Enterprise Business Unit Solutions

Description de service contractuelle

Service Cloud Mail Security

Date 06/09/2018
Confidentialité **Unrestricted**

proximus

Table des matières

1. Introduction

Cloud Mail Security (ci-après dénommé "le Service") protège les systèmes de messagerie compatibles SMTP contre les menaces internes et externes pour la sécurité, comme décrit dans le présent document. Le Service est proposé "dans le cloud", c'est-à-dire qu'il ne requiert pas d'investissement massif en matériel ou logiciels de la part du Client. Tout le trafic e-mail entrant des mailboxes dans le cadre du présent Contrat est dirigé vers une plateforme de sécurité basée sur internet grâce à un changement apporté dans l'enregistrement MX du domaine du Client. Il y est nettoyé sur la base de différents paramètres prédéfinis avant d'arriver sur l'infrastructure du Client. En option, le trafic e-mail sortant peut également être dirigé vers cette plateforme de sécurité et être analysé afin de s'assurer de sa conformité avec les règles de sécurité configurées. Pour ce faire, le Service doit avoir enregistré l'adresse IP d'envoi ou le service de messagerie hébergé. Les fonctionnalités de base du Service visent à protéger l'organisation du Client contre les spams et les logiciels malveillants, à permettre au Client de crypter son trafic e-mail et à fournir au Client des outils de reporting. Selon les options fonctionnelles choisies, le Client peut compléter ces fonctionnalités par plusieurs fonctions avancées.

Le Service est disponible en deux Formules : Reactive Care et Full Care. La différence entre ces deux Formules réside dans le nombre d'activités réalisées par Proximus dans le domaine de l'administration en ligne, de la configuration et du support. La Formule Full Care est disponible à partir de 25 mailboxes.

Le Service se compose des éléments d'infrastructure suivants, appelés "Éléments de la solution" :

- Plateforme
- Portail d'administration
- Portail de mise en quarantaine des spams
- Outil de synchronisation

Le chapitre "Aperçu du Service" dresse la liste des fonctionnalités et des types d'activités de support pouvant être inclus dans le Service et définit le champ d'application de chaque activité de support effectuée par Proximus par Élément de la solution.

La fonctionnalité du Service est décrite de manière plus détaillée dans le chapitre "Description du service fonctionnel". Les services de support ("Assist and Care Services") fournis au Client lors des phases d'implémentation et opérationnelle sont décrits respectivement dans les chapitres "Phase d'implémentation" et "Phase opérationnelle".

2. Aperçu du Service

Le tableau ci-dessous indique les fonctionnalités et types d'activités pouvant être inclus dans le Service (également appelés Composants de Service). Les Composants de Service :

- sont inclus dans le Service par défaut ("DEF") ;
- ou sont facultatifs ("OPT") et doivent être sélectionnés par le Client ;
- ou encore, font l'objet d'un contrat distinct (CD).

2.1 Une fois que le Client a choisi les Composants de Service au moyen du Bon de commande, le champ d'application du présent Contrat est défini. L'ajout ou l'adaptation de Composants de Service entraînera l'établissement d'un nouveau Contrat.Service fonctionnel

Le tableau ci-dessous présente un aperçu des fonctionnalités incluses dans le service de base et les options. Le Chapitre "Description du service fonctionnel" fournit plus d'explications sur ces éléments.

Composants de Service	Détail	Reactive Care	Full Care
Service de base	Antimalware Antispam Cryptage TLS opportuniste Enregistrement d'adresses Traçage des messages Reporting Portail de mise en quarantaine des spams pour l'Utilisateur final et notifications Disclaimer Management	DEF	DEF
Data Loss Prevention (DLP) (prévention de la perte de données)	E-Mail Data protection (protection des données des e-mails) E-Mail Image Control (contrôle des images des e-mails) Enforced TLS Encryption (cryptage TLS renforcé) Basic Policy Based Encryption (cryptage basé sur la Basic Policy) E-Mail Impersonation Controls (contrôle de l'usurpation d'identité par e-mail)	OPT	OPT
Protection avancée contre les menaces	Sandboxing basé sur le cloud Click-time URL Protection Reporting détaillé sur les logiciels malveillants	OPT	OPT
Add-On : intégration de l'Active Directory	Synchronisation des utilisateurs et groupes de l'Active Directory	OPT	OPT

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

2.2 Services d'assistance et de support (Assist and Care)

Le support fourni par Proximus pendant les phases d'implémentation et opérationnelle s'applique aux Éléments de la solution dont la liste est dressée par type d'activité dans le tableau ci-dessous. Le Service ne comprend aucune activité relative à d'autres Éléments de la solution.

Composant de Service	Éléments de la solution concernés		Full Care
Assist			
Service Assist	Plateforme Portail de mise en quarantaine des spams Outil de synchronisation Portail d'administration	DEF	DEF
Service Assist en option	Plateforme	OPT	
Accès au Service Desk	Tous les Éléments de la solution	DEF	DEF
Gestion des Incidents			
Diagnostic à distance	Tous les Éléments de la solution	DEF	DEF
Intervention à distance	Tous les Éléments de la solution	DEF	DEF
Restauration de la configuration	Portail d'administration Portail de mise en quarantaine des spams	DEF	N/A
Gestion de la configuration			
Gestion de la configuration avec droit de lecture du Client	Portail d'administration	N/A	DEF
Gestion de la configuration avec droits d'accès spécifiques	Portail de mise en quarantaine des spams Outil de synchronisation	N/A	OPT
Gestion de la configuration sans droits d'accès	Plateforme	N/A	DEF / OPT

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

Back-up de la configuration	Portail d'administration Portail de mise en quarantaine des spams	DEF	DEF
Gestion des Changements			
Changements standard	Portail d'administration Portail de mise en quarantaine des spams	N/A	CD
Changements personnalisés	Portail d'administration Portail de mise en quarantaine des spams	N/A	CD
Updates et Upgrades	Tous les Éléments de la solution	DEF	DEF
Contrôle			
Contrôle de la Disponibilité du Service	Tous les Éléments de la solution	N/A	DEF
Reporting			
Reporting sur la Disponibilité du Service	Plateforme Portail d'administration Portail de mise en quarantaine des spams	N/A	DEF

3. Description du Service fonctionnel

Le Service repose sur une plateforme de sécurité hébergée (également appelée "Plateforme") destinée à filtrer les messages e-mail entrants et éventuellement sortants qui relèvent du champ d'application du Contrat (c'est-à-dire les adresses e-mail figurant dans la Liste de validation ci-dessous), afin de contribuer à protéger l'infrastructure du Client contre les menaces pour la sécurité décrites dans le présent document.

Les paramètres des fonctionnalités du Service sont configurés via le Portail d'administration mis à la disposition du Client. En cas de Formule Reactive Care, le Client configure lui-même ces paramètres dans

le Portail d'administration. En cas de Formule Full Care, Proximus configure ces paramètres pour le Client dans le Portail d'administration en se basant sur le formulaire d'exigences de configuration technique et les demandes ultérieures du Client. Le Client reconnaît et accepte le fait qu'il est le seul responsable de la sélection de la configuration et que la sélection est conforme à ses policies et procédures.

Le Service supporte les services e-mail de différents fournisseurs, tels que Microsoft Exchange, Office 365, Google Apps, etc. La liste des compatibilités est disponible sur demande.

Le présent chapitre décrit les différentes fonctionnalités pouvant être incluses dans le Service, quelle que soit la Formule sélectionnée.

3.1 Service de base

3.1.1 Antimalware

Cette fonctionnalité vise à fournir au Client une protection contre les logiciels malveillants, connus et inconnus, distribués via des URL ou des fichiers aux mailboxes de la Liste de validation et éventuellement au départ de celles-ci. La protection consiste en une combinaison de différentes technologies, comme des moteurs basés sur la signature, la réputation et l'heuristique.

Le Portail d'administration est utilisé pour configurer les paramètres de cette fonctionnalité, qui permet notamment, mais non exclusivement :

- de supprimer les e-mails infectés ;
- de mettre des virus suspects en quarantaine de manière proactive jusqu'à l'obtention d'une signature/solution ;
- d'envoyer des alertes automatiques à l'administrateur et/ou aux Utilisateurs finaux à titre de notification ;
- de libérer des e-mails à la première adresse de la liste initiale des destinataires, à une adresse e-mail prédéfinie ou à une autre adresse demandée par le Client ;
- de créer des bannières de virus informant les Utilisateurs finaux du scan des e-mails ;
- de fixer la taille maximale des e-mails.

Les e-mails considérés par défaut comme logiciels malveillants sont mis en quarantaine et le restent pendant 30 Jours calendrier. À l'expiration de cette période, ils sont automatiquement supprimés.

3.1.2 Antispam

Cette fonctionnalité vise à fournir au Client une protection contre les spams, c'est-à-dire les e-mails commerciaux non sollicités, en scannant le trafic e-mail entrant et éventuellement sortant des mailboxes relevant de la Liste de validation.

Une approche multicouche est appliquée, c'est-à-dire que les techniques suivantes sont notamment utilisées :

- une liste privée d'expéditeurs approuvés, établie par le Client ou ses Utilisateurs finaux individuels (avec l'approbation du Client) ;

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

- une liste privée d'expéditeurs bloqués, établie par le Client ou ses Utilisateurs finaux individuels (avec l'approbation du Client) ;
- un nombre de listes publiques d'expéditeurs bloqués ;
- un système basé sur la signature ;
- La détection heuristique SkepticTM de Symantec.clouds.

Les e-mails suspectés d'être des spams peuvent faire l'objet de différentes actions en fonction de la configuration dans le Portail d'administration. Les actions définies comme le résultat d'une détection heuristique ou de signature prévalent toujours sur toute action moins sévère assignée antérieurement par une des méthodes précédentes. Actions possibles :

- suppression des e-mails provenant de destinataires suspects en utilisant des filtres de réputation ;
- mise en quarantaine des e-mails provenant de destinataires suspects en utilisant des filtres ;
- supprimer des e-mails provenant d'un spam identifié ;
- mise en quarantaine des e-mails provenant d'un spam identifié ;
- repérage des e-mails suspects dans l'objet ;
- repérage des e-mails suspects dans l'en-tête ;
- déblocage des e-mails mis en quarantaine par les administrateurs ;
- déblocage des e-mails mis en quarantaine par les Utilisateurs finaux.

Les e-mails suspectés d'être des spams et restés en quarantaine sont supprimés comme décrit dans le Portail de mise en quarantaine des spams pour l'Utilisateur final et dans la rubrique "Notifications" ci-dessous.

3.1.3 Cryptage TLS opportuniste

Cette fonctionnalité vise à permettre au Client d'échanger des e-mails en toute sécurité en dehors de son organisation en ayant recours au protocole de cryptage SMTP sur TLS, c'est-à-dire via un canal crypté. Les organisations partenaires avec lesquelles le Client souhaite échanger des e-mails via un canal crypté sont identifiées dans le Portail d'administration. Un réseau de messagerie privé et sécurisé est établi avec ces organisations partenaires, sur la base de certificats d'authentification entièrement gérés pour le Client. L'établissement d'un tel réseau n'est possible que si le serveur e-mail de l'organisation partenaire supporte TLS. Dans les autres cas, les e-mails seront fournis en clair.

De plus, le Client peut recevoir une communication e-mail cryptée envoyée de manière opportuniste par des organisations qui disposent de serveurs e-mail supportant TLS.

Proximus attire l'attention du Client sur le fait que dans le cadre de cette fonctionnalité, seul le canal est crypté, et non l'e-mail. Cette fonctionnalité diffère donc, sur ce point, de la fonctionnalité Basic Policy Based Encryption.

3.1.4 Enregistrement d'adresses

Grâce à cette fonctionnalité, le Client peut charger dans le Portail d'administration une liste d'adresses e-mail valides d'Utilisateurs finaux de l'organisation. Les e-mails envoyés à des Utilisateurs finaux non enregistrés sont bloqués. L'expéditeur recevra le message d'erreur "550 invalid recipient" si l'e-mail était valable, mais que l'adresse avait une forme incorrecte ou était mal orthographiée.

Le Client s'engage à fournir et à tenir à jour une liste d'adresses e-mail valides pour recevoir le Service (la "Liste de validation"). Il appartient au Client de vérifier la Liste de validation avant la mise à disposition du Service et tout au long de la durée du Contrat.

Le Client accepte qu'aucun Niveau de service ne s'applique aux e-mails envoyés à des adresses non valides ou non reprises dans la Liste de validation.

Par souci de clarté, précisons que les Clients qui utilisent le système de mise en quarantaine doivent tenir à jour une Liste de validation et avoir activé la fonction Enregistrement d'adresses. Si le Client n'est pas en mesure de fournir cette Liste de validation et demande que la fonction Enregistrement d'adresses soit désactivée, Proximus examinera chaque demande de ce type au cas par cas et se réserve le droit de rejeter les demandes, à sa seule discrétion.

3.1.5 Traçage des messages

La fonction de recherche Track and Trace du Portail d'administration permet au Client de vérifier comment la Plateforme a traité les e-mails spécifiques. Elle fournit des détails sur les différentes étapes du traitement, comme la réception de l'e-mail par la Plateforme, les actions entreprises au niveau de l'e-mail, la fourniture de l'e-mail, etc. Aucune copie des e-mails n'est conservée.

La fonction de recherche Track and Trace est idéale pour rechercher des e-mails individuels. Elle évite en effet au Client de parcourir un grand nombre d'e-mails pour en trouver un en particulier. La possibilité de traçage se limite aux e-mails traités au cours des 30 derniers Jours calendrier.

La fonction Track and Trace est accessible à l'Administrateur, à savoir Proximus pour la Formule Full Care et le Client pour la Formule Reactive Care. Si nécessaire, des Utilisateurs finaux supplémentaires peuvent se voir accorder des droits de lecture de la fonction Track and Trace.

3.1.6 Reporting

Des tableaux de bord de reporting sont disponibles dans le Portail d'administration. Les tableaux de bord affichent une sélection de statistiques clés et notamment, mais non exclusivement :

- le nombre d'e-mails scannés ;
- le nombre d'e-mails identifiés comme spams ;
- le nombre d'occurrences d'activation d'une politique de protection des données (si l'option DLP est commandée).

Les statistiques dans ces tableaux de bord peuvent être affichées par domaine ou pour tous les domaines.

De plus, le Portail d'administration permet au Client d'obtenir des rapports sous la forme de documents. Les rapports sous la forme de documents peuvent être générés pour tous les domaines du Client ou par domaine individuel, mais pas par mailbox individuelle. Les rapports sont disponibles en différents formats et peuvent également être programmés pour être envoyés à un nombre de destinataires prédéfinis. Les formats spécifiques suivants sont disponibles :

- tableaux de bord graphiques

- rapports de synthèse en .pdf, comprenant des diagrammes, graphiques et tableaux, tout au plus pour la dernière année

- rapports détaillés en .csv, avec une limite de 500.000 rangées. Ceux-ci fournissent un log listing détaillé de toute l'activité de service pour l'ensemble des domaines. Les données de reporting portent sur les 30 derniers Jours calendrier maximum.

Les données de reporting sont disponibles pendant 12 mois.

3.1.7 Portail de mise en quarantaine des spams pour l'Utilisateur final et notifications

Le Portail de mise en quarantaine des spams est un portail qui intercepte les e-mails que le Service a identifiés comme spams ou qui met en quarantaine les e-mails contenant des données ou des images contraires aux règles de conformité du Client.

Dans ce Portail de mise en quarantaine des spams pour l'Utilisateur final, l'Administrateur de l'organisation du Client peut consulter,communiquer et supprimer les e-mails mis en quarantaine, gérer les expéditeurs bloqués et autorisés, et spécifier les paramètres et préférences. L'Administrateur peut également accorder ce droit aux Utilisateurs finaux (ou à certains d'entre eux) pour les e-mails envoyés à l'adresse e-mail de l'Utilisateur final concerné.

En fonction de la configuration, les Utilisateurs finaux peuvent recevoir une notification lorsqu'un e-mail a été mis en quarantaine.

Les e-mails sont conservés sur le portail de mise en quarantaine pendant 14 Jours calendrier, sauf s'ils sont supprimés avant ce délai.

3.1.8 Disclaimer Management

Un e-mail disclaimer est le texte dans le pied de page d'un e-mail entrant ou sortant qui transite par le Service. Grâce à cette fonctionnalité, des disclaimers peuvent être configurés au moyen d'une combinaison d'e-mail disclaimers personnalisés ou par défaut, pour les e-mails entrants et éventuellement sortants des adresses e-mail de la Liste de validation au niveau général, du domaine ou du groupe.

Proximus se réserve le droit de scanner tous les e-mails sortants si le Client configure le Service pour les e-mails sortants. Un message disclaimer par défaut sera appliqué aux e-mails scannés par le Service à partir du moment où le Service est fourni.

Proximus se réserve le droit de mettre à jour à tout moment le message disclaimer par défaut. Cette mise à jour ne pourra pas être considérée comme une modification du Contrat.

3.2 Data Loss Prevention (prévention de la perte de données)

Lorsqu'elle est sélectionnée, l'option Data Loss Prevention fournit au Client les fonctionnalités suivantes en vue de réduire le risque de perte de données :

3.2.1 Protection des données des e-mails

Cette fonctionnalité permet au Client de créer une série de règles sur la base desquelles les e-mails entrants et éventuellement sortants sont filtrés en fonction de leur contenu. Chaque règle identifie un

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

format spécifique d'e-mails (ou pièces jointes : documents Microsoft Office, documents PDF ou fichiers texte) nécessitant l'adoption de mesures déterminées.

Le Portail d'administration est utilisé pour configurer ou adapter les règles applicables et les actions correspondantes à entreprendre au niveau des e-mails entrants et éventuellement sortants. Actions possibles :

- blocage et suppression de l'e-mail suspect ;
- repérage d'un e-mail entrant suspect (ou de son en-tête) ;
- réexpédition ou copie d'un e-mail suspect vers un administrateur spécifique ;
- compression des pièces jointes de l'e-mail ;
- connexion uniquement aux statistiques du portail de gestion ;
- repérage de l'objet.

3.2.2 E-Mail Image Control (contrôle des images des e-mails)

Cette fonctionnalité permet au Client d'identifier, de contrôler et de bloquer les images inappropriées intégrées dans des e-mails ou pièces jointes (dans des pièces jointes en Word, Excel et PowerPoint, à l'exception du contenu relevant du contrôle exclusif de l'expéditeur, comme des fichiers cryptés ou protégés par un mot de passe). Elle scanne les e-mails entrants et éventuellement sortants en utilisant notamment les méthodes suivantes :

- listes d'expéditeurs et de destinataires approuvés
- signatures approuvées pour les images dans une base de données du Client
- base de données globale de la communauté Image Control
- moteur pour l'Image Composition Analysis (ICA).

Le Portail d'administration est utilisé pour configurer les actions à entreprendre sur des e-mails entrants et éventuellement sortants en cas de détection d'images inappropriées. Actions possibles :

- enregistrement de l'e-mail suspect ;
- repérage de l'e-mail entrant suspect dans l'en-tête ;
- réexpédition ou copie de l'e-mail suspect vers une adresse e-mail prédéfinie ;
- suppression de l'e-mail suspect ;
- repérage de l'e-mail suspect dans l'objet ;
- envoi des notifications d'alerte à l'expéditeur/au destinataire concerné.

Cette fonctionnalité vise à détecter les images inappropriées, en particulier les images pornographiques. Veuillez noter qu'une détection à 100 % des images pornographiques n'est pas garantie et que la définition de ce qui constitue une image pornographique est subjective.

3.2.3 Enforced TLS Encryption (cryptage TLS renforcé)

Cette fonctionnalité permet aux organisations de créer des liaisons sécurisées avec leurs partenaires professionnels et/ou avec le Service et de crypter ainsi tout le trafic e-mail échangé entre eux sans action

supplémentaire de la part de l'expéditeur. Le contenu du message reste transparent à la fois pour l'expéditeur et le destinataire.

Veuillez noter que contrairement au cryptage TLS opportuniste, l'e-mail n'est pas délivré si un serveur e-mail du partenaire professionnel ne supporte pas TLS ou si le Service ne parvient pas à authentifier le certificat que le serveur e-mail du tiers présente lorsque le domaine utilise une validation forte. L'e-mail non délivré est renvoyé.

3.2.4 Basic Policy Based Encryption

Cette fonctionnalité sert à scanner les e-mails et pièces jointes. Elle est conçue pour crypter elle-même automatiquement les messages identifiés comme contenant des informations sensibles. Le cryptage est effectué dès l'instant où le message passe par le Service.

Le Service permet aux destinataires de recevoir leurs e-mails via leur mailbox ou via un portail web sécurisé et dédié (ne faisant pas partie du Portail d'administration). Les destinataires peuvent utiliser ce portail web sécurisé pour envoyer leurs réponses ou (éventuellement) de nouveaux e-mails aux Utilisateurs finaux.

La fonctionnalité est soumise aux limites suivantes :

- Le nombre maximal d'e-mails sortants sécurisés par Utilisateur final par mois est fixé à 300 pour cette fonctionnalité. En cas d'envoi à plusieurs destinataires, chaque adresse unique sera prise en compte comme e-mail sortant sécurisé distinct. Si le Client dépasse le nombre d'e-mails sortants sécurisés autorisés pendant un mois calendrier, Proximus se réserve le droit de facturer l'utilisation réelle au Client.

- Les e-mails routés via cette fonctionnalité sont limités à un volume maximal de cinquante megabytes (50 MB. À défaut, ils ne sont pas cryptés.

- En cas d'utilisation du cryptage Pull avec la fonctionnalité Policy Based Encryption (Z) , les e-mails seront par défaut conservés pendant 90 Jours calendrier dans le portail web sécurisé et dédié avant d'être supprimés. Il est possible d'exporter ces e-mails en vue d'une sauvegarde locale par l'Utilisateur final.

- Les Niveaux de service relatifs à la Disponibilité et à la latence ne s'appliquent pas à la Policy Based Encryption.

3.2.4.1 E-Mail Impersonation Control (EIC)

Cette fonctionnalité vise à protéger le Client contre les e-mails d'escroquerie et de harponnage. EIC vérifie l'e-mail entrant par rapport aux adresses e-mail de la Liste de validation en ce qui concerne l'usurpation du nom d'utilisateur, mieux connue sous le nom de "spoofing". Plus spécifiquement, EIC vérifie la légitimité de l'e-mail entrant qui semble être envoyé par les domaines ou les Utilisateurs finaux de l'organisation.

Le Portail d'administration est utilisé pour configurer les actions à entreprendre au niveau de l'e-mail lorsque l'on suspecte une usurpation d'identité. Actions possibles :

- enregistrement
- repérage de l'objet
- mise en quarantaine
- réexpédition vers vers l'Admin

- blocage et suppression

3.3 Advanced Threat Protection (ATP) (Protection avancée contre les menaces)

Lorsqu'elle est sélectionnée, l'option Advanced Threat Protection offre au Client les fonctionnalités décrites ci-dessous :

3.3.1 Sandboxing basé sur le cloud

Afin de détecter les caractéristiques d'un éventuel logiciel malveillant dans un fichier inconnu, une copie du fichier est lancée dans une sandbox basée sur le cloud. Ensuite, les comportements typiques des Utilisateurs finaux au sein de différents environnements de système d'exploitation sont copiés. Si nécessaire, la sandbox fait passer l'exécution d'un environnement virtuel à un environnement physique pour démasquer le logiciel malveillant qui est "virtual-machine-aware". Si le logiciel suspect reste inactif dans l'environnement sandbox, la sandbox continue à le surveiller. Il sera ainsi possible de détecter ultérieurement si le logiciel malveillant essaie de bouger dans l'environnement ou de communiquer avec un serveur de contrôle ou un autre ordinateur. La sandbox établit une corrélation entre les données et celles provenant du Symantec Global Intelligence Network afin de déterminer si les fichiers sont malicieux. Le Portail d'administration est utilisé pour déterminer combien de temps l'e-mail est conservé avant d'être envoyé, avec un maximum de 20 minutes. Si une analyse ultérieure révèle qu'un fichier téléchargé contient un logiciel malveillant, il est possible d'informer jusqu'à 5 adresses e-mail spécifiées. Spécifiquement pour les Clients qui utilisent Office 365, il est en mesure de récupérer les e-mails considérés comme malveillants ayant été délivrés.

3.3.2 Click-Time URL Protection

Cette fonctionnalité vise à "réécrire" et à contrôler certaines URL dans les e-mails délivrés aux adresses e-mail de la Liste de validation. Le processus de réécriture permet au service de gérer l'accès à l'URL afin de garantir que la destination est sûre.

Chaque URL réécrite par Click-time URL Protection est contrôlée à chaque fois qu'un Utilisateur final clique dessus, afin de garantir que la destination de l'URL n'héberge pas un logiciel malveillant ou des risques de phishing ou de spam. De nombreuses URL réécrites peuvent ainsi être contrôlées et identifiées comme dépourvues de risques. Une URL autorisée dans le passé peut, à un stade ultérieur, commencer à héberger un logiciel malveillant, du phishing ou un spam. À ce moment, la fonctionnalité Click-Time URL Protection bloque l'accès à l'URL et une notification est adressée au Portail d'administration.

3.3.3 Reporting détaillé relatif aux logiciels malveillants

Cette fonctionnalité fournit au Client un reporting granulaire concernant les e-mails sûrs et malveillants qui entrent dans son organisation. Ces rapports sont disponibles via le Portail d'administration.

Les rapports fournis comprennent des points de données 60+, comme :

- les URL sources d'une attaque
- les informations relatives à une attaque ciblée
- la catégorisation du logiciel malveillant
- les informations relatives à l'expéditeur et au destinataire
- la méthode de détection
- des informations détaillées concernant les "file hashes"
- la catégorie de la menace
- le degré de gravité

Les données de reporting sont disponibles pendant 12 mois.

3.4 Active Directory Synchronization

Lorsqu'elle est sélectionnée, l'option de synchronisation fournit au Client un outil qui l'aide à synchroniser ses sources de répertoire avec la Plateforme. L'outil permet de combiner les types de synchronisation suivants :

- Synchronisation des e-mails pour synchroniser les adresses e-mail
- Synchronisation des Utilisateurs finaux pour synchroniser les identités des Utilisateurs finaux, les adresses e-mail et l'appartenance à un groupe
- Synchronisation des groupes pour synchroniser les identités des groupes

L'outil de synchronisation guide le Client dans un processus de configuration qui lui permet d'extraire les données requises de son système de répertoire. Après avoir été correctement configuré, le processus de synchronisation peut être exécuté à partir de l'interface de l'outil de synchronisation ou à partir de la ligne de commande. Il est possible de programmer le processus en vue d'un fonctionnement automatique. L'outil de synchronisation peut également envoyer des notifications par e-mail pour rapporter son résultat chaque fois qu'il y est invité.

4. Phase d'implémentation

4.1 Commande

Le Client commande le Service en faisant parvenir à Proximus le Bon de commande concerné, dûment complété et signé. Dans ce Bon de commande, le Client est tenu de préciser notamment :

- La Formule choisie
- Les options choisies
- Le nombre de mailboxes à protéger
- Des informations techniques (p. ex. adresse IP des serveurs e-mail, domaine e-mail)
- Informations relatives au modèle de quarantaine demandé

Le document relatif aux Exigences de configuration technique, applicable à la Formule Full Care, est joint au Bon de commande.

Tout Changement impliquant un changement de redevance du Service fera l'objet d'un nouveau Bon de commande/avenant.

4.2 Activation et services d'assistance pour la Formule Reactive Care

4.2.1 Activation

Dès qu'elle reçoit le Bon de commande dûment complété et signé (y compris les annexes), Proximus lance l'implémentation du Service.

Seuls Proximus ou ses sous-traitants sont autorisés à réaliser les activités d'implémentation décrites ci-dessous. Toutes les activités d'implémentation sont réalisées pendant les Heures de bureau, après l'activation et conformément à la policy "Best practice". Proximus effectue les activités suivantes lors de l'implémentation du Service :

Par défaut, l'implémentation du Service comprend :

- l'activation de la Plateforme pour les domaines commandés, soit 5 au maximum. Les environnements antivirus et antispam sont activés par défaut ;
- la configuration sur la Plateforme des itinéraires empruntés par les e-mails entrants (et par les e-mails sortants si la commande porte également sur ces derniers) ;
- la création de 1 compte sur le Portail d'administration et la fourniture au Client des données d'identification pertinentes ;
- la fourniture de la documentation et des manuels d'utilisation du Service ;
- la création de 1 compte d'administrateur sur le portail de mise en quarantaine des spams (si sélectionné dans le Bon de commande). Les données d'identification pertinentes sont mises à disposition ;
- le back-up de la configuration de la Plateforme ;
- l'activation du Service et la fourniture du ou des Portails.

Dès que le Service est activé et que les Portails liés au Service sur la Plateforme sont fournis au Client pour les domaines e-mail demandés par ce dernier, le Service est considéré comme mis à sa disposition.
Afin d'éviter tout malentendu, Proximus attire l'attention du Client sur le fait que sauf accord explicite décrit dans le Bon de commande, l'implémentation du Service par Proximus ne couvre pas les activités suivantes :

- L'activation de la Plateforle pour plus de 5 noms de domaine

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

- La configuration de la Plateforme. La configuration de la Plateforme via le Portail d'administration relève de la responsabilité du Client. Proximus attire l'attention du Client sur le fait que le Niveau de service ne s'applique que s'il a configuré les paramètres de meilleures pratiques suivants :

    - activation des deux options expéditeurs approuvées et si possible, limitation au strict minimum des entrées sur la liste
    - activation de spoofed sender detection avec SPF – pour les e-mails entrants et sortants
    - activation de DMARC - pour les e-mails entrants et sortants
    - activation des deux listes d'expéditeurs bloqués
    - utilisation de la liste de blocage IP dynamique
    - activation du système d'écriture
    - activation de skeptic heuristics - predictive spam detection
    - activation de l'extension du filtre newsletter
    - activation de spoofed sender detection avec SPF – pour les e-mails sortants
    - activation de DMARC – pour les e-mails sortants

- L'administrateur peut créer lui-même d'autres comptes pour son organisation et attribuer des rôles pointus à ces autres comptes dans le Portail d'administration.
- Formation
- Création de règles de sécurité pour le Client
- Il incombe au Client de changer le mot de passe du compte d'administrateur dès que ce dernier est transmis au contact technique du Client.
- Installation et configuration de l'outil Active Directory Synchronization, s'il a été commandé

4.2.2 Service d'assistance

Si le Client a commandé l'option Assistance, Proximus réalisera les activités d'implémentation suivantes en plus de celles comprises par défaut dans la Formule Reactive Care :

- Configuration du Portail d'administration du Client, y compris, le cas échéant, la policy de synchronisation DLP, ATP et/ou AD, Spam Manager, conformément à la politique du Client en matière de sécurité.
- Proximus configure la Plateforme en se conformant à la politique du Client en matière de sécurité, que ce dernier a communiquée, mais aussi aux paramètres de meilleures pratiques suivants :

    - activation des deux options expéditeurs approuvées et si possible, limitation au strict minimum des entrées sur la liste
    - activation de DMARC - uniquement pour les e-mails entrants
    - activation des deux listes d'expéditeurs bloqués
    - utilisation de la liste de blocage IP dynamique
    - activation du système d'écriture
    - activation de skeptic heuristics - predictive spam detection
    - activation de l'extension du filtre newsletter

Attention : même si le Client a souscrit cette option, il lui appartient de configurer de son côté les paramètres de meilleures pratiques suivants (le Niveau de service n'est pas applicable si ces paramètres ne sont pas configurés par le Client) :

- activation de spoofed sender detection avec SPF – pour les e-mails sortants
- activation de DMARC – pour les e-mails sortants

4.3 Activation et services d'assistance pour la Formule Full Care

Dès qu'elle reçoit le Bon de commande dûment complété et signé (y compris les annexes), Proximus lance l'implémentation du Service.

Seuls Proximus ou ses sous-traitants peuvent réaliser les activités d'implémentation décrites ci-dessous. Toutes les activités d'implémentation sont réalisées pendant les Heures de bureau, après l'activation et conformément à la policy "Best practice". Proximus effectue les activités suivantes lors de l'implémentation du Service :

L'implémentation du Service comprend :

- l'activation de la Plateforme pour les domaines commandés, soit 5 au maximum. Proximus configure la Plateforme conformément aux Exigences de configuration technique jointes au Bon de commande, aux règles de sécurité du Client communiquées en temps utile à Proximus, et aux paramètres de meilleures pratiques suivants :
  - activation des deux options expéditeurs approuvées et si possible, limitation au strict minimum des entrées sur la liste
  - activation de DMARC - uniquement pour les e-mails entrants
  - activation des deux listes d'expéditeurs bloqués
  - utilisation de la liste de blocage IP dynamique
  - activation du système d'écriture
  - activation de skeptic heuristics - predictive spam detection
  - activation de l'extension du filtre newsletter
  - configuration sur la Plateforme des itinéraires empruntés par les e-mails entrants (et par les e-mails sortants si la commande porte également sur ces derniers).

- la création de 1 compte en lecture seule sur le Portail d'administration et la fourniture au Client des données d'identification pertinentes ;

- la configuration du Portail d'administration du Client, y compris, le cas échéant, la policy de synchronisation DLP, ATP et/ou AD, Spam Manager, conformément aux règles de sécurité du Client.

- la fourniture de la documentation et des manuels d'utilisation du Service ;
- la création de 1 compte d'administrateur sur le portail de mise en quarantaine des spams (si sélectionné dans le Bon de commande). Les données d'identification pertinentes sont mises à disposition ;
- le back-up de la configuration de la Plateforme ;
- L'activation du Service et la fourniture du ou des Portails

Dès que le Service est activé et que les Portails liés au Service sur la Plateforme sont fournis au Client pour les domaines e-mail demandés par ce dernier, le Service est considéré comme mis à sa disposition.

Afin d'éviter tout malentendu, Proximus attire l'attention du Client sur le fait que sauf accord explicite décrit dans le Bon de commande, l'implémentation du Service par Proximus ne couvre pas les activités suivantes :

- Activation de la Plateforme pour plus de 5 noms de domaine. Il est possible de demander l'activation et la configuration de domaines supplémentaires via des crédits de changement.

- Configuration des paramètres de meilleures pratiques suivants sur la Plateforme (le Niveau de service ne s'applique que si ces paramètres ont été configurés par le Client) :
  - activation de spoofed sender detection avec SPF – pour les e-mails entrants et sortants
  - activation de DMARC - e-mails sortants

- Formation
- Création des règles de sécurité pour le Client
- Il incombe au Client de changer le mot de passe du compte d'administrateur dès que ce dernier est transmis au contact technique du Client.

4.4 Acceptation

Au terme de la phase d'implémentation, Proximus invitera le Client à accepter la configuration de la Plateforme. À cet égard, le Client peut vérifier la configuration via le Portail d'administration.

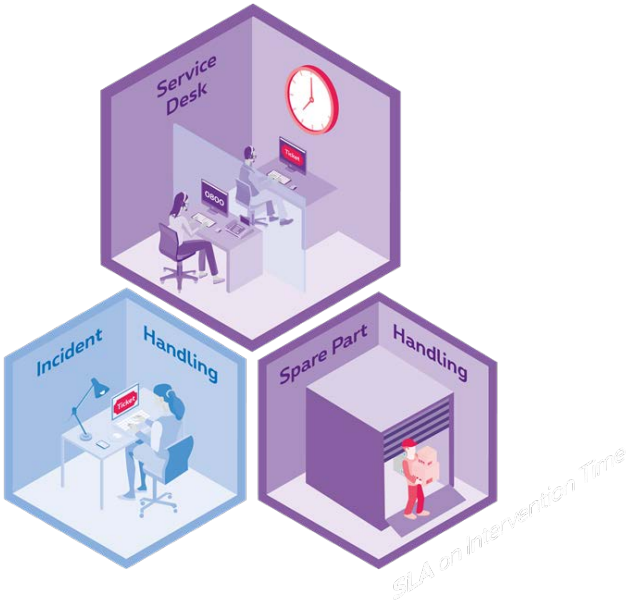
La procédure d'acceptation est décrite dans les Conditions générales pour les Clients professionnels (voir article "Configuration et installation").

5. Phase opérationnelle

Cette section décrit le support fourni par Proximus dès l'acceptation du Service jusqu'au terme de la période contractuelle.

5.1 Formule Reactive Care

Cette section s'applique lorsque le Client a opté pour la Formule Reactive Care. Dans le cadre de cette Formule, le Client bénéficie d'un support **Reactive Care**, c'est-à-dire que Proximus lui fournit un support réactif pour rétablir un fonctionnement normal le plus rapidement possible en cas d'Incidents, grâce aux interventions et aux remplacements de pièce.



5.1.1 Accès au Service Desk

Le Service Desk est l'interface entre le Client et Proximus pour tous les aspects relatifs au Service, y compris la réception, l'enregistrement, la consignation et l'escalade des Incidents et autres demandes. Le Service Desk attribue des ressources (première ligne, deuxième ligne, experts) et communique régulièrement avec le Client.

Proximus octroie au Client un accès centralisé au Service Desk par téléphone ou via le Portail. Seuls les représentants autorisés du Client ont accès au Service Desk (24h/24, 7j/7) via :

Accès au Service Desk	
Téléphone	0800 14888
Portail	https://www.proximus.be/login

Le Client communique au Service Desk le numéro de référence du Contrat concerné.

Le Client sait et accepte expressément que les appels émanant du Service Desk de Proximus ou arrivant au Service Desk de Proximus peuvent être enregistrés afin de servir de preuve en cas de contestation d'une transaction commerciale. Les appels vers ou depuis le service à la clientèle peuvent également être écoutés ou enregistrés, en vue d'un contrôle de la qualité.

5.1.2 Gestion des Incidents

Les activités de gestion des Incidents effectuées par Proximus ont pour but de résoudre un Incident ou d'en diminuer les conséquences dans le cadre du Niveau de service convenu.

Les activités à distance désignent les activités réalisées par Proximus ailleurs que sur le Site du Client.

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

5.1.2.1 Diagnostic à distance

Le Diagnostic à distance sert principalement à évaluer la cause et à confirmer l'impact de l'Incident signalé, au téléphone ou par e-mail. Le Client analyse l'Incident avant de contacter Proximus.

Proximus aidera le Client à réaliser une série d'actions de dépannage élémentaires. Dans certains cas, le Client sera tenu de fournir des informations supplémentaires à Proximus. Les Incidents dus à la configuration de l'Élément de solution (même s'il s'agit de l'Élément de solution concerné pour ce Composant de Service) ne sont pas pris en charge par Proximus.

Le diagnostic à distance permet à Proximus de déterminer les actions à entreprendre pour résoudre l'Incident.

5.1.2.2 Intervention à distance

L'identification d'un problème de Logiciel sur l'outil de synchronisation lors du diagnostic à distance donne lieu à une Intervention à distance, en vérifiant auprès du fournisseur la Disponibilité de patches/Updates pour les suggérer au Client. Le Client se charge de l'installation de ces patches/Updates. L'installation d'un patch/Update n'est pas comprise dans la redevance du Service. Les Incidents dus à la configuration des Éléments de solution (même s'il s'agit de l'Élément de solution concerné pour ce Composant de Service) ne sont pas pris en charge par Proximus.

L'identification d'un problème sur la Plateforme et/ou le Portail d'administration et/ou le portail de mise en quarantaine des spams lors du diagnostic à distance donnera lieu à des interventions de Proximus sur ces Éléments de solution.

5.1.2.3 Restauration de la configuration

Outre les Interventions à distance, Proximus s'efforcera, si la restauration du Service l'exige, de rétablir la configuration de l'Élément de solution concerné, sur la base du dernier back-up de la configuration disponible effectué par Proximus.

À cet égard, Proximus déploiera tous les efforts raisonnables pour effectuer des back-ups de la configuration des Éléments de solution concernés et les mettra à disposition à des fins de restauration en cas d'Incident. Le premier back-up est effectué pendant la phase d'implémentation.

Sauf convention contraire écrite entre les Parties, l'exécution des back-ups est planifiée tous les jours, pendant la nuit. Le back-up de la configuration comprend les logs des changements de configuration depuis la phase d'implémentation, les métadonnées disponibles via l'outil d'administration et les e-mails en quarantaine. La sauvegarde de la configuration effectuée par Proximus ne comprend pas la sauvegarde de toutes autres données du Client.

5.1.3 Updates et Upgrades

Proximus détermine seule les moyens techniques nécessaires pour fournir le Service conformément au Contrat.

Elle décide de déployer des Updates/Upgrades à sa propre discrétion. Proximus n'a aucune obligation de déployer chaque Upgrade et Update que le fournisseur met à sa disposition ou d'étendre l'Élément de

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

solution concerné. Compte tenu du fait que le Service se base sur une plateforme cloud, le Client ne peut pas refuser ces Updates/Upgrades.

5.1.4 Back-up de la configuration

Proximus déploiera tous les efforts raisonnables pour effectuer des back-ups de la configuration des Éléments de solution concernés et les mettra à disposition à des fins de restauration en cas d'Incident.

Le premier back-up est effectué pendant la phase d'implémentation.

Sauf convention contraire écrite entre les Parties, l'exécution des back-ups est planifiée tous les jours, pendant la nuit. Le back-up de la configuration comprend les logs des changements de configuration depuis la phase d'implémentation, les données disponibles via la fonctionnalité de traçage du message et les e-mails en quarantaine.

La sauvegarde de la configuration effectuée par Proximus ne comprend pas la sauvegarde de toutes autres données du Client.

5.2 Formule Full Care

Cette section s'applique lorsque le Client a opté pour la Formule Full Care. Dans le cadre de cette Formule, le Client bénéficie d'un support **Full Care**, c'est-à-dire que Proximus lui fournit un support réactif pour rétablir un fonctionnement normal le plus rapidement possible en cas d'Incidents, grâce aux interventions et aux remplacements de pièce, ainsi qu'à la gestion, au contrôle et au reporting de la configuration des Éléments de Solution concernés.

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

5.2.1 Accès au Service Desk

Le Service Desk est l'interface entre le Client et Proximus pour tous les aspects relatifs au Service, y compris la réception, l'enregistrement, la consignation et l'escalade des Incidents et autres demandes. Le Service Desk attribue des ressources (première ligne, deuxième ligne, experts) et communique régulièrement avec le Client.

Proximus octroie au Client un accès centralisé au Service Desk par téléphone ou via le Portail. Seuls les représentants autorisés du Client ont accès au Service Desk (24h/24, 7j/7) via :

Accès au Service Desk	
Téléphone	0800 14888
Portail	https://www.proximus.be/login

Le Client sait et accepte expressément que les appels en provenance ou à destination du Service Desk de Proximus peuvent être enregistrés afin de servir de preuve en cas de contestation d'une transaction commerciale. Les appels vers ou depuis le service à la clientèle peuvent également être écoutés ou enregistrés, en vue d'un contrôle de la qualité.

.

5.2.2 Gestion des Incidents

Les activités de gestion des Incidents effectuées par Proximus ont pour but de résoudre un Incident ou d'en diminuer les conséquences dans le cadre du Niveau de service convenu.

Les activités à distance désignent les activités réalisées par Proximus à un autre endroit que sur le Site du Client.

5.2.2.1 Diagnostic à distance

Le diagnostic à distance a pour but d'évaluer et d'analyser l'Incident rapporté, d'en déterminer la cause et d'en valider l'impact – oralement ou en accédant à l'environnement du Client via une connexion à distance.

Proximus prendra toutes les mesures nécessaires pour déterminer la cause de l'erreur et localiser le composant défectueux. Ces mesures incluent l'identification des problèmes de performance et des problèmes liés aux fichiers de configuration.

Le diagnostic à distance permet à Proximus de déterminer les actions à entreprendre pour résoudre l'Incident.

5.2.2.2 Intervention à distance

Si une solution provisoire ou permanente a été identifiée et pour autant que l'Incident puisse se résoudre, Proximus entamera une intervention à distance en étroite collaboration avec le Client. Ce dernier est informé à intervalles réguliers de l'état d'avancement de l'intervention.

Proximus restaure la configuration de l'Élément de solution concerné à un état de fonctionnement correspondant au dernier back-up de configuration disponible.

5.2.3 Gestion de la configuration

Les activités de gestion de la configuration effectuées par Proximus aux termes du Contrat ont pour but, dans les limites définies dans la présente section, de :

- gérer la configuration des Éléments de solution concernés
- réaliser un back-up de la configuration de l'Élément de solution concerné
- mettre en œuvre les Changements de la configuration des Éléments de solution concernés
- maintenir à jour le Logiciel concerné

5.2.3.1 Gestion de la configuration et de l'accès

La présente section définit les droits de gestion d'accès détenus par Proximus et le Client en rapport avec l'Élément de solution dans le cadre de ce Composant de Service.

5.2.3.1.1 Gestion de la configuration avec droit de lecture du Client

Proximus recueille et documente les informations à jour concernant l'Élément de solution concerné et utilise des processus planifiés et dans certains cas automatisés pour s'efforcer de maintenir à jour l'Élément de solution.

Proximus met tout en œuvre pour maintenir l'Élément de solution concerné en bon état de fonctionnement. À cet égard, Proximus utilise une plateforme de gestion sécurisée et centralisée avec des droits d'accès. Pour résoudre plus rapidement les problèmes, toutes les activités de cette plateforme sont enregistrées.

Proximus détient tous les droits d'administrateur sur l'Élément de solution pour le compte du Client, même si ce dernier est propriétaire de ce même Élément de solution. Le Client dispose de droits de lecture pour les Éléments de solution concernés. Seuls les représentants autorisés du Client ont accès à la configuration des Éléments de solution via la même plateforme de gestion sécurisée et centralisée avec des droits de lecture seule.

5.2.3.1.2 Gestion de la configuration avec droits d'accès spécifiques

Proximus recueille et documente les informations à jour concernant l'Élément de solution concerné et utilise des processus planifiés et dans certains cas automatisés pour s'efforcer de maintenir à jour l'Élément de solution.

Proximus met tout en œuvre pour maintenir l'Élément de solution concerné en bon état de fonctionnement. À cet égard, Proximus utilise une plateforme de gestion sécurisée et centralisée avec des droits d'accès. Pour résoudre plus rapidement les problèmes, toutes les activités de cette plateforme sont enregistrées.

Proximus détient, pour le compte du Client, tous les droits d'administrateur de l'Élément de solution concerné, même si le Client en est le propriétaire. Le Client dispose de droits d'accès spécifiques pour apporter des Changements limités. Seuls les représentants autorisés du Client ont accès à la configuration des Éléments de solution via la même plateforme de gestion sécurisée et centralisée avec des droits d'accès limités.

Le Client est autorisé à apporter uniquement les Changements suivants aux Éléments de solution concernés :

- création de comptes
- création de groupes de comptes
- création d'alias
- accès à différents comptes
- suppression de comptes

Proximus décline toute responsabilité pour les conséquences éventuelles de Changements effectués par le Client ou des tiers.

5.2.3.1.3 Gestion de la configuration sans droits d'accès

Proximus recueille et documente les informations à jour concernant l'Élément de la solution concerné et utilise des processus planifiés et dans certains cas automatisés pour s'efforcer de maintenir à jour l'Élément de solution.

Proximus met tout en œuvre pour maintenir l'Élément de solution concerné en bon état de fonctionnement. À cet égard, Proximus utilise une plateforme de gestion sécurisée et centralisée avec des droits d'accès. Pour résoudre plus rapidement les problèmes, toutes les activités de cette plateforme sont enregistrées.

Proximus détient tous les droits d'administrateur sur l'Élément de solution concerné pour le compte du Client et ce, même si ce dernier est propriétaire de ce même Élément de solution. Le Client n'a aucun droit d'accès ni d'administrateur et n'est pas autorisé à modifier de quelque manière que ce soit l'Élément de solution ou les interfaces.

5.2.3.2 Back-up de la configuration

Proximus déploiera tous les efforts raisonnables pour effectuer des back-ups de la configuration des Éléments de solution concernés et les mettra à disposition à des fins de restauration en cas d'Incident.

Le premier back-up est effectué pendant la phase d'implémentation.

Sauf convention contraire écrite entre les Parties, l'exécution des back-ups est planifiée tous les jours, pendant la nuit. Le back-up de la configuration comprend les logs des changements de configuration

depuis la phase d'implémentation, les données disponibles via la fonctionnalité de traçage du message et les e-mails en quarantaine.

La sauvegarde de la configuration effectuée par Proximus ne comprend pas la sauvegarde de toutes autres données du Client.

5.2.3.3 Gestion des Changements

La gestion des Changements a pour but d'offrir au Client la possibilité de demander des Changements au niveau de la configuration de l'Élément de solution pendant la durée du Contrat. Ces Changements n'ont aucun impact sur la redevance récurrente du Service.

Deux types de Changements sont possibles : les Changements standard et les Changements personnalisés. Pour pouvoir demander ces Changements, le Client doit avoir conclu un Contrat de gestion des Changements distinct.

Tout Changement impliquant un changement de redevance de Service fera l'objet d'un nouveau Bon de commande ou d'un avenant.

5.2.3.4 Updates et Upgrades

Proximus détermine seule les moyens techniques nécessaires pour fournir le Service conformément au Contrat.

Elle décide de déployer des Updates/Upgrades à sa propre discrétion. Proximus n'a aucune obligation de déployer chaque Upgrade et Update que le fournisseur met à sa disposition ou d'étendre l'Élément de solution concerné. Compte tenu du fait que le Service se base sur une plateforme cloud, le Client ne peut pas refuser ces Updates/Upgrades.

5.2.4 Surveillance

Les activités de surveillance effectuées par Proximus aux termes du présent Contrat permettront à Proximus de recueillir les informations relatives au statut des Éléments de solution concernés et ce, 7 jours sur 7 et 24 heures sur 24. Si un événement pertinent (au sens décrit plus bas) est détecté, Proximus entamera les activités de gestion des Incidents. Les Clients sont informés par la création d'un Ticket d'Incident.

Aux termes du Contrat, Proximus effectue les activités de contrôle suivantes :

5.2.4.1 Contrôle de la Disponibilité du Service

La plateforme de contrôle centrale vérifie la Disponibilité du Service concerné. Les contrôles de la Disponibilité du Service comprennent la vérification du bon fonctionnement des applications ou processus pertinents.

Les activités de gestion des Incidents sont entamées en cas de détection de problèmes de Disponibilité du Service.

5.2.5 Reporting

Proximus fournit au Client des rapports reprenant les informations recueillies via les activités de contrôle effectuées dans le cadre du présent Contrat. Le Client peut consulter le statut des paramètres pertinents via le lien mentionné dans la documentation relative au Service.

Les rapports fournis par Proximus dans le cadre du Contrat sont les suivants :

5.2.5.1 Reporting sur la Disponibilité du Service

Ce reporting fournit un reporting basé sur le contrôle de la Disponibilité du Service.

6. Niveaux de Service

Cette section décrit les Niveaux de service applicables. Les Niveaux de service comprennent le Service Level Objective (SLO) et le Service Level Agreement (SLA). Ils sont décrits dans les tableaux ci-dessous.

6.1 Champ d'application

Ces Niveaux de service sont applicables dès l'activation du Service et la réception des identifiants, dans les Fenêtres de service décrites ci-dessous.

Les Niveaux de service ne s'appliquent qu'au Service décrit dans le présent document et aux Incidents relevant de la responsabilité de Proximus.

Sont exclus du calcul du Niveau de service (application du principe "Stop-Clock") :

- les Incidents, retards ou événements empêchant Proximus de fournir le Service, imputables au Client, à un cas de force majeure ou à un tiers, et
- les heures non comprises dans la Fenêtre de service, et
- les e-mails qui n'ont pas transité par le Service si le Client n'a pas pris les mesures appropriées pour garantir qu'il n'acceptera que les e-mails entrants au départ du Service, et
- les e-mails entrants ou sortants initialement envoyés au Service, qui contiennent plus de 500 destinataires par session SMTP, et
- les Travaux planifiés (en ce compris l'Interruption de maintenance), et
- les Clients dont le provisioning est effectué sur une Tower désignée comme Bulk Cluster Tower (c.-à-d. plusieurs serveurs à charge équilibrée dans plusieurs localisations) ;
- tous les e-mails entrants et sortants pour des adresses e-mail ne faisant pas partie de la Liste de validation, et,
- si les paramètres de meilleures pratiques à implémenter par le Client comme défini dans la section "Phase d'implémentation" n'ont pas été configurés ou mis à jour pendant la durée du Contrat (voir également l'Annexe 1). Cette disposition s'applique à tous les éléments du Niveau de service.

Aucun Niveau de service n'est applicable en cas de Support à la demande.

6.2 SLO et SLA

Le SLO définit une obligation de moyens. Le non-respect de ce SLO ne peut dès lors pas être considéré comme un manquement grave. Aucun crédit de Service ne peut être exigé en cas de manquement.

Le SLA définit une obligation de résultat. En cas de non-respect du SLA, le Client est en droit d'obtenir les crédits de Service de Proximus énumérés dans le tableau ci-dessous. Sauf si le Client a souscrit à un contrat de gestion de service, le Client est tenu de les réclamer personnellement, puisque Proximus ne les fournit pas de manière proactive.

Pour recevoir un crédit de Niveau de service, le Client doit soumettre la notification du non-respect du Niveau de service à Proximus dans les cinq (5) Jours ouvrables suivant la fin du mois calendrier où le non-

respect du Niveau de service a été constaté. Les crédits de Service constituent l'unique compensation en cas de non-respect par Proximus de son SLA.

Le Client ne pourra toutefois pas réclamer de crédits de Service (1) en cas de non-paiement des factures Proximus concernant ce Contrat ou un autre contrat ou (2) en cas de violation du Contrat pendant la durée de l'Incident ou de l'événement. Si le Contrat prend fin ou est résilié avant l'attribution du crédit de Service, ce dernier sera considéré comme nul dès la date de fin ou de résiliation du Contrat.

6.3 Fenêtres de service

Les Niveaux de service s'appliquent dans les limites de la Fenêtre de service sélectionnée.

On entend, par Fenêtre de service, la période durant laquelle s'accomplissent les activités de gestion des Incidents.

Nom de la Fenêtre de service	*Acronyme*	*S'applique à*	*Heures de Fenêtre de service*
24*7	24*7	*Tous les éléments de la Solution*	*24*7*

6.3.1 Fenêtre de mise en œuvre des Changements standard

La Fenêtre de mise en œuvre des Changements est la fenêtre durant laquelle les Changements standard seront effectués dans le cadre du présent Service. La Fenêtre de mise en œuvre des Changements standard est la suivante :

Heures de Service standard	SSH	*Du lundi au vendredi de 8 h à 18 h*

6.4 Priorité de l'Incident

Si le Client détecte un Incident, il peut contacter le Service Desk. Le Service Desk assignera une priorité à l'Incident en se basant sur l'impact de l'Incident.

Définition des priorités

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

P1*	Interruption complète du Service
P2	Détérioration grave du Service (fonctions critiques pour les activités) ou activation du back-up
P3	Impact limité (processus d'entreprise disponibles)
P4	Pas d'impact/demande d'info

S'il apparaît, à la lumière du diagnostic, que l'impact de l'Incident ne correspond pas à celui mentionné par le Client lors de la création du Ticket, Proximus corrigera la priorité assignée à l'Incident.

*Les Incidents P1 doivent être consignés en contactant le Service Desk (uniquement par téléphone).

6.5 Description du Niveau de service

6.5.1 Formule Reactive Care

KPI de SLA	Définition	S'applique à	Objectif	Valable pour	Crédits de service
Délai de réaction à des Incidents	Le délai pendant la Fenêtre de service convenue, entre la création du Ticket et le début de l'intervention par Proximus, moins le temps perdu en raison d'un événement pour lequel le principe "Stop-Clock" est applicable.	Diagnostic à distance pour tous les Éléments de la solution	30 minutes	Incidents P1	10 % de la redevance mensuelle pour chaque Incident P1 validé et impliquant le non-respect du SLA, avec un montant maximum de 25 % de la redevance mensuelle

Efficacité antispam	Le Niveau de service correspond au taux de spams capturés, exprimé sous forme de pourcentage de l'ensemble du trafic e-mail envoyé à une adresse e-mail de la Liste de validation. Ce SLA sera uniquement applicable si le Client a implémenté et mis à jour les paramètres des meilleures pratiques en matière d'antispam, comme décrit à l'Annexe 1.	Portail d'administration Portail de mise en quarantaine des spams	> 99 %	N/A	98 % > X ≥ 99 % : 5 % 97 %> X ≥ 98 % : 10 % 96 % > X ≥ 97 % : 15 % 96 % > X : 20 % de la redevance mensuelle
Précision de l'antispam	Ce Niveau de service définit le taux maximal de spams faux positifs en tant que pourcentage de tout le trafic e-mail à destination, et si configuré, au départ d'une adresse e-mail valide de la Liste de validation. Ce SLA s'applique uniquement si le Client a implémenté et mis à jour les	Portail d'administration Portail de mise en quarantaine des spams	≤ 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 % de la redevance mensuelle

	paramètres des meilleures pratiques comme décrit à l'Annexe 1. Les e-mails suivants ne constituent pas des e-mails spams faux positifs dans le cadre de ce Niveau de service : a) e-mails qui ne sont pas des e-mails professionnels légitimes ; b) e-mails contenant plus de 20 destinataires ; c) e-mails pour lesquels l'expéditeur figure sur la liste des expéditeurs bloqués du Client, comme notamment, mais non exclusivement ceux définis par l'utilisateur individuel si le Client a activé des paramètres au niveau de l'utilisateur ; d) e-mails envoyés au départ d'un appareil infecté ; e) e-mails envoyés au				

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

	départ d'un appareil figurant sur la liste de blocage d'un tiers ; f) e-mails interceptés dans le cadre du scan des spams sortants.				
Efficacité de l'antivirus	Nombre de virus enregistrés introduits via le Service et confirmés par Proximus.	Portail d'administration Plateforme	0 par mois calendrier ou si un virus est envoyé en pièce jointe d'un e-mail et qu'il est détecté mais pas stoppé, le Client en est suffisamment informé pour lui permettre d'identifier et de supprimer l'e-mail infecté.	N/A	100 % de la redevance mensuelle avec un montant maximum de 5.000 EUR
Précision de l'antivirus	Ce Niveau de service définit le taux maximal d'interception de virus faux positifs, exprimé sous forme de pourcentage de tout le trafic e-mail à destination, et si configuré, au départ des adresses e-mail de la Liste de validation.	Portail d'administration Plateforme	≤ 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 de la redevance mensuelle
Latence des e-mails	Le Niveau de service relatif à la latence des e-mails est défini par le Round Trip Time moyen,	Portail d'administration Plateforme	Round Trip Time moyen de 60 secondes par mois calendrier	N/A	60 secondes < X ≤ 90 secondes : 5 % 90 secondes

	tel que mesuré par le Symantec.cloud Tracker, pour les e-mails envoyés pour les e-mails envoyés toutes les cinq (5) minutes au départ et à destination du Service.				< X ≤ 120 secondes : 10 % 120 secondes < X ≤ 150 secondes : 15 % 150 secondes < X : 20 % de la redevance mensuelle

Le montant total des Crédits de service accordés au Client conformément au présent Contrat dans le cadre d'un SLA au cours de n'importe quel mois calendrier ne dépassera pas les redevances mensuelles payées par le Client pour le Service, sauf mention contraire.

KPI de SLO	Définition	S'applique à	Objectif	V
Délai de création des Tickets d'Incident	Le délai entre la notification de l'Incident (via le Service) et la création d'un Ticket d'Incident dans le système de Tickets.	Accès au Service Desk pour tous les Éléments de la solution	15 minutes	I
Délai de réaction à des Incidents	Le délai pendant la Fenêtre de service convenue, entre la création du Ticket et le début de l'intervention par Proximus, moins le temps perdu en raison d'un événement pour lequel le principe "Stop-Clock" est applicable.	Diagnostic à distance pour tous les Éléments de la solution	1 heure	I

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

6.5.2 Formule Full Care

KPI de SLA	Définition	S'applique à	Objectif	Valable pour	Crédits de service
Délai de réaction à des Incidents	Le délai pendant la Fenêtre de service convenue, entre la création du Ticket et le début de l'intervention par Proximus, moins le temps perdu en raison d'un événement pour lequel le principe "Stop-Clock" est applicable.	Diagnostic à distance pour tous les Éléments de la solution	30 minutes	Incidents P1	10 % de la redevance mensuelle pour chaque Incident P1 validé et impliquant le non-respect du SLA, avec un montant maximum de 25 % de la redevance mensuelle
Délai de restauration du Service	Le délai de restauration du Service se définit comme la période comprise entre la création et la Résolution d'un Incident au niveau de l'Élément de solution, pendant la Fenêtre de service convenue, moins le temps perdu en raison d'un événement pour lequel le principe "Stop-Clock" est applicable.	Intervention à distance pour tous les Éléments de la solution	4 heures	Incidents P1	25 % de la redevance mensuelle pour chaque Incident P1 validé et impliquant le non-respect du SLA, avec un montant maximum de 50 % de la redevance mensuelle
Disponibilité annuelle du Service	La Disponibilité du Service est calculée comme suit : 100 % *(1 – durée nette d'interruption du Service/durée totale (24x7)) = % de la Disponibilité du Service La durée nette d'interruption correspond à la durée d'indisponibilité d'un Élément	Disponibilité du Service pour la Plateforme	99,95 %	Incidents P1	25 % de la redevance mensuelle pour chaque Incident P1 validé et impliquant le non-respect du SLA, avec un montant maximum de 50 % de la redevance mensuelle*

	de la solution pendant la Fenêtre de service en raison d'un Incident P1, moins le temps perdu en raison d'un événement pour lequel le principe "Stop-Clock" est applicable et où la durée totale correspond à la période de calcul de la Disponibilité. Pour ce Service, la Disponibilité du Service est définie par la capacité à établir une session SMTP sur le port 25 à partir du MTA du Client vers l'infrastructure du Service Infrastructure, conformément à RFC5321. Ce Niveau de service n'est pas applicable si le Client n'a pas correctement configuré le Service (cf. Paramètres des meilleures pratiques à l'Annexe 1).				
Fenêtre de mise en œuvre des Changements standard	Délai de mise en œuvre des Changements standard, calculé à partir de l'enregistrement de la demande de Changement standard (moment où le Ticket de Changement est créé) jusqu'à la fin de sa mise en œuvre par Proximus (clôture du Ticket de Changement).	Changements standard	> 95 % exécutés en 3 Jours ouvrables	N/A	95 > X ≥ 90 % : 5 % 90 > X ≥ 80 % : 10 % 80 % > X : 25 % de la redevance mensuelle des crédits de Changement
Efficacité antispam	Le Niveau de service correspond au taux de spams interceptés en tant que pourcentage de l'ensemble du trafic e-	Portail d'administration Portail de mise en quarantaine des spams	> 99 %	N/A	98 % > X ≥ 99 % : 5 % 97 % > X ≥ 98 %: 10 % 96 % > X ≥ 97 % : 15 %

	mail envoyé à une adresse e-mail de la Liste de validation. Ce SLA s'applique uniquement si le Client implémente et met à jour les paramètres de meilleures pratiques comme décrit à l'Annexe 1.				96 % > X : 20 % de la redevance mensuelle
Précision de l'antispam	Ce Niveau de service définit le taux maximal de spams faux positifs en tant que pourcentage de tout le trafic e-mail. Ce SLA s'applique uniquement si le Client implémente et met à jour les paramètres de meilleures pratiques comme décrit à l'Annexe 1. Les e-mails suivants ne constituent pas des e-mails spams faux positifs dans le cadre de ce Niveau de service : a) e-mails qui ne sont pas des e-mails professionnels légitimes ; b) e-mails contenant plus de 20 destinataires ; c) e-mails pour lesquels l'expéditeur figure sur la liste des expéditeurs bloqués du Client, comme notamment, mais non exclusivement ceux définis par l'utilisateur individuel si le Client a activé des paramètres au niveau de l'utilisateur ; d) les e-mails envoyés au départ d'un appareil infecté ;	Portail d'administration Portail de mise en quarantaine des spams	≤ 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 % de la redevance mensuelle

	e) les e-mails envoyés au départ d'un appareil figurant sur la liste de blocage d'un tiers ; f) e-mails interceptés dans le cadre du scan des spams sortants.				
Efficacité de l'antivirus	Nombre de virus enregistrés, introduits via le Cloud Mail Security Service et confirmés par Proximus	Portail d'administration	0 par mois calendrier ou si un virus est envoyé en pièce jointe d'un e-mail et qu'il est détecté mais pas stoppé, le Client en est informé de manière adéquate pour lui permettre d'identifier et de supprimer l'e-mail infecté.	N/A	100 % de la redevance mensuelle avec un montant maximum de 5.000 EUR
Précision de l'antivirus	Ce Niveau de service définit le taux maximal d'interception de virus faux positifs en tant que pourcentage de tout le trafic e-mail.	Portail d'administration	≤ 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 de la redevance mensuelle
Distribution des e-mails	Le Niveau de service relatif à la distribution des e-mails est défini par le pourcentage de tous les e-mails envoyés à destination ou au départ du Client, compte tenu des	Portail d'administration Plateforme	100%	N/A	Le Client peut résilier le Service moyennant un préavis écrit.

	conditions suivantes : a) Les e-mails doivent avoir été reçus par le Service, et b) Les e-mails ne doivent pas comporter de logiciel malveillant, de spam ou de contenu ayant donné lieu à son interception par le Service.				
Latence des e-mails	Le Niveau de service relatif à la latence des e-mails est défini par le Round Trip Time moyen, tel que mesuré par le Symantec.cloud Tracker, pour les e-mails envoyés pour les e-mails envoyés toutes les cinq (5) minutes au départ et à destination du Service.	Portail d'administration Plateforme	Round Trip Time moyen de 60 secondes par mois calendrier	N/A	60 secondes < X ≤ 90 secondes : 5 % 90 secondes < X ≤ 120 secondes : 10 % 120 secondes < X ≤ 150 secondes : 15 % 150 secondes < X : 20 % de la redevance mensuelle

Le montant total des crédits de service accordés au Client conformément au présent Contrat dans le cadre d'un SLA au cours de n'importe quel mois calendrier ne dépassera pas les redevances récurrentes payées par le Client pour le Service.

KPI de SLO	Définition	S'applique à	Objectif	Valable pour	Crédits de service
Délai de création des Tickets d'Incident	Le délai entre la notification de l'Incident (via le Service) et la création d'un Ticket d'Incident dans le système de Tickets.	Accès au Service Desk pour tous les Éléments de la solution	15 minutes	Incidents P1 et P2	Néant
Délai de réaction à des Incidents	Le délai pendant la Fenêtre de service convenue, entre la création du Ticket et le début de l'intervention par Proximus, moins le temps perdu en raison d'un	Diagnostic à distance	30 minutes	Incidents P2	Néant

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

	événement pour lequel le principe "Stop-Clock" est applicable.	pour tous les Éléments de la solution			
Délai de restauration du Service	Le délai de restauration du Service se définit comme la période comprise entre la création et la Résolution d'un Incident au niveau de l'Élément de solution, pendant la Fenêtre de service convenue, moins le temps perdu en raison d'un événement pour lequel le principe "Stop-Clock" est applicable.	Intervention à distance Tous les Éléments de la solution	6 heures	Incidents P2	Néant

Proximus SA de droit public, Bd du Roi Albert II, 27, B-1030 Bruxelles, Belgique
TVA BE 0202.239.951, RPM Bruxelles, BE61 0001 7100 3017 BPOTBEB1

7. Conditions spécifiques

7.1 Informations générales

7.1.1. Les Conditions spécifiques complètent les Conditions générales pour les Clients professionnels et la présente Description de service contractuelle. Elles définissent les droits et obligations de Proximus et du Client concernant la fourniture du Service décrit dans le présent document.

7.1.2. Le Service est disponible uniquement pour un Client qui dispose de son propre nom de domaine et qui est en mesure de configurer les enregistrements MX et/ou DNS pour ce nom de domaine.

7.2 Procédure contractuelle

7.2.1 Durée

Par dérogation aux Conditions générales, le contrat est conclu pour une durée indéterminée prenant cours à l'activation du Service.

7.2.2 Résiliation et effets de la résiliation

7.2.2.1. Par dérogation aux Conditions générales, le Client peut résilier le Contrat à tout moment par écrit. Si Proximus reçoit la signification de la résiliation au plus tard le 15 du mois en cours, la résiliation du Contrat prendra effet le dernier jour calendrier du mois en cours. Si Proximus reçoit la signification de la résiliation après le 15 du mois en cours, la résiliation du Contrat prendra effet le dernier jour calendrier du mois suivant. Proximus est en droit de facturer le Service fourni et d'être payée pour celui-ci jusqu'à la date de résiliation effective.

7.2.2.2. À la résiliation du présent Contrat, Proximus désactive le Service et tout compte fourni dans le cadre de celui-ci. Les changements de configuration apportés lors de la fourniture du Service sont annulés. En cas de résiliation du Contrat, le Client s'engage à ne plus utiliser le Service et à détruire toute la documentation reçue de Proximus et toutes les copies, y compris les copies partielles, du Logiciel mis à la disposition du Client dans le cadre du Service. Le Client certifiera que le Logiciel a été effacé de tous les appareils, mémoires informatiques et appareils de stockage sous le contrôle du Client et que la documentation a été détruite. Le Client effectuera les changements de configuration nécessaires afin de remettre l'environnement dans son état initial.

7.2.2.3. Le contenu hébergé par Proximus dans le cadre de ce Service (à savoir les e-mails en quarantaine, les données disponibles via la fonction de traçage des données et le log de configuration) ne

sera plus disponible après la résiliation du Service pour quelque raison que ce soit. Par conséquent, le Client est tenu de prendre les mesures qui s'imposent avant la résiliation du Contrat pour exporter son contenu via le Portail d'administration (il est possible d'exporter des logiciels malveillants moyennant demande spécifique adressée à Proximus).

7.2.3 Suspension

7.2.3.1. En cas de suspension du Service, le Client sera redevable de la redevance normale. En outre, Proximus sera en droit de réclamer des frais de réactivation.

7.2.3.2. En cas de suspension du Service pour quelque raison que ce soit, il ne s'appliquera plus aux e-mails entrants du Client (ni aux e-mails sortants si la commande porte également sur les e-mails sortants). Ces e-mails ne seront pas routés via la Plateforme. Le Client est chargé de rediriger ses e-mails pendant la suspension et de confirmer que toutes les configurations sont exactes si le Service est rétabli.

7.2.4 Extension ou réduction du nombre d'adresses e-mail

7.2.4.1. Durant la période contractuelle, le Client peut augmenter à tout moment le nombre d'adresses e-mail prévu dans le cadre du Contrat. Toute demande écrite formulée par le Client pour augmenter le nombre d'adresses e-mail sera exécutée et facturée dès la date d'enregistrement de la demande par Proximus.

7.2.4.2. Durant la période contractuelle, le Client peut réduire à tout moment le nombre d'adresses e-mail prévu dans le cadre du Contrat. Sans préjudice du nombre minimal d'adresses e-mail requises stipulé dans le Contrat, toute demande écrite du Client visant à diminuer le nombre de mailboxes sera exécutée et facturée dès le premier jour du mois suivant à condition que la date d'enregistrement de la demande par Proximus ait lieu au plus tard le 15 du mois en cours. Si Proximus enregistre la demande après le 15 du mois en cours, celle-ci sera effectuée et facturée dès le premier jour du deuxième mois suivant.

7.2.4.3. Si des mesures spécifiques s'imposent pour permettre l'augmentation ou la réduction du nombre de licences, Proximus en informera le Client. Le Client s'engage à prendre ces mesures dans les délais communiqués par Proximus. À défaut, le Client accepte que Proximus ne puisse pas exécuter sa demande. Le mois en question sera facturé sur la base des règles précédemment applicables.

7.3 Droit d'utilisation

7.3.1. Conformément aux conditions du Contrat et moyennant le paiement de la redevance du Service par le Client, Proximus octroiera à ce dernier, dès la date d'activation du Service, un droit non cessible, non

sous-licenciable, non permanent et non exclusif d'accès au Service et d'utilisation et/ou bénéfice de ce dernier pendant toute la durée du Contrat.

7.3.2. Le Client utilise le Service conformément au Contrat et à la politique d'utilisation acceptable publiée par le fournisseur de Proximus (Symantec) sous le lien suivant https://www.symantec.com/content/dam/symantec/docs/eulas/policy/online-services-acceptable-use-policy-v6-en.pdf (ou tout autre lien ajouté ultérieurement) et à concurrence du nombre maximal pour lequel il a été commandé. Le non-respect ou la violation de cette politique d'utilisation acceptable constitue une violation du Contrat. Proximus se réserve le même droit que son fournisseur.

7.3.3. Le Client s'abstiendra (et n'autorisera ou ne permettra pas de tels comportements de la part de tiers, y compris tout Utilisateur final) de copier ou d'utiliser intégralement ou partiellement le Service, sauf dans les cas expressément autorisés par le présent Contrat, d'utiliser le Service sur des équipements ou produits non autorisés, d'utiliser le Service d'une manière susceptible d'endommager, de perturber ou de désactiver le fonctionnement du Service, de modifier le Service ou de s'en inspirer pour traduire ou créer des travaux dérivés, d'effectuer de l'ingénierie inverse, de décompiler, décrypter, désassembler ou réduire le Service à un format lisible par l'homme, sauf dans les cas autorisés par la loi, de modifier ou d'enlever toute légende ou indication de propriété figurant sur ou dans le Service et d'utiliser le Service en violation des droits d'autres parties. Le Service inclut tout Portail et tout Logiciel mis à la disposition du Client dans le cadre du Contrat.

7.4 Modifications apportées au Contrat

7.4.1. Proximus est en droit de revoir le Service et le Contrat à tout moment, sans notification préalable, pour les raisons suivantes : (i) nécessité découlant des lois applicables et des normes du secteur ; (ii) nécessité justifiée par des raisons technologiques lorsqu'un changement est effectué sans dégrader substantiellement la fonctionnalité du Service; (iii) nécessité de maintenir à niveau le fonctionnement du Service lorsqu'un changement est effectué sans dégrader substantiellement la fonctionnalité du Service ; ou (iv) changements en faveur du Client. En continuant à utiliser le Service, le Client marque son accord sur ces changements.

7.4.2. Dans d'autres cas, la procédure décrite dans les Conditions générales pour les Clients professionnels sera applicable.

7.5 Droits et obligations du Client

7.5.1. Le Client désignera une ou plusieurs personnes possédant les compétences, les connaissances et/ou l'expérience adéquates pour superviser le Service, évaluer la pertinence et les résultats du Service et endosser la responsabilité de ces résultats.

7.5.2. Le Client garantit que seules les personnes autorisées pourront accéder au Service et aux portails sécurisés mis à sa disposition dans le cadre du présent Contrat. Sans préjudice des Conditions générales pour les Clients professionnels, le Client respectera toute norme technique ou de sécurité imposée de temps à autre par Proximus pour se connecter au Service. Proximus ne peut vérifier le bien-fondé des demandes d'accès ni de l'utilisation du Service et décline toute responsabilité concernant les conséquences résultant d'un accès frauduleux ou erroné ou d'une utilisation frauduleuse ou erronée. Le Client informera immédiatement Proximus par écrit de tout changement intervenant dans les données d'identification des personnes autorisées.

7.5.3. Le Client rapportera dûment et sans délai tout Incident lié au Service et toute adaptation technique ou opérationnelle apportée susceptible d'affecter la fourniture du Service par Proximus. Il doit toutefois s'assurer que l'Incident n'a pas été causé par ses soins, ses employés ou son propre équipement.

7.5.4. Le Client garantit que son système (1) ne fait pas office d'Open Relay (c'est-à-dire un serveur e-mail configuré pour recevoir des e-mails d'un tiers inconnu ou non autorisé et les transmettre à un ou plusieurs destinataires qui ne sont pas des utilisateurs du système e-mail auquel le serveur e-mail est connecté), (2) ne fait pas office d'Open Proxy (c'est-à-dire un serveur proxy configuré pour permettre à des tiers inconnus ou non autorisés de consulter, sauvegarder ou transmettre des DNS, pages web ou autres données pour le Service), (3) n'envoie pas de spams (c'est-à-dire des e-mails commerciaux non sollicités), (4) n'envoie ou ne reçoit pas d'e-mails Bulk (c'est-à-dire un groupe de plus de cinq mille (5 000) messages e-mail au contenu largement similaire envoyés ou reçus en une opération unique ou en une série d'opérations liées, ou (5) ne compromet pas la sécurité du Service (notamment via des tentatives de piratage, attaques par déni de service, le mail bombing ou toutes autres activités malveillantes dirigées vers le domaine du Client ou émanant de celui-ci). Proximus se réserve le droit de vérifier à tout moment si le Client respecte cet article. Ces actes seront considérés comme compromettant l'intégrité et le bon fonctionnement du Service et de l'infrastructure sous-jacente. Il en va de même si les systèmes e-mail du Client sont sur liste noire ou si le Client est à l'origine de la mise sur liste noire des systèmes de Proximus (ou des systèmes du Fournisseur de Proximus) à la suite de l'envoi de spams. Sans préjudice des Conditions générales pour les Clients professionnels, Proximus se réserve le droit de facturer au Client tout travail de réparation nécessaire aux tarifs en vigueur.

7.5.6. Le Client fournit et tient à jour pendant toute la durée du Contrat une liste correcte, précise et exhaustive de toutes les adresses e-mail (y compris les alias) qui recevront le Service (la "Liste de validation"). Ces adresses e-mail doivent être associées au domaine mentionné dans le Bon de commande. Les e-mails entrants et sortants envoyés à destination ou au départ d'adresses e-mail non reprises dans la Liste de validation ou introduites de manière incorrecte seront automatiquement bloqués. Proximus décline toute responsabilité si ces e-mails ne peuvent être délivrés à la suite d'erreurs dans les adresses e-mail ou d'omissions d'adresses e-mail. Les Niveaux de service ne s'appliqueront pas à des adresses e-mail non valides. En cas de Formule Reactive Care, le Client introduit lui-même la Liste de validation dans le Portail d'administration. En cas de Formule Full Care, le Client fournit la Liste de validation à Proximus, à charge pour cette dernière de l'introduire dans le Portail d'administration.

7.5.7. Le Client reconnaît expressément avoir reçu de Proximus toutes les informations auxquelles il pouvait raisonnablement s'attendre afin de s'assurer, avant la conclusion du Contrat, que le Service répond à ses besoins et exigences.

7.5.8. Le Client reconnaît et accepte le fait que Proximus a défini ses prix et conclu le présent Contrat compte tenu des exclusions de garantie et de la limitation de responsabilité établies dans le présent

Contrat, que celles-ci reflètent une répartition des risques entre les Parties et constituent un élément fondamental de l'accord conclu entre les Parties.

7.5.9. Le Client s'engage à ne pas utiliser le Service en vue de développer un produit ou service concurrentiel ou de copier ses fonctions ou son interface utilisateur, de procéder à des évaluations ou à toutes autres analyses comparatives destinées à être publiées en dehors de l'organisation du Client sans l'accord écrit préalable de Proximus.

7.5.10. Le Client reconnaît et accepte le fait que le Service (et les Éléments de solution applicables) ainsi que tous les téléchargements ou technologies y afférents ("Technologies contrôlées") peuvent être soumis aux lois, réglementations, règles et licences applicables en matière de contrôle des exportations et de sanctions commerciales, qu'il a connaissance de l'information publiée par le fournisseur de Proximus (Symantec) sur http://www.symantec.com/about/profile/ policies/legal.jsp (ou sur le site web qui lui succédera) et qu'il respectera ce qui précède et les restrictions à l'exportation ultérieures qui peuvent s'appliquer au Service.

7.6 Droits et obligations de Proximus

7.6.1. Le Client reconnaît et accepte le fait que le Service est un service standard qui n'est pas spécialement conçu pour répondre à ses besoins ou attentes professionnels spécifiques. Proximus décline dès lors toute responsabilité en cas de non-respect des objectifs que le Client pourrait s'être fixés dans le cadre du Service. En outre, le Client reconnaît et accepte le fait que Proximus n'a pas d'autres obligations que celles expressément énumérées dans le présent Contrat.

7.6.2. Aucun Service ne peut garantir un taux de détection de 100 % des logiciels malveillants ou du contenu indésirable (spams, images pornographiques, contenu incluant des mots prédéfinis spécifiques, URL bloquée, etc.) ou un taux de protection de 100 % contre un accès non autorisé de tiers. Même si le Service est spécialement conçu pour protéger le réseau et le trafic internet du Client contre ces menaces pour la sécurité ou ce contenu indésirable, Proximus ne fournit aucune garantie quant à la capacité du Service à détecter et rectifier ce contenu indésirable, cet accès non autorisé par des tiers et les menaces pour la sécurité, et à offrir une protection contre ceux-ci. Proximus décline toute responsabilité pour tout préjudice ou perte découlant directement ou indirectement d'un quelconque échec du Service à détecter ces menaces pour la sécurité ou ce contenu indésirable, ou de la mauvaise identification, par le Service, d'un e-mail présumé suspect, qui se révèlera inoffensif par la suite, ou de l'échec du Service à empêcher tout accès non autorisé par des tiers. Conformément aux Conditions générales, Proximus est soumise à cet égard à une obligation de moyen. Sans préjudice de la section "Niveaux de service", Proximus ne garantit pas la non-interruption du Service.

7.6.3. Les activités de maintenance prévues par le présent Contrat sont décrites dans le chapitre "Phase opérationnelle". Le Service n'inclut pas le remplacement ou la réparation de l'Élément de solution affecté ou toute autre intervention de Proximus (l'intervention éventuelle sera néanmoins facturée séparément au tarif actuel en vigueur) (i) en cas d'Incident survenu en raison d'une utilisation ou d'un événement non prévu dans les conditions de fonctionnement normal de l'Élément de solution concerné, (ii) en cas de fourniture d'un Support à la demande ; (iii) en cas d'activités de support afférentes au Logiciel et/ou Matériel que le fabricant ne prend plus en charge, (iv) en cas d'Incident survenu en raison :

a. de causes externes incluant notamment les conditions météo, la fermeture ou coupure de lignes téléphoniques non comprises dans le Service, des pannes de l'air conditionné, des prises défectueuses, des orages, la foudre, des inondations et toute autre cause étrangère à l'Élément

de solution, des facteurs environnementaux inadéquats tels qu'une humidité trop élevée, des températures anormales ou une quantité anormalement élevée de poussière ;

b. d'une utilisation de l'Élément de solution affecté non autorisée par le Contrat ni par une quelconque prescription émanant de Proximus ;
c. d'une utilisation avec l'Élément de solution affecté ou liée à ce dernier pour des éléments non approuvés par Proximus ou du fonctionnement irrégulier de l'élément auquel l'Élément de la solution est connecté ;
d. de l'exécution (ou de la tentative) de maintenance, d'un déménagement, d'une réparation, d'une modification ou d'un Changement au niveau de l'Élément de solution affecté par des personnes autres que Proximus ou autorisées par Proximus sans l'autorisation préalable écrite de Proximus ;
e. d'une négligence ou d'un manquement (par action ou omission) lors de l'utilisation ou l'installation d'un Élément de solution par le Client ou des tiers ;
f. du non-respect par le Client de ses obligations stipulées dans le présent Contrat.

7.6.4. Par dérogation aux Conditions générales, dans le cas où Proximus serait tenue responsable de la perte des données hébergées du Client ou des dommages occasionnés à celles-ci, la responsabilité de Proximus sera limitée par événement, à sa seule discrétion, à la réplication des données au départ des derniers back-ups disponibles réalisés par Proximus dans le cadre du Service ou au montant (à l'exclusion de toute redevance unique) payé par le Client à Proximus pour le Service au cours du mois précédant la cause du dommage.

7.6.5. Proximus décline toute responsabilité pour les pertes, dommages et frais éventuels occasionnés par le Client ou par un tiers à la suite (i) de la délivrance par le Client (ou par Proximus à la demande du Client) d'un e-mail infecté d'un virus ou de tout e-mail mis en quarantaine, (ii) de la suppression, par le Client, d'un e-mail mis en quarantaine, (iii) d'un dysfonctionnement du Service après un changement intentionnel ou non, effectué par le Client ou un tiers, ou (iv) une violation du système de sécurité (acte frauduleux ou attaque) par toute personne (à l'exception des collaborateurs de Proximus). En cas de faute ou de négligence du Client, ce dernier préservera Proximus contre toute plainte, réclamation ou action de tiers (en ce compris les clients, Utilisateurs finaux ou fournisseurs du Client) en la matière.

7.6.6. Proximus ne peut être tenue responsable des dommages, interruptions ou erreurs dans le trafic e-mail du Client résultant de la fourniture, la suspension ou la résiliation du Service ou résultant d'un cas de Force majeure.

7.7 Paiement et facturation

7.7.1 Le Service sera facturé sur une base mensuelle et figurera sur la même facture que les éventuels services télécoms de Proximus souscrits par le Client (à l'exclusion des services mobiles). Tous ces services télécoms seront facturés sur une base mensuelle, quel que soit le moment où ces services ont été souscrits. Le Client reconnaît et accepte le fait que la commande du Service peut influencer la périodicité du cycle de facturation et la date d'envoi des factures relatives à ses services télécoms de Proximus.

7.7.2. La redevance de service classique sera facturée anticipativement au Client (excepté pour le premier cycle de facturation) conformément au tableau des prix figurant dans le Bon de commande et en fonction des adresses e-mail concernées dans le cadre du Contrat.

Toutes les autres redevances (notamment, mais non exclusivement activation, installation, configuration, utilisation (si facturation à l'utilisation), désactivation, réactivation, support spécifique, etc.) seront facturées ultérieurement.

Le Client reconnaît et accepte le fait que ses factures sont basées sur les mesures effectuées par les systèmes de Proximus (ou de ses fournisseurs) pour le cycle de facturation concerné.

7.7.3. La facturation prend cours dès la notification des codes d'identification (mot de passe, nom d'utilisateur, etc.) par Proximus au Client, qu'importe la date d'activation du Service.

7.7.4. Sauf stipulation contraire, les prix n'incluent pas les frais d'équipement nécessaires à l'utilisation du Service ni les frais d'accès internet, de coûts de connexion ou autres formes de transmission de données. Le Client est responsable de tous ces frais accessoires et taxes éventuelles et est légalement tenu au paiement de ces derniers.

7.8 Rapports

Tous les rapports préparés par Proximus dans le cadre du Service sont établis de bonne foi sur la base des informations disponibles au moment concerné. Ils sont exclusivement destinés à un usage interne par le Client. Les tiers ne peuvent les utiliser ni s'y fier sans l'accord écrit préalable de Proximus. Proximus décline toute responsabilité en ce qui concerne tout rapport ou document préparé par ses soins dans le cadre du Service pour toute autre partie que le Client.

7.9 Protection des données à caractère personnel

7.9.1. Proximus intervient en qualité de sous-traitant des données à caractère personnel comprises (1) dans les données de configuration des Éléments de solution, (2) dans les e-mails traités dans le cadre du présent Contrat, (3) dans les données disponibles via l'outil d'administration. Proximus intervient en qualité de responsable du traitement de toutes les autres données à caractère personnel qu'elle traite dans le cadre du présent Contrat.

7.9.2. Si le consentement, l'approbation ou l'autorisation d'une personne autre que le Client est nécessaire afin de permettre à Proximus de fournir le Service, le Client garantit qu'il obtiendra ce consentement, cette approbation ou cette autorisation avant que Proximus ne commence à fournir la partie du Service pour laquelle le consentement, l'approbation ou l'autorisation est nécessaire.

7.9.3. Proximus reconnaît et confirme que le contenu envoyé au Client ou reçu de ce dernier par le Service est confidentiel. Proximus et son fournisseur n'ont pas accès aux e-mails, à leurs pièces jointes ou au contenu associé, s'abstiendront de les lire et de les copier, excepté via des méthodes électroniques à des fins de fourniture du Service. Proximus et son fournisseur se réservent toutefois le droit d'utiliser le contenu lié à un logiciel malveillant et à du spam de ces e-mails, de leurs pièces jointes et du contenu associé, aux seules fins :

- de maintenir et d'améliorer le Service ;
- de se conformer aux décisions judiciaires et à toutes les exigences réglementaires, légales ou contractuelles, et
- de mettre à la disposition du fournisseur toute information passant par le Service et susceptible d'intéresser le fournisseur dans le cadre exclusivement du développement et de l'amélioration du Service.

7.10 Force majeure

Dans le cadre du Service, les cas de Force majeure sont définis comme des faits ou circonstances indépendants de sa volonté, imprévisibles ou inévitables, comme les cas de guerre, d'émeutes, de troubles, d'agitation civile, d'actions de la part d'autorités civiles ou militaires, d'embargos, d'explosions, de faillites d'un donneur de licence ou d'un fournisseur, de grèves ou de conflits sociaux (y compris ceux impliquant son personnel), de coupures de câbles, de coupures d'électricité (en ce compris celles découlant de l'application d'un plan de délestage fixé par les autorités), d'inondations, de gel prolongé, d'incendies ou d'orages découlant de l'application d'un plan de délestage fixé par les autorités), de pénurie de ressources, d'inondations, de gel prolongé, d'incendies ou d'orages.

Compte tenu de la nature spécifique du Service, la possibilité de résiliation pour cas de Force majeure décrite dans les Conditions générales pour les Clients professionnels est accordée aux deux Parties lorsque le cas de Force majeure subsiste pendant plus de 30 Jours calendrier.

7.11 Limitations du Service

Les limites suivantes s'appliquent au Service :

- Le nombre maximal de messages entrants et sortants par Utilisateur est fixé à 10.000 par mois calendrier. Cette limite n'inclut pas les spams et logiciels malveillants adressés au Client.
- Proximus se réserve le droit, moyennant notification, de facturer des Utilisateurs supplémentaires au Client pour les mois restants du Contrat lorsque l'utilisation dépasse le nombre maximal de messages prévu.
- Le système tentera d'envoyer à nouveau les e-mails entrants et sortants pendant 7 Jours calendrier.
- La taille maximale d'un e-mail est fixée par défaut à 50 MB. Le Client peut spécifier une taille maximale jusqu'à 1 000 MB. Les e-mails reçus par le Service qui dépassent la limite spécifiée seront bloqués et supprimés, et un e-mail de notification sera envoyé à l'expéditeur, au destinataire concerné et à un Administrateur.

7.12 Conditions spécifiques du Service

- Les Clients doivent router leurs e-mails entrants via le Service en utilisant les informations de routage fournies par Proximus. Ils ne peuvent pas router les e-mails vers une autre destination.
- Le Client doit accepter les e-mails entrants de toutes les séries IP requises afin d'assurer la continuité du Service si une partie de l' Infrastructure n'est pas disponible.
- Le Client doit spécifier l'(les) adresse(s) IP ou le(s) nom(s) d'hôte du serveur e-mail pour délivrer les e-mails entrants à son organisation.
- Le Client doit veiller à ce que tous les domaines (et les sous-domaines) requis pour le Service soient fournis. Le Client accepte que des fonctionnalités du Service puissent ne pas fonctionner correctement et que la délivrance d'e-mails puisse être indisponible pour des domaines non fournis.

Annexe 1: Paramètres des meilleures pratiques en matière d'antispam

Veuillez noter que le Niveau de service ne s'applique que si le Client configure les paramètres des meilleures pratiques. Quelle que soit la Formule choisie, le Client reste responsable de la configuration.

7.13 Pour la Formule Reactive Care

7.13.1 À configurer par le Client

- Activation des deux options expéditeurs approuvées et si possible, limitation au strict minimum des entrées sur la liste
- Activation de spoofed sender detection avec SPF – recommandé en cas de problème lié à spoofed spam mails - uniquement pour les e-mails entrants
- Activation de DMARC - (Domain-based Message Authentication, Reporting, and Conformance) - aide à déjouer les tentatives de phishing qui peuvent entraîner des failles de sécurité en détectant email sender spoofing - uniquement pour les messages entrants
- Activation des deux listes d'expéditeurs bloqués - action recommandée dans les deux cas : bloquer et supprimer
- Utilisation de la liste de blocage IP dynamique - action recommandée : bloquer et supprimer, car elle contient une liste de séries IP dynamiques d'où aucun e-mail ne peut provenir
- Activation du système de signature - action recommandée : bloquer et supprimer, car elle agit au niveau des caractéristiques du spam connu.
- Activation de Skeptic Heuristics - Predictive Spam detection - action recommandée : repérer l'objet et autoriser l'e-mail, car peut être configuré par les règles Outlook pour les Utilisateurs finaux. Également recommandé, car cette série de règles, bien que très précises, peut fournir potentiellement plus de faux positifs, comme il s'agit d'un système prédictif. Il est également possible de mettre l'e-mail en quarantaine si cette fonction est activée.
- Activation de newsletter filter extension si nécessaire - il s'agit d'un blocage très agressif, qui stoppera toutes les newsletters souhaitées et non souhaitées. Nous recommandons généralement de l'activer et d'accorder des exceptions au cas par cas, en fonction de l'environnement de déploiement.
- Activation de spoofed sender detection avec SPF – pour les e-mails sortants
- Activation de DMARC - (Domain-based Message Authentication, Reporting, and Conformance) - aide à déjouer les tentatives de phishing qui peuvent entraîner des failles de sécurité en détectant email sender spoofing - pour les messages sortants

7.14 Pour Reactive Care avec Formule Assist ou Full Care

7.14.1 À configurer par le Client

- Activation de spoofed sender detection avec SPF – pour les e-mails sortants
- Activation de DMARC - (Domain-based Message Authentication, Reporting, and Conformance) - aide à déjouer les tentatives de phishing qui peuvent entraîner des failles de sécurité en détectant email sender spoofing - pour les messages sortants

8. Annexe 2 : Prérequis techniques

Le Client s'assurera que son système e-mail est compatible SMTP.

Le Client effectuera et préservera les paramètres de configuration suivants pour son infrastructure ICT, afin de permettre un support adéquat du Service :

- Ajouter une clé au DNS du Client. Proximus communiquera cette clé lors de la confirmation de la commande.
- Placer les adresses IP du Service sur liste blanche pour avoir accès à l'environnement du Client, où le serveur e-mail est hébergé. Proximus communiquera ces adresses IP lors de la confirmation de la commande.
- Changer les enregistrements MX. Proximus communiquera les détails lors de la confirmation de la commande.