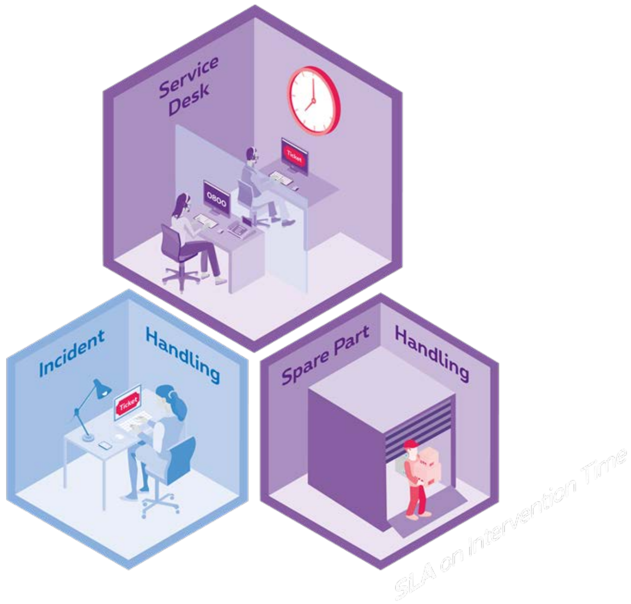
The acceptance procedure is described in the General Terms and Conditions for Professional Customers (see Article Configuration and installation).

5. Operational Phase

This chapter describes the support provided by Proximus as from the acceptance of the Service until the end of the Agreement.

5.1 Reactive Care Flavor

This section is applicable when the Customer has selected the Reactive Care Flavor. In such Flavor, the Customer benefits from a **Reactive Care** support meaning Proximus provides it with a reactive support to shorten Incidents by interventions and replacements.



5.1.1 Service Desk Access

The Service Desk is the interface between the Customer and Proximus for all aspects of the Service, including receiving, recording, registering and escalating Incidents and other requests. The Service Desk allocates resources (first line, second line, experts) and communicates regularly with the Customer.

Proximus provides the Customer with centralized Service Desk Access via phone or portal. The Service Desk is only accessible to authorized Customer representatives (24x7) every day of the year via:

Service Desk Access	
Phone	0800 14888
Portal	https://www.proximus.be/login

The Customer provides the Service Desk with the relevant Agreement reference number in question.

The Customer is informed of, accepts and gives his consent for calls originating from or made to Proximus Service Desk to be recorded in order to serve as proof in case of a contested commercial transaction. Calls to or from the Customer Service may also be listened in on or recorded for quality control purposes.

5.1.2 Incident Handling

The activities related to Incident handling carried out by Proximus aim at resolving or diminishing the consequences of an Incident within the agreed Service Level.

Remote activities means activities performed by Proximus not on the Customer's Site.

5.1.2.1 Remote Diagnostics

The main goal of Remote Diagnostics is to assess the cause and validate the impact of the reported Incident, via phone or e-mail. The Customer analyzes the Incident before contacting Proximus.

Proximus will assist the Customer to perform some basic troubleshooting actions. In some cases, the Customer will be requested to provide Proximus with additional information. Incidents due to the configuration of the Solution element (even of the Solution element in scope for this service component) are not supported by Proximus.

Remote Diagnostics allows Proximus to determine which actions should be taken to solve the Incident.

5.1.2.2 Remote Intervention

In case Remote Diagnostics shows a Software issue on Synchronization Tool, a remote intervention is started and includes checking with the vendor on availability of patches/Updates and suggesting these to the Customer. The Customer takes care of the installation of the patches/Updates. The installation of a patch/update, is not included in the Service fee. Incidents due to the configuration of the solution elements (even of the solution element in scope for this service component) are not supported by Proximus.

In case Remote Diagnostics shows an issue on the Platform and/or Administration Portal and/or - Spam Quarantine Portal, interventions will be performed by Proximus on these Solution elements.

5.1.2.3 Configuration Restore

In addition to the Remote Interventions, Proximus, if required for Service restoration purposes, Proximus will seek to restore the Configuration of the Solution element in scope, based on the last available configuration backup performed by Proximus.

In this regard, Proximus will use reasonable efforts to backups of the Solution element configuration in scope, and make them available for restore purposes in case of Incident. The first backup is made during the implementation phase.

Unless otherwise agreed in writing between parties, the backups are scheduled to be performed daily and to run at night. The backup of the configuration consists of logs of configuration changes since the implementation phase, metadata available via the Administration tool and mails in quarantine. The configuration backup performed by Proximus does not include backup of any other Customer's data.

5.1.3 Updates and Upgrades

Proximus alone shall determine the technical means necessary to provide the Service in compliance with the Agreement.

Proximus decides to implement Updates/Upgrades at its own discretion. Proximus has no obligation to implement each Upgrade and Update made available by the vendor, or to extend the Solution element in the scope. Taking to account the fact that the Service is based on a Cloud Platform, such Updates/Upgrades cannot be refused by the Customer.

5.1.4 Configuration Backup

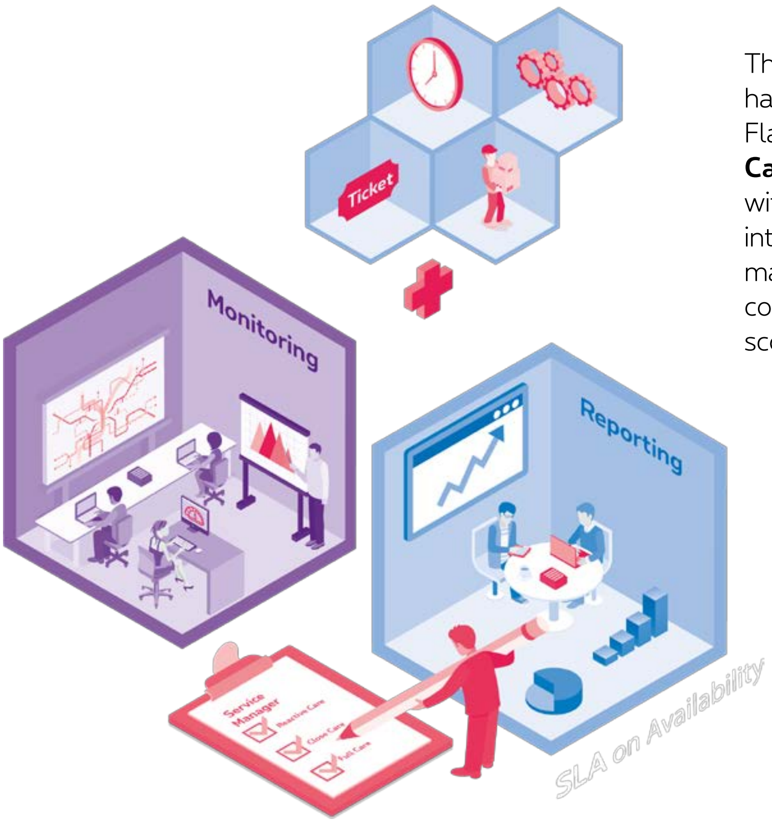
Proximus will use reasonable efforts to backups of the Solution element configuration in scope, and make them available for restore purposes in case of Incident.

The first backup is made during the implementation phase.

Unless otherwise agreed in writing between parties, the backups are scheduled to be performed daily and to run at night. The backup of the configuration consists of logs of configuration changes since the implementation phase, the data available via the message tracing functionality and the mails in quarantine.

The configuration backup performed by Proximus does not include backup of any other Customer's data.

5.2 Full Care Flavor



This section is applicable when the Customer has selected the Full Care Flavor. In such Flavor, the Customer benefits from a **Full Care** support meaning Proximus provides it with a reactive support to shorten Incidents by interventions and replacements and management, monitoring and reporting of the configuration of the Solution elements in scope.

5.2.1 Service Desk Access

The Service Desk is the interface between the Customer and Proximus for all aspects of the Service, including receiving, recording, registering and escalating Incidents and other requests. The Service Desk allocates resources (first line, second line, experts) and communicates regularly with the Customer.

Proximus provides the Customer with centralized Service Desk Access via phone or portal. The Service Desk is only accessible to authorized Customer representatives (24x7) every day of the year via:

Service Desk Access	
Phone*	0800 14888
Portal	https://www.proximus.be/login

The Customer is informed of, accepts and gives his consent for calls originating from or made to Proximus Service Desk to be recorded in order to serve as proof in case of a contested commercial transaction. Calls to or from the Customer Service may also be listened in on or recorded for quality control purposes.

.

5.2.2 Incident Handling

The activities related to Incident handling carried out by Proximus aim at resolving or diminishing the consequences of an Incident within the agreed Service Level.

Remote activities mean activities performed by Proximus not on the Customer's Site.

5.2.2.1 Remote Diagnostics

The main goal of Remote Diagnostics is to assess and analyze the reported Incident, determine the cause and validate the impact of the Incident – either verbally, or by accessing the Customer environment via a remote connection.

Proximus will take all necessary actions to pinpoint the cause of the error and location of the failing component. This includes identifying issues with configuration files and performance issues.

Remote Diagnostics allows Proximus to determine which actions should be taken to solve the Incident.

5.2.2.2 Remote Intervention

In case a workaround or permanent solution has been identified and provided that the Incident can be solved, Proximus will start a remote intervention in close collaboration with the Customer. The Customer is informed about the progress on a regular basis.

Proximus restores the configuration of the Solution element in scope based on the latest available configuration backup.

5.2.3 Configuration Handling

The Configuration Handling activities performed by Proximus under the Agreement aim to, within the limitation defined in this section:

- Manage the configuration of the Solution elements in scope
- Backup the configuration of the Solution element in scope
- Implement Changes on the configuration of the Solution elements in scope
- Keep the Software in scope up to date

5.2.3.1 Access and Configuration Handling

This section defines the access management rights held by Proximus and the Customer related the Solution element in scope of this service component.

5.2.3.1.1 Configuration Handling with Customer Read Access

Proximus collects and documents up to date information about the Solution element and makes use of planned and in some cases automated processes aiming to keep the Solution element up to date.

Proximus performs actions aiming to keep the Solution element working in good order. In this regard, Proximus uses a secure and central management platform with access rights. To allow faster troubleshooting all platform activity is recorded.

Proximus is the holder of all administrator rights on the Solution element, on behalf of the Customer, even in case the said Solution element is owned by the Customer. The Customer has Read Access rights for the Solution elements in scope. Authorized Customer representatives have access to this Solution element configuration via the same secure and central management platform with read-only rights.

5.2.3.1.2 Configuration Handling with Specific Access Rights

Proximus collects and documents up to date information about the Solution element and makes use of planned and in some cases automated processes aiming to keep the Solution element up to date.

Proximus performs actions aiming to keep the Solution element in scope working in good order. In this regard, Proximus uses a secure and central management platform with access rights. To allow faster troubleshooting all platform activity is recorded.

Proximus is the holder of all administrator rights, on behalf of the Customer, of the Solution element in scope, even in case the Customer is owner of the Solution element. The Customer has specific access rights to make limited Changes. Authorized Customer representatives have access to this Solution element configuration via the same secure and central management platform with limited rights.

The Customer is entitled to make only the following changes to the Solution elements in scope:

- Creating accounts
- Creating account groups
- Creating aliases
- Accessing different accounts
- Deleting accounts

Proximus shall not be liable for any consequences of any Changes made by the Customer or third parties.

5.2.3.1.3 Configuration Handling without Access Rights

Proximus collects and documents up to date information about the Solution element in scope and makes use of planned and in some cases automated processes seeking to keep the Solution element up to date.

Proximus performs actions aiming to keep the Solution element in scope working in good order. In this regard, Proximus uses a secure and central management platform with access rights. To allow faster troubleshooting all platform activity is recorded.

Proximus is holder of all administrators' rights on the Solution element in scope, on behalf the Customer, even in case the said Solution element is owned by the Customer. The Customer has no access nor administration rights and is not authorized to make any Changes to the Solution element or interfaces.

5.2.3.2 Configuration Backup

Proximus will use reasonable efforts to backups of the Solution element configuration in scope, and make them available for restore purposes in case of Incident.

The first backup is made during the implementation phase.

Unless otherwise agreed in writing between parties, the backups are scheduled to be performed daily and to run at night. The backup of the configuration consists of logs of configuration changes since the implementation phase, the data available via the message tracing functionality and the mails in quarantine.

The configuration backup performed by Proximus does not include backup of any other Customer's data.

5.2.3.3 Change Handling

Change Handling aims at providing the Customer with the opportunity to request changes on the Solution element configuration during the Agreement. These changes have no impact on the recurring Service fee.

There are two types of changes: Standard and Custom Changes. To be able to request these changes, the Customer has to have a separate Change Handling Agreement.

Any change involving a change of Service fee shall be subject to a new Order Form or an Addendum.

5.2.3.4 Updates and Upgrades

Proximus alone shall determine the technical means necessary to provide the Service in compliance with the Agreement.

Proximus decides to implement Updates/Upgrades at its own discretion. Proximus has no obligation to implement each Upgrade and Update made available by the vendor, or to extend the Solution element in the scope. Taking to account the fact that the Service is based on a Cloud Platform, such Updates/Upgrades cannot be refused by the Customer.

5.2.4 Monitoring

The monitoring activities performed by Proximus under this Agreement allow Proximus to collect status information on the Solution elements in scope on a 24x7 basis. When a relevant event (as described below) is detected, Proximus will initiate Incident handling activities. Customers are notified by the creation of an Incident ticket.

Under the Agreement, Proximus performs the following monitoring activities:

5.2.4.1 Service Availability Monitoring

The central monitoring platform checks the availability of the Service in scope. Service availability checks include verifying if relevant applications or processes are still up and running.

Incident handling activities are started in case service availability issues are detected.

5.2.5 Reporting

Proximus provides the Customer with reports based on information collected via the performed monitoring activities under this Agreement. Status on relevant parameters can be viewed by the Customer via the link mentioned in the Service documentation.

The report provided by Proximus under the Agreement are the following:

5.2.5.1 Service Availability Reporting

This provides reporting based on the Service Availability Monitoring

6. Service Levels

This section describes the Service levels applicable. The Service Levels includes Service Level Objective (SLO) and Service Level Agreement (SL A). They are described in the tables below.

6.1 Scope

These Service Levels are applicable when the Service has been activated and the credentials are received within the Service windows set out below.

The Service Levels shall only apply to the Service described in this document and to Incidents for which Proximus is responsible.

Are excluded from the calculation of the Service Level (application of the "stop clock" principle):

- Incidents, delays or events prohibiting Proximus from providing the Service due to the Customer, Force majeure event, or to a third party, and
- time outside the Servicing Window, and
- E-mails that have not passed through the Service if Customer has not taken appropriate steps to ensure that it will only accept inbound e-mail from the Service, and
- inbound or outbound e-mails that were initially sent to the Service containing more than 500 recipients per SMTP session and
- planned works (including maintenance interruption), and
- Customers provisioned on any Tower designated as a Bulk Cluster Tower (i.e. two or more load balanced servers in two or more locations);
- any inbound or outbound e-mails for emails addresses not included in the Validation list and,
- If the best practice settings which have to be implemented by the Customer such as defined in the implementation phase Chapter haven not been configured or have not been maintained throughout term of the Agreement (see also Annex 1). This is valid for all items of the Service Level.

No Service Levels are applicable for on-demand support.

6.2 SLO and SLA

The SLO defines obligation of means (obligation de moyen/middelenverbintenis). Therefore, the breach of these SLO cannot be regarded as a material breach. In case of breach, no Service credit can be claimed.

The SLA defines obligation of result (obligation of résultat/resultaatsverbintenis). In case of breach the Customer is entitled to Service Credits listed in the table below from Proximus. Unless the Customer has subscribed to a Service Management Agreement, the Customer must claim these Service Credits itself, as Proximus does not provide them proactively.

In order for the Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted in writing to Proximus within three within 5 Business days of the end of the calendar month in which the suspected service level non-compliance occurred. The Service credits are the sole remedy for any failure by Proximus to meet this SLA.

The Customer will not be eligible to receive Service Credits if (1) the Customer is in failure to pay its Proximus invoices related to this Agreement or another contract or (2) the Customer is in violation of the Agreement during the time of the Incident or event. If the Agreement expires or is terminated prior to the issuance of the Service Credit, the Service Credit will become void as of the date of the expiration or termination of the Agreement.

6.3 Service windows

Service levels are applicable within the following Service window.

The Service Window is the timeframe during which Incident handling activities are carried out

Service Window Name	*Acronym*	*Applicable on*	*Service Window Hours*
*24*7*	24*7	*All Solution Elements*	*24*7*

6.3.1 Standard Change Implementation Window

The Change Implementation Window is the window during which Standard Changes in the scope of this Service will be executed. The Standard Change Implementation Window is:

Standard Service Hours	SSH	*Monday-Friday 8:00-18:00*

6.4 Incident Priority

In case the Customer detects an Incident, the Customer can contact the Service Desk. The Service desk will assign the Incident priority based on the impact of the Incident.

Priority definitions	
P1*	Service completely interrupted
P2	Service severely degraded (critical business functions) or backup active
P3	Limited impact (business processes can continue)

P4	No impact/request for info

In case, after diagnosis, the impact of the Incident does not correspond with the impact mentioned by the Customer at ticket creation Proximus will correct the assigned Incident priority.

*P1 Incidents should be logged by contacting the Service desk by phone only

6.5 Service Level Description

6.5.1 Reactive Care Flavor

SLA KPI	Definition	Applicable on	Target	Valid for	Service Credits
Incident Response Time	The time inside the agreed Servicing Window between the ticket creation and the start of the troubleshooting by Proximus, minus all time as a result of an event for which the stop-clock principle is applicable.	Remote Diagnostics for all Solution Elements	30 mins	P1 Incidents	10% of the Monthly Fee for each validated P1 Incident with breached SLA, with a maximum of 25% of the Monthly Fee
Antispam Efficacy	The Service Level corresponds to the rate of captured Spam as a percentage of all e-mail traffic, sent to a valid e-mail address of the Validation list. This SLA will	Administration Portal Spam Quarantine Portal	>99%	N/A	98%> X ≥ 99%: 5% 97%> X ≥98%: 10% 96%> X ≥97%: 15% 96%> X: 20%

	only apply if Customer has implemented and maintained the Antispam Best Practice Settings as provided in the Appendix 1.				of the Monthly Fee
Antispam Accuracy	This Service Level defines the maximum rate of Spam False Positives as a percentage of all e-mail traffic to and if configured from a valid email address of the Validation list This SLA will only apply if Customer has implemented and maintained the Best Practice Settings as provided in the Appendix 1 The following e-mails do not constitute Spam False Positive e-mails for the purposes of this service level: a) E-mails that are not legitimate business e-mail; b) E-mails containing	Administration Portal Spam Quarantine Portal	≤0.0003%	N/A	0.0003%< X ≤ 0.003%: 5% 0.003%< X ≤ 0.03%: 10% 0.03%< X ≤ 0.3%: 15% 0. 3%< X: 20% of the Monthly Fee

	more than 20 recipients; c) E-mails where the sender of the e-mail is on Customer's blocked senders list, including without limitation, those defined by the individual user if Customer has enabled user-level settings; d) E-mails that are sent from a compromised machine; e) E-mails that are sent from a machine which is on a third-party block-list; f) E-mails intercepted by outbound Spam scanning.				
Antivirus Efficacy	Number of registered virus infections which entered via the Service and were confirmed by Proximus.	Administration Portal Platform	0 per calendar month or in the event that a virus sent via e-mail as an attachment and this is detected and not stopped, the Customer is notified sufficiently to identify and delete the infected e-mail.	N/A	100% of the Monthly Fee with a maximum of 5.000 EUR
AntiVirus Accuracy	This Service Level defines the maximum Virus False Positive Capture Rate as a percentage of	Administration Portal Platform	≤0.0001%	N/A	0.0001%< X ≤ 0.001%: 5% 0.001%< X ≤ 0.01%: 10%

	all e-mail traffic to and if configured from the valid e-mail addresses of the Validation list.				0.01< X ≤ 0.1%: 15% 0.1%< X: 20% of the Monthly Fee
E-mail Latency	The E-mail Latency Service Level is defined by the average round trip time, as measured by the Symantec.cloud Tracker, for e-mails sent every five (5) minutes to and from the Service.	Administration Portal Platform	60 seconds average roundtrip time per calendar month	N/A	60 seconds< X ≤ 90 seconds: 5% 90 seconds< X ≤120 seconds: 10% 120 seconds< X ≤150 seconds: 15% 150 seconds< X: 20% of the Monthly Fee

The total amount of the Service credits granted to the Customer under this Agreement in connection with any of SLA in any calendar month will not exceed the monthly fees paid by Customer for the Service, unless specified differently.

SLO KPI	Definition	Applicable on	Target
Incident Ticket Creation Time	The time between the Incident notification (via the Service) and the creation of an Incident ticket in the ticketing system.	Service Desk Access for all Solution Elements	15 minutes
Incident Response Time	The time inside the agreed Servicing Window between the ticket creation and the start of the troubleshooting by Proximus, minus all time as a result of an event for which the stop-clock principle is applicable.	Remote Diagnostics for all Solution Elements	1 hour

6.5.2 Full Care Flavor

SLA KPI	Definition	Applicable on	Target	Valid for	Service Credits
Incident Response Time	The time inside the agreed Servicing Window between the ticket creation and the start of the troubleshooting by Proximus, minus all time as a result of an event for which the stop-clock principle is applicable.	Remote Diagnostics for all Solution Elements	30 mins	P1 Incidents	10% of the Monthly Fee for each validated P1 Incident with breached SLA, with a maximum of 25% of the fee
Service Restoration Time	The Service restoration time is defined as the time between the creation and the resolution of an Incident on the Solution element, within the agreed Servicing Window and minus all time as a result of an event for which the stop clock principle is applicable.	Remote Intervention for all Solution Elements	4 hours	P1 Incidents	25% of the Monthly Fee for each validated P1 Incident with breached SLA, with a maximum of 50% of the Monthly Fee
Yearly Service Availability	The service availability is computed as follows: 100*(1 – Net Downtime/Total Time (24x7)) = Service Availability % Net Downtime is the time during which a Solution element is not available during the Servicing Window as a result of a P1 incident minus all time as a result of an	Service Availability for the Platform	99,95%	P1 Incidents	25% of the Monthly Fee for each validated P1 Incident with breached SLA, with a maximum of 50% of the recurring fee

	event for which the stop clock principle is applicable, and where Total Time is the time period over which the Availability is calculated. For this Service, the Service Availability Service Level is defined by the ability to establish an SMTP session on port 25 from the Customer MTA to the Service Infrastructure, in compliance with RFC5321. This service level shall not apply if the Customer has incorrectly configured the Service (cfr. the best practices setting in the Annex 1)				
Standard Change implementation time	Time for the implementation of Standard Changes, calculated as from the registration of the Request for Standard Change (time of Change Ticket Creation) until the end of its execution by Proximus (Change Ticket Closed).	Standard Changes	>95% executed in 3 Business days	N/A	95> X ≥ 90%: 5% 90> X ≥ 80%: 10% 80% > X : 25% of the Monthly Fee Bundle of the Change Credits
Antispam Efficacy	The Service Level corresponds to the rate of captured Spam as a percentage of all e-mail traffic, sent to a valid e-mail address. This SLA will only apply if Customer implements and maintains the Best Practice Settings as provided in the Appendix 1.	Administration Portal Spam Quarantine portal	>99%	N/A	98%> X ≥ 99%: 5% 97%> X ≥98%: 10% 96%> X ≥97%: 15% 96%> X: 20% of the Monthly Fee

AntiSpam Accuracy	This Service Level defines the maximum rate of Spam False Positives as a percentage of all e-mail traffic. This SLA will only apply if Customer implements and maintains the Best Practice Settings as provided in the Appendix 1. The following e-mails do not constitute Spam False Positive e-mails for the purposes of this service level: a) E-mails that are not legitimate business e-mail; b) E-mails containing more than 20 recipients; c) E-mails where the sender of the e-mail is on Customer's blocked senders list, including without limitation, those defined by the individual user if Customer has enabled user-level settings; d) E-mails that are sent from a compromised machine; e) E-mails that are sent from a machine which is on a third party block-list; f) E-mails intercepted by outbound Spam scanning.	Administration Portal Spam Quarantine portal	≤0.0003%	N/A	0.0003%< X ≤ 0.003%: 5% 0.003%< X ≤ 0.03%: 10% 0.03%< X ≤ 0.3%: 15% 0. 3%< X: 20% of the Monthly Fee
Antivirus Efficacy	Number of registered virus infections which entered via the Cloud Mail Security Service and were confirmed by Proximus.	Administration Portal	0 per calendar month or in the event that a virus sent via e-mail as an attachment and this	N/A	100% of the Monthly Fee with a maximum of 5.000 EUR

			is detected and not stopped, the Customer is notified sufficiently to identify and delete the infected e-mail.		
AntiVirus Accuracy	This Service Level defines the maximum Virus False Positive Capture Rate as a percentage of all e-mail traffic.	Administration Portal	≤0.0001%	N/A	0.0001%< X ≤ 0.001%: 5% 0.001%< X ≤ 0.01%: 10% 0.01< X ≤ 0.1%: 15% 0.1%< X: 20% of the Monthly Fee
E-mail Delivery	The E-mail Delivery Service Level is defined by the percentage of all e-mails sent to or from Customer subject to the following conditions: a) The e-mail must have been received by the Service; and b) The e-mail must not contain a Malware, Spam or other content which has caused it to be intercepted by the Service.	Administration Portal Platform	100%	N/A	Customer can terminate the Service upon prior written notice.
E-mail Latency	The E-mail Latency Service Level is defined by the average round trip time, as measured by the Symantec.cloud Tracker, for e-mails sent every five (5) minutes to and from the Service.	Administration Portal Platform	60 seconds average roundtrip time per calendar month	N/A	60 seconds< X ≤ 90 seconds: 5% 90 seconds< X ≤120 seconds: 10% 120 seconds< X ≤150 seconds: 15% 150 seconds< X: 20% of the Monthly Fee

The total amount of the Service credits granted to the Customer under this Agreement in connection with any of SLA in any calendar month will not exceed the recurring fees paid by Customer for the Service.

SLO KPI	Definition	Applicable on	Target	Valid for	Service Credits
Incident Ticket Creation Time	The time between the Incident notification (via the Service) and the creation of an Incident ticket in the ticketing system.	Service Desk Access for all Solution Elements	15 minutes	P1 and P2 Incidents	None
Incident Response Time	The time inside the agreed Servicing Window between the ticket creation and the start of the troubleshooting by Proximus, minus all time as a result of an event for which the stop-clock principle is applicable.	Remote Diagnostics for all Solution Elements	30 mins	P2 Incidents	None
Service Restoration Time	The Service restoration time is defined as the time between the creation and the resolution of an Incident on the Solution element, within the agreed Servicing Window and minus all time as a result of an event for which the stop clock principle is applicable.	Remote Intervention All Solution Elements	6 hours	P2 Incidents	None

7. Specific Terms and Conditions

7.1 General information

7.1.1. The Specific Terms and Conditions complement the General Terms and Conditions for Professional Customers and this Contractual Service Description. They set out the rights and obligations of Proximus and Customer with regard to the provision of the Service described in this document.

7.1.2. The Service is only available to a Customer who has its own email domain name and has the ability to configure the MX records and/or DNS for that domain name.

7.2 Agreement procedure

7.2.1 Term

As deviation to the General Terms and Conditions, the Agreement has been concluded for an indefinite term as from the activation of the Service.

7.2.2 Termination and Termination effects

7.2.2.1 As deviation to the General Terms and Conditions, the Customer can terminate the Agreement at any time in writing. If notice of termination is received by Proximus at the latest on the 15th of the month underway, the Agreement shall effectively terminate on the last calendar day of the month underway. If notice is received by Proximus after the 15th of the month underway, the Agreement shall effectively terminate on the last day of the following month. Proximus is entitled to invoice and be paid for the Service provided up to the date of termination is effective.

7.2.2.2. Upon termination of this Agreement, Proximus disables the Service and any account provisioned as part of the Service. The configuration changes made to the provisioning of the Service are reversed. Upon termination of the Agreement, the Customer shall stop using the Service, destroy all documentation received from Proximus along with any copies, including partial copies, of the Software made available to the Customer in the framework of the Service. The Customer shall certify that the Software has been purged from all devices, computer memories and storage devices within the Customer’s control and that the documentation has been destroyed. The customer shall make the necessary configuration changes to restore his environment to the original state.

7.2.2.3. The content hosted by Proximus in the framework of this Service (meaning emails in quarantine, data available via the message tracing function and the log of configuration) will no longer be available after the Service has been terminated, regardless of the reason therefore. Consequently, before the termination of the Agreement, the Customer must take the necessary measures to export his content via the Administration Portal (upon specific request to Proximus malware can be exported).

7.2.3 Suspension

7.2.3.1. In case of a Service suspension, the regular fee for the Service shall be payable by the Customer. In addition, Proximus shall be entitled to request a reactivation fee.

7.2.3.2. Should the Service be suspended for any reason whatsoever, the Service will not be applied to the Customer inbound e-mails (and outbound emails if ordered). These emails will not be routed through the Platform. Customer is responsible for redirecting its emails during the suspension and confirming that all configurations are accurate if the Service is reinstated.

7.2.4 Upsize and Downsize

7.2.4.1. The Customer may increase the number of the email addresses in scope of the Agreement at any time during the Term. Any requests in writing from the Customer to increase the number of email addresses, will be implemented and invoiced as from the date they are registered by Proximus.

7.2.4.2. The Customer may decrease the number of the emails address in scope of the Agreement at any time during the Term. Without prejudice to the minimum numbers of emails addresses required mentioned in the Agreement, any written request to decrease the numbers of mailbox will be implemented and invoiced as from the first day of the next month, provided that the request is registered by Proximus by no later than the 15th of the month underway. If the request is registered by Proximus after the 15th of the month underway, the request will be implemented and invoiced as from the first day of the next month.

7.2.4.3. If certain specific measures are necessary to enable the downsize and/or the upsize to be implemented, Proximus will inform the Customer. The Customer shall perform such measures within the timeline given by Proximus. The Customer agrees that if he fails to do so, Proximus will not be able to implement the Customer's request. The month in question will then be invoiced on the basis of the previously applicable rules.

7.3 Right to use

7.3.1. Subject to the terms and conditions of the Agreement and provided that the Customer pays the Service fee, Proximus will grant the Customer, as from the Service activation date and for the Term of the Agreement, a non-transferable, non-sublicensable, non-perpetual and non-exclusive right to access, use and/or benefit from the Service.

7.3.2. The Customer uses the Service in compliance with the Agreement and the acceptable use policy published by the supplier of Proximus (Symantec) on the following link https://www.symantec.com/content/dam/symantec/docs/eulas/policy/online-services-acceptable-use-policy-v6-en.pdf (or any subsequent link) and up to the maximum quantities for which it has been ordered. Failure to comply with or breach of the acceptable use policy constitutes a breach of the Agreement. Proximus reserves the same right than its supplier.

7.3.3. The Customer shall not copy or use the Service or authorize or permit any third party (including any End User), to copy or use the Service or any portion thereof, except as expressly authorized by this Agreement; use the Service on any unauthorized equipment or products; use the Service in any way that may damage, impair or disable the operation of the Service; modify the Service, translate or create derivative works based on the Service, reverse engineer or decompile, decrypt, disassemble or reduce the Service to human-readable form, except as allowed by law; alter or remove any proprietary notices or legends contained in or on the Service; use the Service in breach of other parties' rights. The Service includes any Portal and Software put at the Customer's disposal in the framework of the Agreement

7.4 Amendment to the Agreement

7.4.1. Proximus is entitled to revise the Service and the Agreement at any time, without prior notification for the following reasons: (i) it becomes necessary due to applicable law or industry standards; (ii) it becomes necessary for technological reasons when any change is made without materially degrading the functionality of the Service; (iii) it become necessary to maintain the operation of the Service when any change is made without materially degrading the functionality of the Service; or (iv) changes in favor of the Customer. By continuing to use the Service, the Customer agrees to these changes.

7.4.2. In other cases, the procedure described in the General Terms and Conditions for Professional Customers shall be applicable.

7.5 The Customer rights and obligations

7.5.1. The Customer will designate one or more individuals who possess the appropriate skills, knowledge and/or experience to oversee the Service, evaluate the adequacy and results of the Service, and accept responsibility for the results of the Service.

7.5.2. The Customer shall ensure that only authorized persons are granted access to the Service and secure portals placed at its disposal under this Agreement. Without prejudice to the General Terms and Conditions for Professional Customers, the Customer shall comply with any security or technical standards imposed by Proximus from time to time to connect with the Service. Proximus cannot verify whether access requests and the use of the Service are legitimate and declines any responsibility for any consequences resulting from fraudulent or erroneous access and use. The Customer shall immediately inform Proximus in writing of any changes to the identification data of the authorized persons.

7.5.3. The Customer shall duly and promptly report any Incidents concerning the Service and any technical or operational changes that may affect Proximus' provision of the Service. He must make sure, however, that the Incident is not caused by himself, his employees or his own equipment.

7.5.4. The Customer ensure that its systems do not (1) act as an Open Relay (means an email server configured to receive email from an unknown or unauthorized third party and forward the email to one or more recipients that are not user of the email system to which that email server is connected), (2) act as Open Proxy (means an a proxy server configured to allow unknown or unauthorized third parties to access, store or forward DNS, web pages or other data for the Service), (3) send Spam (means unsolicited commercial email), (4) send or receive Bulk email (means a group of more than five thousand (5000) email messages with substantially similar content sent or received in a single operation or a series of related operations, or (5) compromise the security of Service (without limitation, to hacking attempts, denial of service attacks, mail bombs or other malicious activities either directed at or originating from the Customer's domain). Proximus reserves the right at any time to review Customer's compliance with this article. Such acts shall be deemed as compromising the integrity and proper functioning of the Service and the infrastructure underlying the Service. It is the same if the Customer's email systems are blacklisted or Customer causes the Proximus systems (or the systems of its Supplier) to become blacklisted due to the sending of Spam. Without prejudice to the General Terms and Conditions for Professional Customers, Proximus reserve the right to charge the Customer at then current rates for any remedial work.

7.5.6. The Customer provides and maintains throughout the Agreement a correct, accurate and exhaustive list of all e-mail addresses (including aliases) to receive the Service (the 'Validation list'). These e-mail addresses have to be linked to domain mentioned in the Order form. Inbound and outbound e-mail sent to or from e-mail addresses which are not specified in the Validation list or incorrectly entered, will be blocked automatically. Proximus accepts no liability due to the non-delivery of such email resulting from errors in or omissions of email addresses. Service Levels shall not be applied to invalid e-mail addresses. In case of Reactive care Flavor, the Customer himself enters the Validation list in the Administration Portal whereas in case of Full care Flavor, the Customer provides Proximus with the Validation list to be entered in the Administration Portal by Proximus.

7.5.7. The Customer expressly acknowledges having received from Proximus all the information he could reasonably expect to allow him to check, prior to the conclusion of the Agreement, that the Service meets his needs and requirements.

7.5.8. The Customer acknowledges and agrees that Proximus has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitation of liability set forth herein; the same reflect an allocation of risk between the Parties and form an essential basis of the bargain between the Parties.

7.5.9. Customer agrees not to use the Service for the purposes of building a competitive product or service or copying its features or user interface, performing Service evaluations, benchmarking or other comparative analysis intended for publication outside Customer organization without Proximus' prior written consent.

7.5.10. The Customer acknowledges and agrees that the Service (and applicable solution elements) and any related download or technology ('Controlled Technology') may be subject to applicable export control and trade sanction laws, regulations, rules and licenses, and that the Customer is on notice of the information published by Proximus' supplier (Symantec) on http://www.symantec.com/about/profile/policies/legal.jsp (or successor website) and will comply with the foregoing and with such further export restrictions that may govern the Service.

7.6 Proximus rights and obligations

7.6.1. The Customer acknowledges and accepts that the Service is a standard service which has not been designed to explicitly meet his particular business needs or expectation. Consequently, Proximus cannot be held responsible for non-compliance with any objectives the Customer may have set with regard to the Service. Moreover, the Customer acknowledges and accepts that Proximus has no obligations other than those exhaustively enumerated in this Agreement.

7.6.2. No Service can guarantee a 100% detection of malware or undesirable content (such as spam, image pornographic, content including specific predefined words, blocked URL etc.) or a 100% protection against unauthorized third-party access. Although the Service is specially designed to protect the network and, the internet traffic of the Customer against such security threats or undesirable content, Proximus gives no guarantee on the ability of the Service to detect, correct or protect against all such undesirable content, unauthorized third-party access and security threats. Proximus disclaims any liability for any damage or loss resulting directly or indirectly from any failure of the Service to detect such security threat or undesirable content or for wrongly identifying an email of content as suspected which proved subsequently not to be so or prevent unauthorized third-party access. In compliancy with the General Terms and Conditions, Proximus is subject to an obligation of means in this respect. In addition, without prejudice the Service Level Chapter, Proximus does not warranty an uninterrupted Service.

7.6.3. The maintenance activities covered by this Agreement are described in the Chapter Operational Phase. Replacement, repair of the affected Solution element or any other Proximus intervention is not included in the Service (however, if delivered, the intervention shall be invoiced separately at the current applicable rate) when (i) the Incident is due to any use or events outside the normal operating conditions of the affected Solution element, (ii) On-demand support is provided; (iii) support activities relating to Software and/or Hardware are not supported by the manufacturer any more, (iv) the Incident is due to:

a. external causes including but not limited to weather conditions, shut-off or cut communication lines that are not included in the Service, breakdowns of the air conditioning, poorly functioning sockets, storms, lightning strikes, floods, and all other causes alien to the Solution element, inappropriate environmental factors such as too high humidity, abnormal temperatures or an abnormally high amount of dust
b. use of the affected Solution element not authorized by the Agreement and any prescription given by Proximus
c. the use with or connection of affected Solution element to items not approved by Proximus or the irregular operation of the item to which the Solution element is connected;
d. the performance (or the attempting) of maintenance, a move, a repair, a modification or a change to the affected Solution element by persons other than Proximus or as authorized by Proximus without the prior written consent of Proximus
e. negligence or fault (by act or omission) by the Customer or third parties in using or setting up Solution element;
f. the failure of the Customer to respect his obligations as stipulated in this Agreement;

7.6.4. As deviation to the General Terms and Conditions, in case Proximus is held liable for loss of or damage to the hosted Customer's data, Proximus' liability shall be limited, at the Proximus discretion, per event to replicate the data from the last available backups made by Proximus in the framework of the Service or the amount (excluding all one-time fees) that the Customer paid to Proximus for the Service over the month preceding the cause of the damage.

7.6.5. Proximus disclaims any liability for losses, damages, costs and expenses the Customer or a third party may occur as a result of (i) a release by the Customer (or by Proximus under Customer's instruction) of virus infected email or any email put in quarantine, (ii) the deletion by the Customer of email put in quarantine, (iii) malfunctioning of the Service following an intentional or unintentional change made by the Customer or a third party, or (iv) a breach of the security system (fraudulent operation or attack) by any person whatsoever (with the exception of Proximus employees). In case of Customer's fault or neglect, it shall hold Proximus harmless from claim, complaint or action by a third party (included the Customer's own customers, End Users or suppliers) in this respect.

7.6.6. Proximus cannot be held liable for damage, interruption or errors in the mail traffic of the Customer following or due to the provisioning, suspension or termination of the Service or due to the consequence of Force majeure.

7.7 Payment and billing

7.7.1 The Service will be invoiced monthly and appear on the same invoice as the potential Proximus telecom services to which the Customer has subscribed (excluding mobile services). All these telecom services will be invoiced monthly regardless of when these services have been subscribed. The Customer acknowledges and accepts that the ordering of the Service may impact the periodicity of its billing cycle and the invoice issue date for its Proximus telecom services.

7.7.2. The regular fee for the Service will be invoiced to the Customer in advance (except for the first billing cycle) according to the price table mentioned in the Order form and depending on the emails addresses in the scope of the Agreement.

All other fees (including, but not limited to, activation, installation, configuration, usage (in case of pay-as-you-use), deactivation, reactivation, specific support, etc.) shall be invoiced in arrears.

The Customer acknowledges and accepts that his invoices are based on the measurements performed by Proximus' (or its suppliers') systems for the billing cycle concerned.

7.73. Billing will start as soon as Proximus provides the Customer with his identification codes (password, user name, etc.), regardless of the Service activation date.

7.74. Unless specified otherwise, the prices do not include any equipment costs necessary for using the Service, nor any Internet access and connection charges or any other data transmissions charges. The Customer is responsible for all such incidental charges and any taxes and is legally required to pay them.

7.8 Reports

All reports prepared by Proximus in the framework of the Service are made in good faith on the basis of information available at the time. They are intended solely for the Customer for internal use only. They may not be used or relied upon by any third party without the prior written consent of Proximus. Proximus accepts no responsibility or liability for any report or document that it has prepared in the framework of the Service for any party other than the Customer.

7.9 Protection of personal data

7.9.1. Proximus is acting as data processor for the personal data included (1) in the configuration data of the Solution elements (2) in emails processed under this Agreement, (3) data available via the Administration tool. Proximus acts as data controller for all other personal data processed by Proximus under this Agreement.

7.9.2. If the consent, approval or authority of a person other than the Customer is required in order for Proximus to provide the Service, the Customer warrants that it will obtain that consent, approval or authority before Proximus commences provision of that part of the Service for which the consent, approval or authority is required.

7.9.3. Proximus recognizes and confirms that the content sent to or received from the Customer by the Service is confidential. Proximus (and its supplier) does not access, read or copy email, their attachments or linked content other than by electronic methods for the purposes of provisioning the Service. However, Proximus (and its supplier) reserves the right to utilize the malware and spam related content of such emails, their attachments and linked content solely for the purpose of:

- maintain and improving the Service,
- complying with court orders and all regulatory, legislative or contractual requirements, and
- making available to the supplier any information passing through the service which may be of interest to the supplier solely for the purpose of further developing and enhancing the Service

7.10 Force majeure

In the context of this Service, an event of Force majeure is defined as events or circumstances that are beyond its control, unpredictable or unavoidable, such as acts of war, riots, disturbances, civil unrest, actions of civil or military authorities, embargoes, explosions, bankruptcy of a licensor or a supplier, strikes or labor conflicts (including those involving its employees), cable cuts, power blackouts (including those blackouts arising from the application of a power cut plan drawn up by the authorities), shortages of resources, flooding, prolonged frost, fires or storms.

Because of the specific nature of the Service, the Force majeure termination possibility set out in the General Terms and Conditions for Professional Customers is granted to both Parties for the duration of the Force Majeure event continued for more than 30 Calendar days

7.11 Service limitations

The following limits apply to the Service

- The maximum amount of inbound and outbound messages, per User per calendar month is 10.000. This limit is not inclusive of Spam and Malware directed at Customer.
- Proximus reserves the right to invoice Customer for additional Users, upon notification, for the remaining months on the contract where usage exceeds the message limit.
- The inbound and outbound mail retry schedule is 7 calendar days.
- The default maximum e-mail size is 50MB. Customer can specify any maximum e-mail size up to 1000MB. Any e-mails that are received by the Service that exceed the specified limit will be blocked and deleted, and a notification alert e-mail will be sent to the sender, intended recipient, and an Administrator.

7.12 Service Specific Conditions

- Customers must route their inbound e-mail through the Service using the routing information provided by Proximus and must not route e-mail to any other destination.
- Customer must accept inbound e-mail from all required IP ranges to ensure continuity of service in the event that a portion of the Infrastructure is not available.
- Customer must specify the mail server IP address(es) or hostname(s) for the delivery of inbound e-mails to their organization.
- Customer must ensure that all domains (including sub-domains) requiring the Service are provisioned. Customer accepts that Service features may not function correctly and e-mail delivery may be unavailable for domains that are not provisioned.

8. Appendix 1: Anti-Spam Best Practice settings

Please note the SL is only applicable if the following best practice settings are configured by the Customer. Customer remains responsible for the configuration for any flavor.

8.1 For Reactive Care Flavor

8.1.1 To be configured by Customer

- Enable both Approved Sender options and keep entries on the list to a minimum where possible
- Enable spoofed sender detection with SPF - recommended if having an issue with spoofed spam mails – Only for incoming mails
- Enable DMARC - (Domain-based Message Authentication, Reporting, and Conformance) helps thwart phishing attempts that can lead to security breaches by detecting email sender spoofing - – Only for incoming mails
- Enable Both Blocked Senders Lists - The recommended action for both is to 'block and delete'
- Utilize the dynamic IP block list - Recommended action is block and delete as this contains a list of dynamic IP ranges that no mail should be coming from
- Enable the Signature System - Recommended action Block and Delete as this works on characteristics of known spam.
- Enable Skeptic Heuristics - Predictive Spam detection - Recommended action is to tag the subject line and allow mail through as this can then be actioned by outlook rules for the end users. This is also recommended as this rule set while still very accurate has more of a potential for false positives as it is a predictive system. Alternately Quarantine the mail should be utilized if it is enabled/activated.
- Enable the newsletter filter extension if needed - this is a very aggressive newsletter block which will stop all wanted and unwanted newsletters. We generally recommend that this be enabled and exceptions made on a case-by-case basis depending on the environment that you are deploying to.
- Enable spoofed sender detection with SPF – For outgoing e-mails
- Enable DMARC - (Domain-based Message Authentication, Reporting, and Conformance) helps thwart phishing attempts that can lead to security breaches by detecting email sender spoofing - For outgoing e-mails

8.2 For Reactive Care with Assist or Full Care Flavor

8.2.1 To be configured by Customer

- Enable spoofed sender detection with SPF – For outgoing e-mails
- Enable DMARC - (Domain-based Message Authentication, Reporting, and Conformance) helps thwart phishing attempts that can lead to security breaches by detecting email sender spoofing - For outgoing e-mails

9. Appendix 2: Technical prerequisites

The Customer shall ensure that its email system is SMTP compliant.

The Customer shall implement and maintain the following configuration settings for his ICT infrastructure to enable the proper support of the Service:

- Add a key to the DNS of the Customer. This key will be communicated by Proximus at order confirmation.
- Whitelist the IP addresses of the Service to get access to the Customer environment, where the e-mail server is hosted. These IP addresses will be communicated by Proximus at order confirmation.
- Change the MX records. Details will be communicated by Proximus at order confirmation.