Bilaga 1
Allmän beskrivning av Tjänsten

BESKRIVNINGAR AV TJÄNSTER OCH/ELLER SLA SOM ANGES I BILAGA 2 OCH 3 NEDAN OCH SOM INTE BESTÄLLTS AV KUNDEN I AVSNITT B I AVTALET SKALL INTE GÄLLA FÖR KUNDEN.

1. Definitioner

Termer nämnda nedan skall ha följande innebörd i avtalet:

Med ”massutskick”	menas en grupp med mer än femtusen (5 000) e-postmeddelanden med i stort sett samma innehåll som sänds eller mottas i en enda manöver eller en serie sammanhörande manövrar.
Med ”e-post”	menas alla SMTP-meddelanden som sänds eller mottas via Tjänsten.
Med ”ej uppdelningsbara tjänstepaket”	menas ett paket med Tjänster enligt beskrivning i Avsnitt B ”Tjänst och avgifter” i avtalet samt Klausul 7 nedan och som lyder under bestämmelserna i Klausul 3.6 i avtalet.
Med ”medlem”	menas kunden och organisationer med vilka kunden skapar ett krypterat nätverk genom att använda funktionen gränskryptering.
Med ”normal arbetstid”	menas mellan kl. 08:30 och 17:30 lokal tid i Storbritannien, måndag till fredag, utom helgdagar i Storbritannien.
Med ”öppen proxy”	menas en proxyserver som konfigurerats så att den tillåter okända eller icke-auktoriserade tredje parter att komma åt, förvara eller vidarebefordra DNS, webbsidor och annan data.
Med ”öppen relay”	menas en e-post-server som konfigurerats så att den tar emot e-post från en okänd eller icke-auktoriserad tredje part och vidarebefordrar e-posten till en eller flera mottagare som inte är användare hos det e-postsystem som denna e-postserver är ansluten till. Öppen relay kan även kallas för ”skräppost relay” eller ”offentlig relay”.
Med ”skräppost”	menas oönskad kommersiell e-post.
Med ”torn”	menas en grupp av belastningsbalanserade e-postservrar.
Med ”användare”	menas en person, postlåda eller maskin som använder Tjänsten.
Med ”virus”	menas programkod som innehåller ett självkopierande element, vanligtvis förklädd som något annat och utformat för att infektera andra datasystem.

2. Inledning

2.1 Symantec är en leverantör av hanteringstjänster som är specialiserad på Internetbaserad e-post, snabbmeddelanden och webbsäkerhet.

2.2 Tjänsten underhålls tjugofyra (24) timmar per dygn, sju (7) dagar i veckan från Symantec Globala Center. Tjänsten bevakas vad det gäller tillgång till hårdvara, tjänstekapacitet och utnyttjande av nätverksresurser.

2.3. Om Symantec inte kan leverera e-post till en kunds e-postserver, kommer Symantec att förvara kundens inkommande e-post i upp till sju (7) dagar i väntan på leverans.

2.4. Tjänsten är tillgänglig för kunder som är permanent anslutna till Internet med fast IP-adress. Leverans kan inte ske till kunder vars system är anslutna till Internet via uppringningsmodem eller ISDN-linje eller vars IP-adress tilldelas dynamiskt.

2.5. Avsändarens IP-rykte bekräftas för all inkommande e-post. E-post som kommer från källa med dåligt rykte (t.ex. utsändare av skräppost) kommer att bromsas för att minimera påverkan på nätverkets kapacitet.

2.6 Kunden bör konfigurera sina e-postservrar att begränsa antalet mottagare per utgående SMTP-anslutning till mindre än 500. En mottagare är en enskild e-postadress. En e-postgrupp kan innehålla en eller flera mottagare. Om ett inkommande eller utgående e-postmeddelande innehåller mer än 500 mottagare i en SMTP-anslutning, kommer Symantec att behandla de första 500 mottagarna, samt skicka en SMTP-svarskod till den e-postserver som skickade meddelandet med en begäran om att e-postservern skickar om e-postmeddelandet till de resterande mottagarna.

3. Planerat underhåll

3.1. Med ”planerat underhåll” menas i denna Klausul 3, underhållsperioder som Symantec har meddelat kunden om sju (7) dagar i förväg och som kan komma att orsaka avbrott i Tjänsten på grund av att torn inte är tillgängliga. Planerat underhåll skall inte pågå i mer än åtta (8) timmar per kalendermånad och skall under inga omständigheter ske mellan 08:00 och 18:00 (i den tidszon där ett torn är placerat).

3.2. Där så är möjligt, kommer planerat underhåll ske utan att Tjänsten påverkas. Detta kommer i allmänhet att åstadkommas genom att det planerade underhållet utförs under perioder då trafiken förväntas vara låg och genom att det planerade underhållet utförs på en del av och inte hela nätverket på en gång. Under perioder av planerat underhåll kan trafiken omdirigeras till delar av nätverket som inte genomgår underhåll för att minimera avbrott i Tjänsten.

3.3. Om nödfallsunderhåll krävs och kan förväntas påverka Tjänsten kommer Symantec att vidta åtgärder för att informera berörda parter och kommer snarast möjligt och under alla omständigheter inom en (1) timme efter att nödfallsunderhållet påbörjats att publicera varningsmeddelanden på ClientNet.

4. ClientNet

4.1. Symantec internetbaserade hanterings- och rapporteringsverktyg kallat ClientNet utgör en integrerad del av Tjänsten. ClientNet finns tillgängligt för kunden via en skyddad inloggning med säkert lösenord som inte skall avslöjas för tredje parter. ClientNet erbjuder kunden möjlighet att granska data och statistik beträffande kundens användande av Tjänsten samt erbjuder ett antal konfigurerings- och hanteringsmöjligheter.

5. Teknisk support

5.1. Symantec kommer tjugofyra (24) timmar per dygn och sju (7) dagar i veckan att:

a) erbjuda kunden teknisk support när det gäller problem med Tjänsten
b) samarbeta med kunden för att lösa sådana problem.

6. Kundtjänst

6.1. Symantec kommer att erbjuda kundtjänst under normal arbetstid för att:

a) ta emot och behandla beställningar gällande tillhandahållande av Tjänsten
b) ta emot och behandla begäran om modifieringar av driftsmässiga aspekter av Tjänsten
c) svara på fakturarelaterade frågor.

6.2. Om inte annat anges i relevant beskrivning av Tjänsten kommer Symantec Globala Team vid mottagande av fullständigt ifylld och verkställningsbar beställning eller begäran om ändring av Tjänst att tillhandahålla Tjänsten inom tjugosju (27) timmar av normal arbetstid, förutsatt att alla faser av nödvändiga tekniska förberedelser har genomförts.

7. Ej uppdelningsbara tjänstepaket

7.1 Ej uppdelningsbara tjänstepaket (om sådant väljs i Avsnitt B ”Tjänst och Avgifter” i avtalet) omfattar följande ingående Tjänster:

Aktuellt namn på Odelbart paket med Tjänster	Tjänster som ingår i paketet (Tjänster som tidigare ingick i paketet)	Tidigare namn på oOdelbart paket med tjänster
Symantec MessageLabs Email Protect.cloud	Email AV, Email AS	MessageLabs Email Protect
Symantec MessageLabs Email Control.cloud	Email IC, Email CC	MessageLabs Email Control
Symantec MessageLabs Email Safeguard.cloud	Email AV, Email IC, Email AS, Email CC	MessageLabs Email Safeguard (or MessageLabs Email Protect & Control)
Symantec MessageLabs Web v2 Protect & Control.cloud	Web v2 Protect, Web v2 URL	MessageLabs Web Protect & Control
Not Offered	(Email AV, Email AS, Web AVASv2)	MessageLabs Email Protect & Web Protect
Not Offered	(Email AV, Email IC, Email AS, Email CC, Web AVASv2)	MessageLabs Email Protect & Control & Web Protect
Not Offered	(Email AV, Email AS, Web AVASv2, Web URLv2)	MessageLabs Email Protect & Web Protect & Control
Symantec MessageLabs Email & Web Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Web v2 Protect, Web v2 URL (Email AV, Email IC, Email AS, Email CC, Web AVASv2, Web URLv2)	MessageLabs Email & Web Safeguard (or MessageLabs Email & Web Protect & Control)
Symantec MessageLabs 2 Email Services Bundle	2 Email Services from Email AV, Email IC, Email AS, or Email CC	MessageLabs 2 Email Services Bundle
Symantec MessageLabs 3 Email Services Bundle	3 Email Services from Email AV, Email IC, Email AS, or Email CC	MessageLabs 3 Email Services Bundle
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving (P))	MessageLabs Email Protect & Control & Archiving (P)
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving Lite (P))	MessageLabs Email Protect & Control & Archiving Lite (P)
Not Offered	(Email AV, Email IC, Email AS, Email CC, Email Archiving Premium(P))	MessageLabs Email Protect & Control & Archiving Premium(P)
Symantec MessageLabs Security Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Web AVASv2, Web URLv2, IMSS	MessageLabs Security Safeguard
Symantec MessageLabs Complete Email Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec Enterprise Vault Mailbox Continuity.cloud **(För kunder som köpt Tjänster före 1 oktober 2011:** Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud)	MessageLabs Complete Email Safeguard
Symantec MessageLabs Complete Email & Web Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec Enterprise Vault Mailbox Continuity.cloud, Web v2 Protect, Web v2 URL **(För kunder som köpt Tjänster före 1 oktober 2011:** Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud, Web v2 Protect, Web v2 URL)	MessageLabs Complete Email & Web Safeguard
Symantec MessageLabs Ultimate Safeguard.cloud	Email AV, Email IC, Email AS, Email CC, Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec Enterprise Vault Mailbox Continuity.cloud, Web v2 Protect, Web v2 URL, IMSS **(För kunder som köpt Tjänster före 1 oktober 2011:** Email AV, Email IC, Email AS, Email CC, Symantec Email Continuity Archive.cloud, Symantec Email Continuity.cloud, Web v2 Protect, Web v2 URL, IMSS)	MessageLabs Ultimate Safeguard
Symantec Enterprise Vault.cloud	Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud	MessageLabs Email Archiving L or Email Archiving.cloud (L)
Symantec Enterprise Vault Enhanced.cloud	Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud, Symantec EnterpriseVault Mailbox Continuity.cloud	Messagelabs Email Enhanced Archive L or Email Enhanced Archiving.cloud (L)

8. Tidigare namn på Tjänster

8.1 I det här dokumentet används inte de ursprungliga namnen på Tjänsterna som gällde före den 1 juni 2011, utan vi introducerar nu en ny nomenklatur. I tabellen nedan visas vilka nya namn som ersätter de gamla så att Kunderna kan fastställa vilka avsnitt i dokumentet som gäller Tjänster som köpts under den tidigare nomenklaturen.

Tidigare namn på Tjänst	Aktuellt namn på Tjänst
MessageLabs Email Anti-Virus	Symantec MessageLabs Email Anti-Virus.cloud
MessageLabs Email Image Control	Symantec MessageLabs Email Image Control.cloud
MessageLabs Email Anti-Spam	Symantec MessageLabs Email Anti-Spam.cloud

MessageLabs Email Content Control	Symantec MessageLabs Email Content Control.cloud
MessageLabs Boundary Encryption	Symantec MessageLabs Email Boundary Encryption.cloud
MessageLabs Web Anti-Spyware and Anti-Virus Service v2	Symantec MessageLabs Web v2 Protect.cloud
MessageLabs Web URL Service v2	Symantec MessageLabs Web v2 URL.cloud
MessageLabs Email Archiving P	Symantec MessageLabs Email Archiving.cloud (P)
MessageLabs Enterprise Instant Messenger (EIM)	Symantec MessageLabs EIM.cloud
MessageLabs EIM Connect	Symantec MessageLabs EIM Connect.cloud
MessageLabs EIM Communicate	Symantec MessageLabs EIM Communicate.cloud
MessageLabs Policy Based Encryption	Symantec MessageLabs Policy Based Encryption.cloud
MessageLabs Email Continuity (EC), or Symantec MessageLabs Email Continuity.cloud (D)	Symantec Email Continuity.cloud (EC)
Schemus Tool	Schemus Tool
MessageLabs Instant Messaging Security Service (IMSS)	Symantec MessageLabs Instant Messaging Security.cloud
MessageLabs Email Archiving D, or Symantec MessageLabs Email Archiving.cloud (D)	Symantec Email Continuity Archive.cloud
MessageLabs Email Archiving Lite D, or Symantec MessageLabs Email Archiving.cloud Lite (D)	Symantec Email Continuity Archive Lite.cloud
MessageLabs Volume Mail	Symantec MessageLabs Volume Mail
Hosted Endpoint Protection	Symantec Endpoint Protection.cloud
MessageLabs Personal Archive L or Symantec MessageLabs Email Personal Archiving.cloud (L)	Symantec Enterprise Vault Personal.cloud
MessageLabs Email Discovery Archive L, or Symantec MessageLabs Email Discovery Archiving.cloud (L)	Symantec Enterprise Vault Discovery.cloud
MessageLabs Personal Archive L for BlackBerry®, or Symantec MessageLabs Personal Archive for BlackBerry®.cloud (L)	Symantec Enterprise Vault.cloud Blackberry Option
MessageLabs Email Archiving Premiium L , or Symantec MessageLabs Email Premium Archiving.cloud (L)	AdvisorMail on Symantec.cloud™
MessageLabs Email Archiving IM Premium L, or Symantec MessageLabs Email Premium Archiving.cloud for IM (L)	AdvisorMail IM Option on Symantec.cloud™
MessageLabs Email Archiving Bloomberg Message Premium L, or Symantec MessageLabs Premium Archiving.cloud for Bloomberg	AdvisorMail Bloomberg Option on Symantec.cloud™
MessageLabs Email Archive Import Service L, or Symantec MessageLabs Email Archiving.cloud (L) Import	Symantec Enterprise Vault.cloud Data Import Option
MessageLabs Email Continuity L, or Symantec MessageLabs Email Continuity.cloud (L)	Symantec Enterprise Vault Mailbox Continuity.cloud
MessageLabs User Roaming Agent Service (“Smart Connect”)	Symantec MessageLabs Web v2 Smart Connect.cloud

Bilaga 2
Beskrivningar av Tjänsterna

Appendix 1 – Symantec MessageLabs Email Anti-Virus.cloud (Email AV)

1. Översikt

1.1. Symantec MessageLabs Email Anti-Virus.cloud (”Email AV”, ”e-post AV”) är Symantec Tjänst för virusskanning på Internetbaserad för e-post. Kundens inkommande och utgående e-post, inklusive alla bilagor, makron och programfiler leds genom e-post AV med hjälp av DNS- och MX-registerinställningar.

1.2. E-post och bilagor skannas av flera branschledande anti-virusprodukter inklusive Symantec egen heuristiska skanner, Skeptic™.

2. Varningsmeddelanden

2.1. Om en kunds inkommande e-post eller bilagor visar sig innehålla virus kommer en automatisk varning, om så valts av kunden, att sändas till avsändaren och mottagaren via ett meddelande. När det gäller kundens utgående e-post kan Tjänsten enbart meddela avsändaren och inte mottagaren. Användarmeddelanden kan i båda fallen även sändas till en e-postadministratör. Det infekterade e-postmeddelandet vidarebefordras till en säker server i väntan på att förstöras efter sju (7) dagar förutsatt att det inte sänts som massutskicksvirus då det kommer att raderas omedelbart.

2.2. Vid stora utbrott av ett nytt virus kommer ett varningsmeddelande att publiceras på ClientNet.

3. Konfigurering

3.1. ClientNet kan användas för att anpassa banderolltexter, släppa virusinfekterade e-postmeddelanden och ställa in maximal storlek för e-postmeddelande.

4. Frisläppa virusinfekterat e-postmeddelande

4.1. När ett virusinfekterat e-postmeddelande visas klart för att släppas, kan detta ske från säker server med hjälp av ClientNet. E-postmeddelandet kommer att släppas till antingen den första adressen i den ursprungliga mottagarlistan eller till en specificerad adress som tidigare meddelats Symantec och som av Symantec registrerats på ClientNet (OBS Dessa adresser kan vara e-postgrupper eller alias och i sådana fall kommer e-postmeddelandet att sändas till alla adressater i gruppen eller aliaset). Som ett alternativ kan Symantec släppa det virusinfekterade e-postmeddelandet till en alternativ adress, efter tillstånd från Symantec. Symantec kommer enbart att handla på begäran från auktoriserade kunder när det gäller att vidarebefordra virusinfekterade e-postmeddelanden. Symantec kommer inte att återsända virusinfekterade e-postmeddelanden till avsändaren. Symantec kommer inte att vidarebefordra virusinfekterade e-postmeddelanden till tredje parter. Vissa virusinfekterade e-postmeddelanden som skickas till kunden kan inte släppas på grund av att de innehåller virus som är speciellt smittsamt eller skadligt. Dessa visas på ClientNet som ej möjliga att släppa.

5. Villkor och bestämmelser för e-post AV

5.1. Vid begäran om att släppa ett virusinfekterat e-postmeddelande kommer Symantec att släppa det inom åtta (8) timmars normal arbetstid efter mottagande av auktoriserad begäran.

Appendix 2 – Symantec MessageLabs Email Image Control.cloud (Email IC)

1. Översikt

1.1. Symantec MessageLabs Email Image Control.cloud (”Email IC”, ”e-post IC”) är Symantec Bildkontroll för Internetbaserad e-post och är utformad för att detektera pornografiska bilder i bildfiler.

2. Beskrivning av Tjänsten

2.1. Kundens inkommande och utgående e-post kan skannas med hjälp av bildkompositionsanalys (Image Composition Analysis, ICA) för att upptäcka pornografiska bilder i bildfiler som bifogas e-post.

2.2. Om en kunds inkommande eller utgående e-post misstänks innehålla en pornografisk bild kommer en av flera åtgärder att vidtas beroende på vilka konfigureringsalternativ som valts av kunden.

3. Konfigurering

3.1. Vid mottagande av en fullständigt ifylld och accepterad beställning, kommer Symantec att tillhandahålla e-post IC för kunden. E-post IC aktiveras initialt på alla kundens domäner. Kunden ansvarar för att ställa in konfigureringsalternativ för e-post IC för varje enskild domän enligt behov. Kunden konfigurerar e-post IC via ClientNet.

3.2. Alternativ finns för att specificera nivån av detekteringskänslighet som ICA-filtret skall använda. Känsligheten kan ställas till Hög, Medium eller Låg. Inställningarna är mycket subjektiva men som en riktlinje kan anges att fler bilder kommer att misstänkas vara pornografiska vid Hög känslighet och färre kommer att misstänkas vara pornografiska vid Låg känslighet.

3.3. Alternativ finns för att ange vilka åtgärder som skall vidtas vid detektering av en misstänkt pornografisk bild. Dessa alternativ kan ställas in oberoende för inkommande och utgående e-post och bör ställas in i enlighet med kundens befintliga riktlinjer för accepterad datoranvändning (eller motsvarande). Alternativen är:

3.3.1. Registrera misstänkta e-postmeddelanden (skapar statistik som kan ses via ClientNet).

3.3.2. Märka misstänkta e-postmeddelanden i rubriken (enbart för inkommande e-post).

3.3.3. Kopiera misstänkta e-postmeddelanden till en förutbestämd e-postadress.

3.3.4. Omdirigera misstänkta e-postmeddelanden till en förutbestämd e-postadress.

3.3.5. Radera misstänkta e-postmeddelanden.

3.3.6. Märka misstänkta e-postmeddelanden i ämnesrubriken.

3.4. Om kunden har identifierat tillförlitliga e-postavsändare eller mottagare för administration av e-post IC, kommer dessa avsändares och mottagares e-post inte att skannas av e-post IC.

4. Rapportering

4.1. Om de valda alternativen i Klausul 3.3 i detta Appendix är att omdirigera eller radera e-post som innehåller en misstänkt pornografisk bild, skall en automatisk varning sändas till avsändaren. Om e-postmeddelandet är inkommande till kunden kan en automatisk varning också skickas till mottagaren. Sådana automatiska varningar kan aktiveras och avaktiveras av kunden via ClientNet.

4.2. Rapportering om effektiviteten hos e-post IC sker via ClientNet där statistik finns beträffande antalet inkommande och utgående e-postmeddelanden som misstänks innehålla pornografiska bilder. ClientNet kan konfigureras så att det skapar rapporter som via e-post sänds till kunden varje vecka eller varje månad.

5. Villkor och bestämmelser för e-post IC

5.1. INGEN PROGRAMVARA FÖR DETEKTERING AV PORNOGRAFISKA BILDER KAN GARANTERA 100 % DETEKTERING OCH DÄRFÖR KAN SYMANTEC INTE PÅTA SIG NÅGOT ANSVAR FÖR SKADA ELLER FÖRLUST SOM DIREKT ELLER INDIREKT UPPSTÅR PÅ GRUND AV ATT TJÄNSTEN MISSLYCKATS MED ATT DETEKTERA EN PORNOGRAFISK BILD ELLER FELAKTIGT IDENTIFIERAT EN BILD SOM MISSTÄNKT PORNOGRAFISK VILKEN SENARE VISAR SIG INTE VARA PORNOGRAFISK.

5.2. Det kan hända att det inte är möjligt att skanna bilagor med innehåll som direkt kontrolleras av avsändaren (t.ex. lösenordsskyddade och/eller krypterade bilagor).

5.3. E-post IC kan skanna efter pornografiska bilder som finns i vissa versioner av Word, Excel, PowerPoint och pdf dokument men inte i andra dokument.

5.4. Symantec betonar att konfigureringen av e-post IC helt kontrolleras av kunden. E-post IC är ämnat att användas enbart för att möjliggöra för kunden att bevaka existerande, verkliga och tillämpade riktlinjer för godtagbar datoranvändning (eller motsvarande). I vissa länder kan det krävas att individuell personal ger sitt samtycke. Symantec rekommenderar att kunden alltid kontrollerar lokal lagstiftning före användande av e-post IC. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av e-post IC. Kunden bekräftar att man är medveten om att definitionen för vad som utgör och inte utgör en pornografisk bild är subjektiv. Kunden bör beakta detta vid konfigureringen av Tjänsten.

5.5. Om kunden släpper eller begär att ett virusinfekterat e-postmeddelande ska släppas, kommer detta inte att skannas av e-post IC innan det släpps.

Appendix 3 – Symantec MessageLabs Email Anti-Spam.cloud (Email AS)

1. Översikt

1.1. Symantec MessageLabs Email Anti-Spam.cloud (Email Anti-Spam, ”e-post AS”) är Symantec Skräppostskydd för Internetbaserad e-post och är utformad för att skydda kunden från oönskad e-post.

2. Beskrivning av Tjänsten

2.1. Kundens inkommande e-post kan skannas med hjälp av ett antal olika detekteringsmetoder för att avgöra om det rör sig om skräppost. Om ett inkommande e-postmeddelande misstänks vara skräppost kommer en av flera åtgärder att vidtas beroende på vilka konfigureringsalternativ som valts av Kunden i Klausul 3.2 nedan.

2.2. En privat lista över godkända avsändare kan sammanställas av kunden liksom av individuella användare om kunden har aktiverat inställning på användarnivå. Om denna detekteringsmetod väljs och ett inkommande e-postmeddelande mottas från en avsändare vars domän har godkänts på listan, kommer det automatiskt att ledas förbi alla valda detekteringsmetoder för skräppost.

2.3. En privat lista över blockerade avsändare kan sammanställas av kunden liksom av individuella användare om kunden har aktiverat inställning på användarnivå. Om denna detekteringsmetod väljs och ett inkommande e-postmeddelande mottas från en avsändare vars domän har blockerats på listan kommer en åtgärd att vidtas enligt konfigureringsalternativen i Klausul 3.2 nedan.

2.4. Ett antal offentliga listor över blockerade avsändare kan användas. Om någon av dessa detekteringsmetoder väljs och ett inkommande e-postmeddelande mottas från en avsändare vars domän finns med på en av de offentliga listorna över blockerade avsändare kommer en åtgärd att vidtas enligt konfigureringsalternativen i Klausul 3.2 nedan.

2.5. Om e-postmeddelandet inte har raderats på grund av att det blockerats enligt ovan och signatursystemet valts samt den åtgärd som skulle vidtas som ett resultat av detektering av e-postmeddelandet som skräppost är allvarligare än att det redan valts som ett resultat av att det detekterats att avsändaren finns med på listan över blockerade avsändare, kommer Kundens inkommande e-postmeddelande att skannas med hjälp av signatursystemet. Om ett e-postmeddelande med hjälp av denna metod detekteras som skräppost kommer åtgärd att vidtas enligt definition i konfigureringsalternativen i Klausul 3.2 nedan. Denna åtgärd kommer att ersätta alla mindre allvarliga åtgärder som tidigare utsetts genom någon av metoderna med listor över blockerade avsändare.

2.6. Om e-postmeddelandet inte har raderats som ett resultat av föregående processer och heuristisk detektering valts och den åtgärd som skulle vidtas som ett resultat av att e-postmeddelandet detekterats som skräppost enligt kundens konfigurering är allvarligare än den som redan valts som ett resultat av detektering genom de föregående processerna, kommer kundens inkommande e-postmeddelanden att skannas med hjälp av heuristisk skanning. Om ett e-postmeddelande med hjälp av heuristisk metod detekteras som skräppost kommer åtgärd att vidtas enligt definition i konfigureringsalternativen i Klausul 3.2 nedan. Denna åtgärd kommer att ersätta alla mindre allvarliga åtgärder som tidigare utsetts genom någon av de föregående metoderna.

2.7. Listor med blockerade avsändare/godkända avsändare som tillhandahålls av Symantec är enbart ämnade som exempel.

3. Konfigurering

3.1. Vid mottagande av en fullständigt ifylld och accepterad beställning, kommer Symantec att aktivera e-post AS för kunden. E-post AS aktiveras initialt på alla kundens domäner. KUNDEN BEKRÄFTAR ATT MAN ÄR MEDVETEN OM ATT E-POST AS FRÅN BÖRJAN KOMMER ATT FÖRSES MED SYMANTEC STANDARDINSTÄLLNINGAR OCH ATT DET HELT ÅLIGGER KUNDENS ANSVAR ATT KONFIGURERA E-POST AS VIA CLIENTNET SÅ ATT TJÄNSTEN MOTSVARAR DE EGNA BEHOVEN. Standardinställningarna för e-post AS omfattar följande åtgärder:

3.1.1. Blockering och radering av e-postmeddelandet; eller
3.1.2. Placering av e-postmeddelandet i karantän; samt
3.1.3. Användande av lista över godkända avsändares IP-adresser, domäner och e-postadresser; samt
3.1.4. Användande av automatisk skräppostdetektering (Skeptic).

3.2. Det finns alternativ för specificering av vilka åtgärder som skall vidtas om ett e-postmeddelande misstänks vara skräppost. Dessa alternativ som anges nedan kan väljas för var och en av de tillgängliga detekteringsmetoderna:

3.2.1. Märka misstänkta e-postmeddelanden i rubriken.

3.2.2. Märka misstänkta e-postmeddelanden i ämnesrubriken.

3.2.3. Omdirigera misstänkta e-postmeddelanden till en förutbestämd e-postadress (som måste finnas på en domän som skannas av Tjänsten).

3.2.4. Radera misstänkta e-postmeddelanden.

3.2.5. Placera skräppost i karantän.

4. Beskrivning av karantän för skräppost

4.1. Om kunden konfigurerar karantän för skräppost för en domän, kommer varje användares konto för karantän för skräppost att skapas automatiskt första gången misstänkt skräppost identifieras av e-post AS och användaren kommer automatiskt att meddelas per e-post.

4.2. användare kan komma åt karantän för skräppost via gränssnittet för skräpposthantering.

4.3. Misstänkt skräppost kan förvaras i maximalt fjorton (14) dagar och kommer därefter automatiskt att raderas. Kunden kan köpa förlängd förvaring i mer än fjorton (14) dagar genom betalning av en extraavgift som räknas ut på basen av användare per dag (”Symantec MessageLabs Extended Spam Quarantine”).

4.4. Om karantän för skräppost inte kan ta emot e-postmeddelandet kommer den misstänkta skräpposten att märkas och sändas till mottagaren.

5. Konfigurering av karantän för skräppost

5.1. Kunden konfigurerar karantän för skräppost via ClientNet

5.2. Generella användarmeddelanden ställs in enligt 5.2.1 nedan. användaren kan när som helst välja ett av följande meddelandealternativ:

5.2.1. Dagliga meddelanden;

5.2.2. Meddelanden med vissa mellanrum;

5.2.3. Inga meddelanden.

5.3. Följande alternativ för att släppa skräppost finns via skräpposthanteraren: (i) Radera e-post; (ii) Släppa e-postmeddelande till ursprunglig mottagaradress; (iii) Granska text i e-postmeddelande.

5.4. För att kunna använda karantän för skräppost måste kunden ha registrerat en godkännandelista hos Symantec. Godkännandelistan innehåller alla giltiga e-postadresser som används av kunden. Alla mottagaradresser som inte finns med på godkännandelistan bedöms som ogiltiga och e-post kommer inte att levereras till sådana adresser.

5.5. Kunderna kan kontrollera andra aspekter av skräpposthanteraren via ClientNet: (a) automatisk eller manuell meddelandepolicy; (b) skapande av sammanfattningsmeddelanden; (c) standard språkinställningar; (d) inställning på användarnivå; (e) förinställda alias e-postadresser; samt (f) specialiserade användare (t.ex. Karantänadministratörer).

5.6. Kunden kan skapa grupper med e-postadresser för karantän för skräppost för att kunna länka ett antal individuella e-postadresser till en ”ägar e-postadress” för e-post alias och delegerad åtkomst. Det maximala antalet e-postadresser som kan länkas till en enda e-postadress är femtio (50). Symantec förbehåller sig rätten att ta bort kunders kontogrupper eller aliaslänkar om detta maximala antal överskrids.

6. Rapportering

6.1. Rapportering beträffande effektiviteten hos e-post AS erbjuds via ClientNet. ClientNet kan konfigureras så att det skapar rapporter som via e-post sänds till kunden varje vecka eller varje månad.

7. Villkor och bestämmelser för e-post AS

7.1. INGEN PROGRAMVARA FÖR DETEKTERING AV SKRÄPPOST KAN GARANTERA 100 % DETEKTERING OCH DÄRFÖR KAN SYMANTEC INTE PÅTA SIG NÅGOT ANSVAR

FÖR SKADA ELLER FÖRLUST SOM DIREKT ELLER INDIREKT UPPSTÅR PÅ GRUND AV ATT TJÄNSTEN MISSLYCKATS MED ATT DETEKTERA SKRÄPPOST ELLER FELAKTIGT IDENTIFIERAT ETT E-POSTMEDDELANDE SOM MISSTÄNKT SKRÄPPOST VILKET SENARE VISAR SIG INTE VARA SKRÄPPOST.

7.2. Symantec betonar att konfigureringen av e-post AS helt kontrolleras av kunden. Symantec rekommenderar att kunden skaffar sig riktlinjer för godtagbar datoranvändning (eller motsvarande). I vissa länder kan det krävas att individuell personal ger sitt samtycke. Symantec rekommenderar att kunden alltid kontrollerar lokal lagstiftning före användande av e-post AS. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av e-post AS.

Appendix 4 – Symantec MessageLabs Email Content Control.cloud (Email CC)

1. Översikt

1.1. Symantec MessageLabs Email Content Control.cloud (Email Content Control, ”e-post CC”) är Symantec innehållskontroll som utformats för att möjliggöra för kunden att konfigurera sina egna regelbaserade filtreringsstrategier i samband med e-post i enlighet med policy för accepterad datoranvändning (eller motsvarande).

2. Beskrivning av Tjänsten

2.1. e-post CC ger kunden möjlighet att bygga upp en samling med regler enligt vilka inkommande och utgående e-post filtreras i enlighet med detta Appendix 4. En regel är en instruktion som skapas av kunden och som används för att identifiera ett visst format av meddelande/bilaga eller innehåll som tillskrivits en viss åtgärd i samband med e-postmeddelandet.

3. Konfigurering

3.1. Vid mottagande av en fullständigt ifylld och accepterad beställning, kommer Symantec att aktivera e-post CC för var och en av kundens tillämpliga domäner. Kunden ansvarar för att implementera konfigureringsalternativ för e-post CC för varje enskild domän enligt behov. Kunden konfigurerar e-post CC via ClientNet.

3.2. Kunden kan konfigurera regler för varje enskild domän, grupp eller individ.

3.3. Regeländringar som görs av kunden kommer att träda i kraft inom 24 timmar.

3.4. Alternativ finns för att ange vilken åtgärd som skall vidtas vid detektering av ett misstänkt e-postmeddelande. Dessa alternativ kan ställas in oberoende för inkommande och utgående e-post och bör ställas in i enlighet med kundens befintliga riktlinjer för accepterad datoranvändning (eller motsvarande). Alternativen är:

3.4.1. Blockera och radera misstänkta e-postmeddelanden.

3.4.2. Märka misstänkta (inkommande) e-postmeddelanden och omdirigera dem till en specificerad administratör.

3.4.3. Märka misstänkta (inkommande) e-postmeddelanden och skicka en kopia av dem till en specificerad administratör.

3.4.4. Märka rubriken på misstänkta (inkommande) e-postmeddelanden.

3.4.5. Komprimera e-postbilagor.

3.4.6. Registrera bara i ClientNets statistik.

3.4.7. Märka i ämnesrubriken.

4. Rapportering

4.1. Genom ClientNet kan en kund granska resultatet av sina regler i form av sammandrag för varje dag, vecka, månad och år sorterade efter både regel och användare.

4.2. Rapporter som innehåller loggning av tjänstens aktiviteter kan skapas varje vecka eller varje månad och på begäran skickas till kunden via e-post.

4.3. Genom ClientNet kan kunden aktivera och avaktivera meddelanden som konfigurerats av kunden för varje enskild regel.

5. Support för Innehållskontroll

5.1. Support inkluderar Genomgång av gränssnittet för e-post CC inklusive en beskrivning av Tjänsten samt Frågor och Svar.

6. Jokertecken

6.1. e-post CC fungerar på basen av exakt matchning av kundens konfigurerade regler. Jokertecken ger dock kunden möjlighet att som ett specifikt undantag från detta konfigurera e-post CC via ClientNet så att vissa alfanumeriska formuleringar som följer ett specifikt mönster identifieras (t.ex. personnummer, statliga försäkringsnummer och kreditkortsinformation).

7. Villkor och bestämmelser för innehållskontroll

7.1. Symantec tillhandahåller listor och exempel på regler med ord som kan ses som stötande.

7.2. Kunden accepterar och samtycker till att Symantec får sammanställa och publicera listor med standardord hämtade från kundens egna ordlistor.

7.3. Kunden är medveten om att om e-post CC används tillsammans med karantänåtgärder i e-post skräppostskydd kan det resultera i att misstänkt skräppost sätts i karantän innan den filtrerats av e-post CC.

7.4. E-post CC kan skanna efter innehåll i vissa versioner av Word, Excel, PowerPoint och pdf dokument men inte i andra dokument.

7.5. Symantec betonar att kunden helt kontrollerar konfigureringen av e-post CC och att denna konfigurering kommer att avgöra funktionen hos e-post CC. Därför kan Symantec inte påta sig något ansvar för skada eller förlust som direkt eller indirekt uppstår på grund av att Tjänsten misslyckas med att detektera misstänkt innehåll eller felaktigt identifierar ett e-postmeddelandes innehåll som misstänkt vilket senare visar sig inte vara misstänkt.

7.6. Symantec rekommenderar att kunden skaffar sig riktlinjer för godtagbar datoranvändning (eller motsvarande) som reglerar sina användares nyttjande av e-post, samt att eventuella exempel på mallar som tillhandahålls av Symantec stöder denna policy. I vissa länder kan det krävas att individuell personal ger sitt samtycke. Symantec rekommenderar att kunden alltid kontrollerar lokal lagstiftning före användande av e-post CC. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av e-post CC.

Appendix 5 – Symantec Email Boundary Encryption.cloud

1. Översikt

1.1. Symantec MessageLabs Email Boundary Encryption.cloud (Boundary Encryption, ”BE”) tillhandahåller krypterade kommunikationskanaler som ger kunden möjlighet att skapa ett säkert privat e-postnätverk (SPEN) med utvalda partnerorganisationer (”SPEN-partner”). Denna konfigurering kallas för ”Tvingande” kryptering.

1.2. Dessutom kan kunden även ta emot krypterade e-postmeddelanden som sänts opportunistiskt från organisationer som har e-postservrar med TLS för vilka ingen tvingande kryptering till kunden föreligger om dessa organisationer har e-postservrar med TLS. Denna konfigurering kallas för ”Opportunistisk” kryptering.

1.3. Om kunden abonnerat på BE men inte uttryckligen har identifierat några SPEN-partner kan kunden ta emot opportunistisk inkommande e-post sänd via TLS och kan sända opportunistiskt krypterade e-postmeddelanden till organisationer som inte är SPEN-partner.

1.4. Kunden kan även konfigurera sina e-postservrar för BE:s ”Säker anslutningsmodell” vilket innebär att:

1.4.1 E-postutbyte mellan Symantec och kundens e-postservrar med säker anslutning kommer att skyddas av TLS-kryptering. Vidarebefordran sker i krypterat eller okrypterat format beroende på (i) TLS-regler specificerade av kunden och (ii) destinationsserverns kapacitet när det gäller att ta emot e-postmeddelanden via opportunistisk TLS.

1.4.2 **KUNDEN BEKRÄFTAR ATT MAN ÄR MEDVETEN OM OCH ACCEPTERAR ATT I FALL DÄR SÄKER ANSLUTNINGSMODELL INTE HAR TILLÄMPATS FÖR EN VISS E-POSTSERVER, KOMMER KUNDENS INKOMMANDE OCH UTGÅENDE E-POSTMEDDELANDEN, SOM KOMMER FRÅN ELLER MOTTAS AV DENNA E-POSTSERVER, INTE ATT SKYDDAS AV TLS-KRYPTERING. DÄRMED BEKRÄFTAR KUNDEN ATT MAN ÄR MEDVETEN OM OCH ACCEPTERAR ATT MAN INTE BÖR SÄNDA ELLER MOTTA KÄNSLIGA DATA VIA EN SÅDAN E-POSTSERVER SAMT ATT MAN GÖR DET HELT PÅ EGEN RISK**.

1.5 Om kunden använder BE tillsammans med PBE, rekommenderar Symantec att kunden som bästa metod tillämpar BE:s säker anslutningsmodell för alla sina e-postservrar.

1.6 **BE FUNGERAR ENBART DÅ DET ANVÄNDS TILLSAMMANS MED EN AV FÖLJANDE TJÄNSTER OCH KAN INTE FUNGERA SOM EN ENSKILD TJÄNST: E-POST AV, E-POST AS, E-POST IC OCH/ELLER E-POST CC.**

2. Leverans och fakturering

2.1. Symantec ska börja debitera för BE från det datum då Symantec bekräftar att kundens nätverk har teknisk möjlighet att stödja BE (”datum för tekniskt godkännande”).

2.2 Punkt 5.2 i Bilaga 1 ska inte gälla BE. Symantec har som mål att leverera BE-order och begäran om BE-förändringar inom fyra veckor från datumet för tekniskt godkännande, under förutsättning att all nödvändig informationsinhämtning, så kallad due diligence, har utförts av kunden.

2.3 Om Symantec skulle behöva använda ytterligare tekniska resurser för att kunna tillhandahålla BE på grund av att kunden underlåtit att utföra nödvändiga tekniska förberedelser förbehåller sig Symantec rätten att för detta arbete ta ut en extraavgift på £1500/€1500 (beroende på vilken valuta kunden faktureras i) per person per dag.

3. Konfigurering

3.1. Kunden kommer att definiera med vilka SPEN-partner för varje domän man vill ha skyddad kommunikation. SPEN-partner kan vara BE-kunder eller inte, däremot kommer Symantec inte att stöda SPEN-partner direkt. Organisationer som inte är SPEN-partner kan få e-postmeddelanden via opportunistisk utgående TLS enligt beskrivning i Klausul 1 ovan om deras e-postservrar stöder mottagande av krypterad e-post.

3.2. BE baseras på standard ”SMTP via TLS” (Simple Mail Transfer Protocol over Transport Layer Security) (”STARTTLS”).

3.3. Både kundens och SPEN-partnerns e-postserver måste stöda STARTTLS för att BE skall kunna användas.

3.4. BE stöds av valda torn genom vilka all STARTTLS e-post kommer att ledas. Kunden väljer vilka av sina domäner som skall använda BE.

3.5. När BE används tillsammans med signatursystemsfunktionen hos e-post AS, rekommenderar Symantec att kunden inkluderar alla sina SPEN-partners domäner i sin lista över godkända avsändare för e-post AS. Om kunden inte följer denna rekommendation, bekräftar kunden att man är medveten om och accepterar att e-post under vissa omständigheter, i sammanhang där det lokala signatursystemet inte är tillgängligt, kan komma att omdirigeras till ett fristående signatursystem via ett offentligt nätverk.

4. Certifikat och autentisering

4.1. Om kunden initierar en STARTTLS-anslutning måste den accepterande e-postservern uppvisa sitt certifikat för autentisering. Om den accepterande e-postservern önskar autentisera Tjänsten kommer Symantec att uppvisa sitt kundcertifikat för autentisering. Om den accepterande e-postservern inte kan autentisera e-postmeddelandet kommer det att återsändas till kunden.

4.2. Om en extern e-postserver initierar en STARTTLS-anslutning kommer Tjänsten att uppvisa sitt servercertifikat för autentisering men kommer inte att insistera på att den externa e-postservern uppvisar sitt kundcertifikat för autentisering.

4.3. All verifiering av certifikat baseras på den certifikatutfärdare som undertecknat certifikatet. För varje certifikat som överlämnas av en fristående e-postserver som en del av en STARTTLS-anslutning kommer Tjänsten att verifiera att en erkänd certifikatutfärdare har undertecknat certifikatet. Om det inte går att verifiera att ett certifikat kommer från en erkänd certifikatutfärdare kommer anslutningen av avbrytas och e-postmeddelandet kommer att återsändas till avsändaren.

5. Villkor och bestämmelser för kryptering

5.1. Symantec kan inte påta sig ansvar för om kunden eller en tredje part (inklusive utan att inskränkas till SPEN-partner) underlåter att uppfylla sina förpliktelser gällande registrering av certifikat eller lämnande av korrekt information i rätt tid.

5.2. BE är ämnat att användas enbart för att möjliggöra för kunden att bevaka existerande, verkliga och tillämpade riktlinjer för godtagbar datoranvändning (eller motsvarande). Användandet av krypteringstjänster kan i vissa länder påverkas av lagstiftning. Kunden rekommenderas att alltid kontrollera relevant lagstiftning före användande av BE. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av BE.

Appendix 6 – Symantec MessageLabs Web v2 Protect.cloud

1. Översikt

1.1. När relevanta konfigureringsändringar har gjorts kommer begäran om webbsidor och bilagor att elektroniskt ledas via Symantec Skydd mot spionprogram och virus (”Web v2 Protect”) och undersökas digitalt för att upptäcka virus.

2. Beskrivning av Tjänsten

2.1. Kundens externa begäran om HTTP och FTP-över-HTTP inklusive alla bilagor, makron och programfiler leds genom Web v2 Protect.

3. Konfigurering

3.1. De konfigureringsinställningar som krävs för att dirigera denna externa trafik via Web v2 Protect utförs och upprätthålls av kunden och är beroende av kundens tekniska infrastruktur. Kunden bör se till att intern HTTP/FTP-över-HTTP-trafik (t.ex. till företagets intranät) inte leds via Web v2 Protect. Om kunden har Internettjänster som kräver en direkt anslutning i stället för via proxy ansvarar kunden för att göra nödvändiga ändringar i sin egen infrastruktur för att möjliggöra detta.

3.2. Åtkomst till Web v2 Protect begränsas med hjälp av skannings-IP, dvs. IP-adress(er) från vilka kundens webbtrafik kommer. Skannings-IP används även för att identifiera kunden och dynamiskt välja kundspecifika inställningar.

3.3. Web v2 Protect kommer att skanna lämpliga element i en webbsida och dess bilagor som kan innehålla virus, skadlig kod, spionprogram och adware. Vissa webbsidor, visst innehåll och vissa bilagor (t.ex. om de är lösenordsskyddade) kan vara omöjliga att skanna. Bilagor som specifikt identifieras som omöjliga att skanna kommer inte att blockeras. Sk streamad och krypterad trafik (dvs. streamad media och/eller HTTPS/SSL) kan inte skannas och kommer att ledas genom Web v2 Protect utan att skannas.

3.4. Fjärranvändarsupport är ett frivilligt alternativ som utökar Web v2 Protect till användare som inte befinner sig inom företagets nätverk (t.ex. användare som arbetar hemifrån). Kunden måste installera en PAC-fil på användarens dator så att användaren förs till Symantec webbportal när han startar sin webbläsare. För att nå portalen måste användaren skriva in ett lösenord och användarnamn. En mall för PAC-fil kan laddas ner från ClientNet och modifieras av kunden.

4. Varningar

4.1. Om en kunds webbsida eller bilagor upptäcks innehålla något som identifieras som virus, spionprogram eller Adware kommer åtkomst till den berörda webbsidan eller bilagan att nekas och Internetanvändaren kommer se en automatisk varningssida. I sällsynta fall, där ett eller flera element i innehållet i en begäran blockerats, kan det hända att det inte går att visa varningssidan och varningssidan kan komma att ersätta innehållet i den begärda sidan, men åtkomst till den infekterade sidan eller bilagan kommer fortfarande att nekas.

4.2. Det finns en del i den automatiska varningssidan som kunden kan anpassa via ClientNet.

5. Rapportering

5.1 Rapportering om effektiviteten hos Web v2 Protect erbjuds via ClientNet.

5.2 För att möjliggöra rapportering för varje enskild användare eller grupp, kan kunden behöva installera relevant programvara (”kundens webbplatsproxy”) enligt installationsanvisningarna. Användning av kundens webbplatsproxy lyder under det Slutanvändarlicensavtal som medföljer kundens webbplatsproxy.

5.3 Kunden bekräftar att man är medveten om att data för detaljerade rapporter sparas i maximalt fyrtio (40) dagar och att de därefter inte kommer att finnas tillgängliga för kunden. ClientNets sammanställda data finns tillgängliga under en period på maximalt tolv (12) månader.

5.4 Kunden kan begära en förlängd rapporteringsperiod för ClientNets detaljerade rapport på upp till maximalt sex (6) månader genom att abonnera på WSS Utökat Sparande av data.

6. Allmänna villkor och bestämmelser

6.1. INGEN SKANNINGSPROGRAMVARA KAN GARANTERA 100 % DETEKTERING OCH DÄRFÖR KAN SYMANTEC INTE PÅTA SIG NÅGOT ANSVAR FÖR SKADA ELLER FÖRLUST SOM DIREKT ELLER INDIREKT UPPSTÅR PÅ GRUND AV ATT Web v2 Protect MISSLYCKATS MED ATT DETEKTERA VIRUS, SKADLIG KOD, SPIONPROGRAM ELLER ADWARE.

6.2. Symantec betonar att konfigureringen av Web v2 Protect helt kontrolleras av kunden. Web v2 Protect är ämnat att användas enbart för att möjliggöra för kunden att bevaka existerande, verkliga och tillämpade riktlinjer för godtagbar datoranvändning (eller motsvarande). I vissa länder kan det krävas att individuell personal ger sitt samtycke. Symantec rekommenderar att kunden alltid kontrollerar lokal lagstiftning före användande av Web v2 Protect. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av Web v2 Protect.

6.3 Kundens webbtrafik vid användande av Web v2 Protect får inte överskrida trettio megabyte (30 MB) per användare per dag (uträknat som ett genomsnitt per användare bland kundens totala registrerade användning gällande Web v2 Protect). Om denna dagliga gräns skulle överskridas förbehåller sig Symantec rätten att:

6.3.1 omedelbart upphöra att tillhandahålla eller avbryta all eller del av Web v2 Protect fram tills dess att denna överanvändning åtgärdats; eller

6.3.2 kräva att kunden köper ytterligare användare för att motsvara kundens faktiska webbtrafikanvändning samt lämna ytterligare fakturor och/eller justera efterföljande fakturor för att proportionerligt täcka kostnaderna för ökningen av registrerad användning under den resterande delen av den aktuella faktureringsperioden.

Appendix 7 – Symantec MessageLabs Web v2 URL.cloud

1. Översikt

1.1. När de relevanta konfigureringsändringarna har gjorts kommer begäran om webbsidor och bilagor att elektroniskt ledas via Symantec webbadressfiltrering (”Web v2 URL”) och undersökas digitalt.

2. Beskrivning av Tjänsten

2.1. Kundens externa begäran om HTTP och FTP-över-HTTP inklusive alla bilagor, makron och programfiler leds genom Web v2 URL.

3. Konfigurering

3.1. Konfigureringsinställningar som krävs för att dirigera extern trafik via Web v2 URL utförs och upprätthålls av kunden och är beroende av kundens tekniska infrastruktur. Kunden bör se till att intern HTTP/FTP-över-HTTP-trafik (t.ex. till företagets intranät) inte leds via Web v2 URL. Om kunden har Internettjänster som kräver en direkt anslutning i stället för via proxy ansvarar kunden för att göra nödvändiga ändringar i sin egen infrastruktur för att möjliggöra detta.

3.2. Åtkomst till Web v2 URL begränsas med hjälp av skannings-IP, dvs. IP-adress(er) från vilka kundens webbtrafik kommer. Skannings-IP används även för att identifiera kunden och dynamiskt välja kundspecifika inställningar.

3.3. Kunden kan konfigurera Web v2 URL för att skapa policyregler för åtkomstbegränsning via ClientNet (baserat både på kategorier och på typ av innehåll), samt kan använda dessa vid specifika tillfällen för specifika användare eller grupper genom kundens webbplatsproxy som beskrivs i Klausul 5.1.

3.4. KUNDEN BEKRÄFTAR ATT MAN ÄR MEDVETEN OM ATT WEB URLv2 FRÅN BÖRJAN KOMMER ATT FÖRSES MED SYMANTEC STANDARDINSTÄLLNINGAR OCH ATT DET HELT ÅLIGGER KUNDENS ANSVAR ATT KONFIGURERA WEB URLv2 VIA CLIENTNET SÅ ATT TJÄNSTEN MOTSVARAR DE EGNA BEHOVEN. Standardinställningarna omfattar en funktion med ”Blockera och registrera” för följande URL-adresskategorier:

3.4.1 Pornografi/sexuellt anstötlig
3.4.2 Spionprogram
3.4.3 Skräppostadresser
3.4.4 Kriminell aktivitet.

3.5 Fjärranvändarsupport är ett frivilligt alternativ som utökar Webb URL v2 till användare som inte befinner sig inom företagets nätverk (t.ex. användare som arbetar hemifrån). Kunden måste installera en PAC-fil på användarens dator så att användaren förs till Symantec webbportal när han startar sin webbläsare. För att nå portalen måste användaren skriva in ett lösenord och användarnamn. En mall för PAC-fil kan laddas ner från ClientNet och modifieras av kunden.

4. Varningar

4.1. Om en användare begär en webbsida eller bilaga för vilken en policy för åtkomstbegränsning gäller kommer åtkomst till webbsidan att nekas och användaren kommer se en automatisk varningssida. I sällsynta fall, där ett eller flera element i innehållet i en begäran blockerats, kan det hända att det inte går att visa varningssidan och varningssidan kan komma att ersätta innehållet i den begärda sidan, men åtkomst till den berörda sidan eller bilagan kommer fortfarande att nekas.

4.2. Det finns en del i den automatiska varningssidan som kunden kan anpassa via ClientNet.

5. Rapportering

5.1. Rapportering om resultatet av en kunds riktlinjer för åtkomstbegränsning vilka skapats enligt Klausul 3.3 ovan tillhandahålls via ClientNet.

5.2 För att möjliggöra administration och rapportering för varje enskild användare eller grupp, måste kunden installera relevant programvara (”kundens webbplatsproxy”) enligt installationsanvisningarna. Användning av kundens webbplatsproxy lyder under det Slutanvändarlicensavtal som medföljer kundens webbplatsproxy.

5.3 Kunden bekräftar att man är medveten om att data för detaljerade rapporter enbart sparas i maximalt fyrtio (40) dagar och att de därefter inte kommer att finnas tillgängliga för kunden. ClientNets sammanställda data finns tillgängliga under en period på maximalt tolv (12) månader.

5.4 Kunden kan begära en förlängd rapporteringsperiod för ClientNets detaljerade rapport på upp till maximalt sex (6) månader genom att abonnera på WSS Utökat Sparande av data.

6. Allmänna villkor och bestämmelser

6.1. INGEN WEBBADRESSFILTRERING KAN GARANTERA 100 % DETEKTERING OCH DÄRFÖR KAN SYMANTEC INTE PÅTA SIG NÅGOT ANSVAR FÖR SKADA ELLER FÖRLUST SOM DIREKT ELLER INDIREKT UPPSTÅR PÅ GRUND AV ATT Web v2 URL MISSLYCKATS MED ATT DETEKTERA BLOCKERADE URL-ADRESSER ELLER INNEHÅLL.

6.2. Symantec betonar att konfigureringen av Web v2 URL helt kontrolleras av kunden. Web v2 URL är ämnat att användas enbart för att möjliggöra för kunden att bevaka existerande, verkliga och tillämpade riktlinjer för godtagbar datoranvändning (eller motsvarande). I vissa länder kan det krävas att individuell personal ger sitt samtycke. Symantec rekommenderar att kunden alltid kontrollerar lokal lagstiftning före användande av Web v2 URL. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av Web v2 URL.

6.3 Kundens webbtrafik vid användande av Web v2 URL får inte överskrida trettio megabyte (30 MB) per användare per dag (uträknat som ett genomsnitt per användare bland kundens totala registrerade användning gällande Web v2 URL). Om denna dagliga gräns skulle överskridas förbehåller sig Symantec rätten att:

6.3.1 omedelbart upphöra att tillhandahålla eller avbryta all eller del av Web v2 URL fram tills dess att denna överanvändning åtgärdats; eller

6.3.2 kräva att kunden köper ytterligare användare för att motsvara kundens faktiska webbtrafikanvändning, samt lämna ytterligare fakturor och/eller justera efterföljande fakturor för att proportionerligt täcka kostnaderna för ökningen av registrerad användning under den resterande delen av den aktuella faktureringsperioden.

Appendix 8 – Symantec e-postarkivering P (Email Archiving P)

1. Översikt av Tjänsten

1.1 Symantec MessageLabs Email Archiving.cloud (P), Symantec MessageLabs Email Archiving.cloud Lite (P) och Symantec MessageLabs Email Archiving.cloud Premium (P) (tillsammans ”Arkivering (P)”) är hybridhanterade arkiveringstjänster för arkivering, lagring och hämtning av e-postmeddelanden.

1.2 För kunder med *upp till 500 användare*, inkluderar *Symantec MessageLabs Email Archiving.cloud Lite (P)* följande:

(i) standardfunktioner enligt beskrivning i Klausul 3 nedan
(ii) lagringstid på 3 år
(iii) maximal lagring på 3 GB per användare (uträknat som ett genomsnitt per användare baserat på totalt antal användare).

För kunder med *över 500 användare*, inkluderar *Symantec MessageLabs Email Archiving.cloud Lite (P)* följande:

(i) standardfunktioner enligt beskrivning i Klausul 3 nedan
(ii) lagringstid på 3 år
(iii) maximal lagring på 1,5 GB per användare (uträknat som ett genomsnitt per användare baserat på totalt antal användare).

1.3 För kunder med *upp till 500 användare*, inkluderar *Symantec MessageLabs Email Archiving.cloud (P)* följande:

(i) standardfunktioner enligt beskrivning i Klausul 3 nedan
(ii) lagringstid på 10 år
(iii) maximal lagring på 10 GB per användare (uträknat som ett genomsnitt per användare baserat på totalt antal användare).

För kunder med *över 500 användare*, inkluderar *Symantec MessageLabs Email Archiving.cloud (P)* följande:

(i) standardfunktioner enligt beskrivning i Klausul 3 nedan
(ii) förvaring i obegränsad tid
(iii) maximal lagring på 6 GB per användare (uträknat som ett genomsnitt per användare baserat på totalt antal användare).

1.4 För kunder med *upp till 500 användare*, inkluderar *Symantec MessageLabs Email Archiving.cloud Premium (P)*följande:

(i) standardfunktioner enligt beskrivning i Klausul 3 nedan
(ii) premiumfunktioner enligt beskrivning i Klausul 4 nedan
(iii) lagringstid på 10 år
(iv) maximal lagring på 10 GB per användare (uträknat som ett genomsnitt per användare baserat på totalt antal användare).

För kunder med *över 500 användare*, inkluderar *Symantec MessageLabs Email Archiving.cloud Premium (P)* följande:

(i) standardfunktioner enligt beskrivning i Klausul 3 nedan
(ii) premiumfunktioner enligt beskrivning i Klausul 4 nedan
(iii) lagring i obegränsad tid
(iv) maximal lagring på 6 GB per användare (uträknat som ett genomsnitt per användare baserat på totalt antal användare).

1.5 Kunden måste konfigurera alternativ för journal i Exchange för att deponera en kopia av interna och externa e-postmeddelanden i en lokal postlåda på Exchange-servern. Enhet(er) som befinner sig bakom brandväggen inne i kundens företagsnätverk (”enhet(er) för e-postarkivering”) kan sedan användas för att hämta data från denna postlåda för inlämnande till e-postarkivering (P). E-postmeddelanden raderas inte från journalpostlådan före lagring i e-postarkivering (P) bekräftats.

1.6 Symantec kommer att bevaka kundens faktiska användande av e-postarkivering (P) och om den faktiska lagring överskrider den mängd lagring som köpts kommer kunden att behöva köpa ytterligare lagringsblock till Symantec aktuell taxa. Symantec kommer att sända ytterligare fakturor och/eller göra justeringar i efterföljande fakturor för att proportionerligt täcka avgifter för den ökade lagringen under kvarstående del av den aktuella faktureringsperioden.

1.7 Kunden bekräftar att man är medveten om och samtycker till att ett e-postmeddelande då det arkiverats inte kan raderas före den förutbestämda lagringsperioden gått ut. Det betyder att det inte går att selektivt radera individuella e-postmeddelanden.

1.8 Kunden bekräftar att man är medveten om och samtycker till att Symantec inte kan agera som tredje parts nedladdare. Om kunden behöver utse en tredje parts nedladdare för att följa vissa regler, skall Symantec för detta ändamål vidta rimliga åtgärder för att underlätta ett direkt och oberoende avtal mellan kunden och Symantec tredjeparts tjänsteföretag. Kunden bekräftar att man är medveten om att denna tredje part kan ta ut avgifter för denna tjänst.

2. Aktivering av Tjänsten

2.1 Kunden måste korrekt fylla i Symantec formulär gällande tillhandahållande av Tjänsten.

2.2 Kunden måste köpa enhet(er) för e-postarkivering för att kunna erhålla tjänsten e-postarkivering (P). Enhet(er) för e-postarkivering som inköpts (och medföljande dokumentation) kommer att levereras till kunden för installation och konfigurering. Kunden ansvarar för alla fraktavgifter, tullavgifter, försäkringar och skatter gällande enheten för e-postarkivering.

2.3 Symantec kommer att kontakta kunden för att planera in ett första kundsamtal.

2.4 Åtgärderna som beskrivs i Symantec Installationsdokument för kunden måste slutföras av kunden före det första kundsamtalet och omfattar men inskränks inte till att:

2.4.1 Skapa nytt Active Directory-användarkonto
2.4.2 Skapa ytterligare Active Directory-grupper
2.4.3 Lägga användare i Exchange-grupper
2.4.4 Konfigurera brandvägg (om det behövs)
2.4.5 Aktivera Microsoft Exchange journal (tidigast 48 timmar före installation av enheten för e-postarkivering)
2.4.6 Installera enheten för e-postarkivering (”in rack” och ”booted up”)
2.4.7 Kontrollera att alla postlådor som behövs för arkivering har ”e-post aktiverad”
2.4.8 Konfigurera fjärråtkomst för Symantec.

Kunden kan ringa Symantec kundtjänstansvarige för hjälp med ovanstående åtgärder.

2.5 Det första kundsamtalet skall ske via WebEx. Under detta samtal skall parterna:

2.5.1 kontrollera att alla åtgärder i kundens Installationsdokument har genomförts
2.5.2 installera arkiveringsprogram och annan programvara med hjälp av Symantec Dokument med installationsprocedurer för arkivering
2.5.3 kontrollera Active Directory-installationen
2.5.4 aktivera Tjänsten
2.5.5 kontrollera att användargränssnittet går att komma åt
2.5.6 kontrollera arkivering (plats-till-plats)
2.5.7 skapa kopior av krypteringsnycklar i enlighet med Symantec Dokument med procedurer för säkerhetskopiering av nycklar.

2.6 En utbildning finns tillgänglig vid eller efter det första kundsamtalet och omfattar delar som fokuserar på: (i) IT, (ii) policy, (iii) bevakning, (iv) slutanvändare.

2.7 Ett uppföljningssamtal äger rum cirka en (1) vecka efter aktiveringen. Efter att uppföljningssamtalet genomförts och allt är i ordning kan kunden följa standardprocedurer för support om vidare hjälp behövs.

3. Standardfunktioner

3.1 *Adressresolution och Distributionslista/Gruppexpansion*. Alla e-postadresser som av Exchange markerats som interna kommer att härledas till motsvarande användares postlåda. För varje distributionslista som anges som en mottagare av ett meddelande kommer en lista på de vid tillfället aktuella medlemmarna att sparas som extra metadata rörande e-postmeddelandet.

3.2 *Index med fullständig text*. Enheten för e-postarkivering kan ta ut textinnehåll från olika typer av bilagor liksom från gemensamma fält i meddelandet för att hjälpa till att skapa ett index med fullständig text för sökning inom e-postarkivering (P).

3.3 *Kryptering.* Meddelandets innehållsdata och indexdata (med undantag för fält som datum och annan ej personligen identifierbar information) krypteras med hjälp av branschens standardteknik för kryptering på basen av en krypteringsnyckel som är specifik för kunden och som enbart kunden har tillgång till. Enbart kunden har tillgång till alla lösenord, krypteringsnycklar och konfigureringsinställningar. Därför bör kunden se till att de skyddas och förvaras deponerade eller på annan lämplig plats. Symantec kan inte påta sig ansvar för förlust av lösenord, krypteringsnycklar eller konfigureringsinställningar. Kunden är medveten om att förlust av lösenord och krypteringsnycklar kommer att medföra att arkivet blir omöjligt att komma åt.

3.4 *Riktlinjer för lagring*. Kunden kan definiera och uppdatera riktlinjer för lagring via användargränssnittet. Varje riktlinje för lagring kan ta hänsyn till olika kriterier, inklusive berörda parter, nyckelord/fraser i innehållet samt bilagors filtyper. Varje gång ett meddelande arkiveras kommer det att utvärderas enligt de riktlinjer för lagring som vid tillfället är aktuella. Om ett meddelande matchar mer än ett kriterium i riktlinjen för lagring kommer det kriterium som medför den längsta lagringstiden att tillämpas. Om inget specifikt kriterium i riktlinjer för lagring matchar meddelandet kommer standardriktlinjer att tillämpas.
3.5 *Informationstaggar (metadata)*. Kunden kan definiera och uppdatera informationstaggar via användargränssnittet. Varje informationstagg för sparande kan ta hänsyn till olika kriterier, inklusive berörda parter, nyckelord/fraser i innehållet samt bilagors filtyper. Varje gång ett meddelande arkiveras kommer det att utvärderas enligt aktiva informationstaggar och flaggas för varje informationstagg som gäller.
3.6 *Spårning av riktlinjer*. Ändringar i riktlinjer för lagring och bevakning sparas i referenssyfte av systemet i oförändrad form. Kunden kan skapa en PDF-fil med aktuella eller tidigare versioner av riktlinjer via användargränssnittet.
3.7 *Spårning av användarhistorik*. En lista över alla användare som har en postlåda inom Exchange lämnas varje kväll in till systemet för att kunna hålla en löpande lista över alla postlådor som funnits sedan e-postarkivering (P) implementerades. Denna information kan användas för att skapa riktlinjer och juridiskt förvar som omfattar användare som tagits bort från Active Directory, liksom för att ge användare tillgång till före detta anställdas e-post.
3.8 *Stubbning av bilagor*. Kunden kan aktivera en funktion som ersätter bilagors innehåll i kundens e-postsystem (”postlådedata”) med en pekare som leder till kopia av dokumentet inom arkivet. Kunden kan definiera och uppdatera riktlinjer för stubbning med olika regler för varje grupp av postlådor, baserat på meddelandets ålder och storlek liksom i vilken mapp det befinner sig. För att underlätta automatisk hämtning av den ursprungliga bilagan från arkivet när användare vidarebefordrar e-post, kan kunden installera sitt eget formulär för stubbning av bilagor i sitt bibliotek av organisationsformulär (en speciell offentlig mapp i Exchange-servern). Outlook kommer automatiskt att installera det egna formuläret från servern. För att underlätta åtkomst vid hämtning av bilagor utanför kundens nätverk kan kunden installera Archive Proxy i sina front-end (OWA) Exchange-servrar. Som standard kommer enbart postlådedata som tidigare arkiverats att stubbas. Kunden kan aktivera ett alternativ som lagrar en kopia av bilagor som inte tidigare arkiverats för att underlätta stubbning av bilagorna i postlådan. Kunden kan konfigurera riktlinjer för lagring beträffande varje enskild postlåda för att definiera hur länge bilagor som lagras på detta sätt skall sparas. Om detta inte specificeras kommer standardriktlinjer för lagring att gälla för dessa. Bilagor som lagras på detta sätt kan inte sökas i arkivet.
3.9 *Slutanvändares åtkomst*. Kunden kan välja att ge individuella användare åtkomst för sökning i arkivet, antingen i användargränssnittet eller direkt i Outlook.
3.10 *Åtkomst vid juridisk utredning*. Kunden kan genom användargränssnittet söka i hela arkivet. Kunden kan skapa ”juridisk förvaring” som är en lagringsplats för meddelanden som är relevanta i ett visst fall. Kunden kan söka inom juridisk förvaring på samma sätt som i det aktiva arkivet.
3.11 *Ad-hoc juridisk förvaring*. Kunden kan använda användargränssnittet för riktlinjer för att definiera och uppdatera ad-hoc juridisk förvaring. Juridisk förvaring kan ta hänsyn till olika kriterier, inklusive berörda parter, nyckelord/fraser i innehållet samt bilagors filtyper. Varje gång ett meddelande arkiveras kommer det att utvärderas enligt juridisk förvaring som vid tillfället är aktuell. Meddelandet sammanlänkas med varje juridisk förvaring det matchar. För att hämta befintliga arkiverade data till ett ad-hoc juridisk förvaring kan kunden göra en sökning med liknande kriterier, kopiera resultatet till en mapp och sedan kopiera innehållet i mappen till juridisk förvaring. Varje ad-hoc juridisk förvaring har en obegränsad lagringstid – alla meddelanden i en viss ad-hoc juridisk förvaring sparas tills förvaringen upphävs.
3.12 *Personbaserad juridisk förvaring*. Kunden kan använda användargränssnittet för riktlinjer för att definiera och uppdatera personbaserad juridisk förvaring. Varje personbaserad juridisk förvaring definierar ett antal användare. Varje gång ett meddelande arkiveras kommer det, om det involverar en av de personer som finns med på listan för en viss juridisk förvaring, att associeras med denna förvaring. Systemet hämtar automatiskt även befintliga e-postmeddelanden tillhörande användare som finns med på listan för juridisk förvaring och skapar en ny kopia av meddelandet i förvaringen. När användare tas bort från listan för en personbaserad juridisk förvaring, kommer enbart de meddelanden som tillhör de användare som tagits bort från listan att automatiskt tas bort från förvaringen. Meddelanden gällande användare som finns med på en lista för en juridisk förvaring sparas tills förvaret upphävs.
3.13 *Dataexport*. Meddelanden från det aktiva arkivet eller en juridisk förvaring kan exporteras till PST-filer. Systemet kommer att skapa flera PST-filer om så krävs på grund av filstorleksbegränsningar.
3.14 *Rapportering*. Rapporter om arkivets storlek och tillväxt finns tillgängliga för kunden via användargränssnittet och kan visas i HTML-format eller exporteras till PDF- eller CSV-format (enbart data).
3.15 *Granskningsspår*. Sökningar, visa meddelanden, export, hämtning och bevakning spåras. Granskningsspåret kan visas som egenskap för ett visst meddelande. En visning av granskningsspår för alla meddelanden möjliggör filtrerade visningar enligt typ av aktivitet, personen som utförde aktiviteten och/eller datum då aktiviteten ägde rum.
3.16 *Integrering med Active Directory.* Åtkomst till arkivet hanteras genom att lägga till användare (eller befintliga grupper av användare) i ett antal förutbestämda säkerhetsgrupper inom Active Directory. Var och en av dessa grupper har ett antal associerade privilegier. En användare kan inneha flera olika roller genom att tillhöra flera av dessa säkerhetsgrupper. Autentisering sker direkt gentemot Active Directory. Användare loggar in med hjälp av standard Active Directory användarnamn och lösenord och inaktiverade konton kommer att förlora sina åtkomsträttigheter för arkivet. Active Directory grupper kan även konsulteras av ett antal andra aspekter i systemet för att underlätta administration av element som t.ex. riktlinjer. En synkronisering sker varje natt för att registrera ändringar i gruppmedlemskap.
3.17 *Hantering av lagring och radering*. På basen av riktlinjer för lagring som kunden angett i användargränssnittet, kommer e-postarkivering (P) att kategorisera meddelanden och antingen tilldela dem ett datum för radering eller registrera den månad då meddelandet arkiverades för lagring i obegränsad tid. Datum för radering förläggs till början av varje månad. När ett meddelande har uppnått datum för radering kan kundens auktoriserade användare formellt godkänna radering av alla meddelanden som länkats till radering vid detta datum. För meddelanden som arkiverats för lagring i obegränsad tid, kan kundens auktoriserade användare formellt godkänna radering för alla meddelanden som arkiverats under en viss månad. Kunden bekräftar att man är medveten om och samtycker till att data som raderats på detta sätt inte kan återställas från någon typ av lagringsmedia (inklusive men utan att inskränkas till från säkerhetslagring) på ett sätt som är och blir läsbart.

4. Premiumfunktioner
Följande funktioner ingår enbart i *Symantec MessageLabs Email Archiving.cloud Premium (P)*:
4.1 *Bevakning.*
4.1.1 *Automatiska val för bevakande granskning.* Kunden kan definiera och uppdatera riktlinjer via användargränssnittet och lägga till meddelanden i en granskningskö. Varje riktlinje beaktar involverade parter, nyckelord/fraser i innehållet, liksom filtyper. Dessutom kan slumpmässiga provtagningsriktlinjer konfigureras för specifika användare.
4.1.2 Bevakande granskning. Kunden kan tilldela åtkomsträttigheter för granskare som får läsa meddelanden som lagts till i granskningskön och flagga dem som acceptabla eller ej.
4.2 *Bloomberg arkivering*
4.2.1 E-postarkivering Premium (P) använder Bloomberg Professional Services loggningsarkivering som registrerar e-postmeddelanden och snabbmeddelandekonversationer i XML-filer som varje natt publiceras på Bloombergs FTP-webbplats.
4.2.2 Om kunden abonnerar på Bloomberg Professional Service, kan enheten för e-postarkivering användas för att hämta kopior av dessa XML-filer från FTP-webbplatsen för omvandling till HTML-formaterade meddelanden och inlämning till arkivet.

4.2.3 FIRMA-formatet men inte KONTO-formatet eller historikformatet i Bloomberg loggningen stöds.
4.2.4 Bloomberg arkiveringsintegrationen tömmer inte innehållet från Bloombergs FTP-webbplats, men spårar vilka filer som har bearbetats. Då Bloomberg regelbundet tömmer innehåll från sin FTP-webbplats och Bloomberg arkiveringsintegrationen tömmer kopior som skapats i enheter för e-postarkivering måste kunden kontinuerligt bevaka att arkiveringsintegrationen fungerar så att filer inte raderas innan Bloomberg arkiveringsintegrationen har hunnit hämta och bearbeta dem fullständigt.
4.2.5 En lista över Bloombergs FIRMA-identiteter används för att identifiera vilka av de användare som anges i XML som är interna anställda. Bloomberg arkiveringsintegrationen tillhandahåller ett webbaserat användargränssnitt för mappning vilket gör att en administratör kan länka vart och ett av Bloomberg användarkontona till motsvarande Active Directory användarkonto. Då XML-filerna bearbetas kommer en adress där meddelandet refererar till en intern användare som ännu inte mappats att föras in på en lista över ej mappade adresser och meddelandet kommer inte att bearbetas. När administratören har mappat dessa adresser kan de utlösa återbearbetning av de associerade meddelandena. De härledda företags e-postadresserna används som avsändare/mottagare av meddelandet.
4.2.6 Ett informationsfält i meddelandetexten ger ytterligare information om de faktiska adresserna/visningsnamnen tillhörande parterna i konversationen, inklusive användarens Bloomberg kontoinformation.

5. Import av äldre data
5.1 Kunden kan importera äldre data till e-postarkivering (P) mot en avgift baserad på mängden data som importeras. Om den faktiska mängden äldre data överskrider den mängd dataimport som köpts förbehåller sig Symantec rätten att ta ut en avgift för denna ytterligare mängd data till den standardtaxa som gäller vid tillfället.
5.2 Om kunden väljer att använda en oberoende tredje parts programvara för att underlätta importen av data till arkivet bekräftar kunden att man är medveten om och samtycker till att Symantec inte ansvarar för denna tredje parts programvara och att kunden gör detta på egen risk och bekostnad.

6. Uppsägning av Tjänst
6.1 Vid uppsägning av Tjänsten Archiving.cloud (P) tar Symantec bort Kundens uppgifter från arkivet. Före uppsägning kan Kunden antingen hämta sina data från arkivet eller begära att annan part utsedd av Symantec för över arkiverade data till Kunden i PST-filformat enligt punkt 6.2 nedan. .
6.2 Om Kunden begär att en utomstående part utsedd av Symantec ska föra över arkiverade data vid uppsägning gäller följande:
6.2.1 Kunden måste ingå ett direkt avtal med den utsedda parten. Symantec ska inte vara part i avtalet.
6.2.2 Eftersom data lagras i krypterat format ska Kunden tillhandahålla den utomstående parten en krypteringsnyckel så att e-posten kan avkodas till ett fritt format.
6.2.3 Kunden ansvarar för överföringskostnaderna. Kostnaderna ska fastställas i avtalet med den utomstående parten. Kostnaderna beror på följande: (i) mängden data, (ii) format/överföringsmedium, (iii) kostnader för att organisera överföringsprocessen, (iv) tid och material som används för att genomföra överföringen.
6.2.4 Symantec förbehåller sig rätten att debitera Kunden enligt sina vid tidpunkten gällande priser för lagring, om Kundens data inte har exporterats och tagits bort från arkivet vid det faktiska uppsägningsdatumet.

7. Villkor och bestämmelser för Tjänsten
7.1 Symantec kan helt enligt eget gottfinnande, med omedelbar verkan och utan föregående meddelande, säga upp e-postarkivering (P), samt vidta de försvarsåtgärder man finner nödvändiga:
7.1.1 På order av domstol eller auktoriserad myndighet.
7.1.2 Vid angrepp mot e-postarkivering (P) eller nätverket.
7.1.3 Om kunden eller någon av kundens användare bryter mot riktlinjerna för godtagbar användning i Klausul 7.3 nedan.
7.2 Kunden ansvarar för att tillse att kunden själv och alla kundens användare är medvetna om och följer riktlinjerna för godtagbar användning i Klausul 7.3 nedan.
7.3 *Riktlinjer för godtagbar användning*. Användare får under inga som helst omständigheter begå, försöka begå, hjälpa till att begå eller medverka till handlingar som medvetet, på grund av vårdslöshet eller omedvetet kan hota e-postarkivering (P). Detta skall omfatta men inte inskränkas till:
7.3.1 Försök att krascha tjänstens värdar eller nätverk.
7.3.2 Angrepp med ”nekande av tjänst” eller ”översvämningsangrepp” mot tjänstens värdar eller nätverk.
7.3.3 Försök att kringgå användarautentiseringen eller säkerheten hos tjänstens värdar eller nätverk.
7.3.4 Orimlig användning av e-postarkivering (P).
7.3.5 Skapa, överföra, lagra eller publicera någon typ av virus, skadliga program eller skadliga data.
7.3.6 Alla andra handlingar som negativt kan påverka e-postarkivering (P) eller dess funktion.
7.4 INGEN E-POSTARKIVERINGSTJÄNST KAN GARANTERA 100 % KORREKTHET OCH DÄRFÖR KAN SYMANTEC, MED UNDANTAG FÖR VAD SOM UTTRYCKLIGEN ANGES I TJÄNSTENIVÅAVTALET, INTE PÅTA SIG NÅGOT ANSVAR FÖR SKADA ELLER FÖRLUST SOM DIREKT ELLER INDIREKT UPPSTÅR PÅ GRUND AV ATT TJÄNSTEN MISSLYCKATS MED ATT UTFÖRA SIN FUNKTION.
7.5 Kunden bekräftar att man är medveten om att e-post kan innehålla personligen identifierbar information och att arkivering av e-post därmed medför bearbetning av personlig information. Vidare bekräftar kunden att man är medveten om att e-postarkivering (P) är en konfigureringstjänst och att kunden ensam ansvarar för konfigureringen av e-postarkivering (P) i enlighet med sina riktlinjer för godtagbar datoranvändning (eller motsvarande), liksom alla gällande lagar och bestämmelser. Alla exempel som tillhandahålls av Symantec är enbart ämnade att hjälpa kunden att skapa sina egna anpassade riktlinjer och exempel. Därför rekommenderar Symantec att kunden alltid kontrollerar lokal lagstiftning före användande av e-postarkivering (P) och ser till att alla anställda är medvetna om och uppfyller sina ansvarsområden beträffande dataskydd, sekretesslagstiftning och/eller regler gällande kundens användning av e-postarkivering (P). I vissa länder kan det krävas att individuell personal ger sitt samtycke före e-postarkivering (P) tas i bruk. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av e-postarkivering (P). Kunden bör beakta detta vid konfigureringen av e-postarkivering (P).
7.6 Kunden måste välja ort för arkiveringsdatacenter vid beställningstillfället och avgifter räknas ut på basen av detta val. OM ETT ARKIVERINGSDATACENTER VÄLJS I USA SAMTYCKER KUNDEN TILL ATT VIDTA ALLA NÖDVÄNDIGA ÅTGÄRDER FÖR ATT (I) INFORMERA ALLA SINA ANSTÄLLDA, REPRESENTANTER OCH UNDERLEVERANTÖRER, LIKSOM TREDJE PARTER SOM ANVÄNDER KOMMUNIKATIONSSYSTEMET SOM TÄCKS AV E-POSTARKIVERING (P) OM ATT ALL INFORMATION, INKLUSIVE MEN UTAN ATT INSKRÄNKAS TILL INDIVIDERS PERSONLIGEN IDENTIFIERBARA INFORMATION KAN KOMMA ATT BEARBETAS I USA; SAMT (II) FÖR ATT SKAFFA SIG DESSA ANSTÄLLDAS, REPRESENTANTERS, UNDERLEVERANTÖRERS OCH TREDJE PARTERS SAMTYCKE TILL DENNA BEARBETNING FÖRE E-POSTARKIVERING (P) TAS I BRUK.
7.7 Kunden bekräftar att man är medveten om och samtycker till (i) att Symantec skanningstjänster (e-post AV, e-post AS, e-post IC och e-post CC) inte skannar alla e-postmeddelanden när de förs in i arkivet och (ii) att Symantec skanningstjänster (e-post AV, e-post AS, e-post IC och e-post CC) inte skannar e-postmeddelanden som släpps från arkivet för återinförande i användarens postlåda. Därför kan Symantec inte hållas ansvarigt för virus, skräppost, bilder eller olämpligt innehåll i sådana återinförda e-postmeddelanden och Servicenivåavtalet skall inte heller gälla sådana återinförda e-postmeddelanden.

8. Programvarulicens
8.1 Följande villkor och bestämmelser gäller för programvaran som installeras i enheten för e-postarkivering (”programvaran”):
8.1.1 Kunden bekräftar att man är medveten om och samtycker till att Symantec och/eller dess leverantörer alltid förblir ägare till programvaran. Detta avtal ger kunden en begränsad licens utan ensamrätt för användande av programvaran i samband med e-postarkivering (P) som beskrivs i detta Appendix och avser inte försäljning av programvaran eller någon annan immateriell

egendom. Alla rättigheter som uttryckligen beviljas i detta avtal förbehålles Symantec och dess leverantörer.

8.1.2 Kunden får använda en kopia av programvaran tillsammans med en enhet för e-postarkivering. I samband med detta avtal betyder ”använda” att driva, köra, visa och lagra programvaran under den tid e-postarkivering (P) tillhandahålls.

8.1.3 Programvaran skyddas av kanadensisk och amerikansk upphovsrättslagstiftning och av internationella fördrag. Kunden får inte hyra eller leasa ut programvaran eller kopiera den dokumentation som medföljer programvaran. Kunden får inte kopiera, bakåtkompilera, ta isär, demontera eller avkoda programvaran eller försöka återskapa dess källkod.

8.1.4 Kunden samtycker till att brott mot dessa bestämmelser kommer att förorsaka Symantec och dess leverantörer irreparabel skada, samt samtycker härmed till att Symantec och/eller dess leverantörer direkt får upprätthålla denna del, inklusive (men utan att inskränkas till) genom specifikt utövande av ålagd ersättningsåtgärd utöver all annan lindring som denna part i övrigt enligt lag eller rätt kan vara berättigad till.

8.1.5 All teknologi, programvara, dokumentation och alla processer som används av Symantec för att tillhandahålla e-postarkivering (P) tillhör med ensamrätt Symantec eller dess leverantörer.

Appendix 9 – Symantec MesageLabs EIM.cloud

1. Beskrivning av Tjänsten

1.1 Symantec Snabbmeddelandetjänst för Företag (Enterprise IM, ”EIM”) är en hanterad tjänst som möjliggör administrativ kontroll, central lagring och domänhantering för snabbmeddelanden.

1.2 Med undantag för MSI- och Java-versioner installeras EIM-klienten (”POD”) i varje användares arbetsstation. Alla varianter möjliggör för användaren att säkert ansluta till EIM-plattformen och använda EIM. En POD har följande funktioner:

(a) Fildelning;
(b) Säkra snabbmeddelandekonferenser;
(c) Samfunktion med offentliga nätverk för snabbmeddelanden (enbart med CONNECT-paket).

1.3 EIM-administrationsverktyget är en webbaserad konsol som gör att utsedda administratörer kan hantera domänstruktur och användarbas.

2. EIM-tjänstens funktioner

Tjänstens funktioner – Symantec MessageLabs EIM Communicate.cloud (”COMMUNICATE”)

(i) Integrerad fildelning (kapacitet på 100 MB per användare)
(ii) Lösning med säkerhetskopiering till dator
(iii) Förmåga att dela information med EIM-användare både online och offline
(iv) Listor för åtkomstkontroll
(v) Säker, 168-bits 3DES SSL krypterad POD-till-POD-kommunikation
(vi) Webbaserad administrationskonsol
(vii) Omfattande gränssnitt med användaralternativ
(viii) Avancerad detektering och spårning av närvaro
(ix) Support för ett stort antal olika proxyservrar
(x) HTTP-tunnelkapacitet
(xi) Meddelande om nya filer
(xii) Objektorienterat filsystem med omfattande sökmöjligheter.

Tjänstens funktioner – Symantec MessageLabs EIM Connect.cloud (”CONNECT”)

Alla funktioner i COMMUNICATE-paketet gäller med tillägg av följande:

(i) Kompatibilitet med andra snabbmeddelandeklienter (AOL, MSN, Yahoo!)
(ii) SMS-meddelanden (2 meddelanden per användare eller ”Användarkvot”)
(iii) Möjlighet att logga snabbmeddelanden.

Tjänstens funktioner – COLLABORATE

Alla funktioner i CONNECT-paketet gäller med tillägg av följande:

(i) Integration med WebEx
(ii) Integration med Salesforce.com.

3. Ansvar för kontonummer/lösenord.

3.1 Kunden ansvarar för all användning av administrationswebbplatsen, vare sig användningen auktoriserats av kunden eller ej och kunden ansvarar för att hemlighålla sina inloggningsuppgifter och sitt lösenord för kontot. Kunden samtycker till att omedelbart meddela Symantec vid otillåten användning av kundens konto.

4. Ansvar för innehåll och kommunikation på kundens konto.

4.1 Symantec lämnar ingen uttrycklig eller underförstådd garanti i samband med tillhandahållandet av EIM utöver vad som anges i detta avtal. Symantec garanterar inte 100 % detektering av virus och skräppost och därför kan Symantec inte påta sig något ansvar för skada eller förlust som direkt eller indirekt uppstår på grund av att EIM misslyckas med att detektera virus eller skräppost eller felaktigt identifierar ett meddelande som misstänkt virus eller skräppost vilket senare visar sig inte vara det. 4.2 Symantec lämnar ingen uttrycklig eller underförstådd garanti i samband med tillgång till EIM eller förmågan hos EIM att spara alla data.

4.3 Symantec betonar att kunden helt kontrollerar konfigureringen av EIM. I vissa länder kan det krävas att individuell personal ger sitt samtycke. Symantec rekommenderar att kunden alltid kontrollerar lokal lagstiftning före användande av EIM. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av EIM.

5. Förpliktelser

5.1 Kunden samtycker till att inte:

5.1.1 Via POD eller EIM sända eller lagra data, text, video, ljud, programvara eller annat innehåll som är olagligt.

5.1.2 Via POD eller EIM sända eller lagra innehåll som kränker patent, varumärken, upphovsrätter, publiceringsrättigheter eller andra immateriella rättigheter.

5.1.3 Sända eller lagra innehåll som bryter mot gällande lokala, delstatliga, statliga eller internationella lagar vilka skulle kunna ge upphov till civilt eller kriminellt ansvar.

5.1.4 Sända eller lagra oombett marknadsföringsmaterial, reklam, skräppost, skräpmeddelanden, kedjebrev eller andra sådana oombedda meddelanden.

5.1.5 Använda POD eller EIM för att offentligt utsända, sända eller visa innehåll för andra ändamål än för företagskommunikation.

5.1.6 Använda POD eller EIM för att medvetet sända innehåll som innehåller virus, maskar, cancelbot, tidsbomber, trojanska hästar, sniffer eller annan programkod som är utformad för att skaffa information om andra användare eller störa funktionen eller tillgången till dataprogram, databaser, EIM eller andra Internetvärdar.

5.1.7 Dölja POD-användarens identitet genom förklädnad, förfalskade rubriker, användande av tredje parters relays eller annat döljande av det sända materialets ursprung, inklusive men utan att inskränkas till att utge sig för att vara någon annan.

6. Samfunktion

6.1 Kunden erhåller samfunktion enligt Klausul 2 ovan (se CONNECT-paketet ovan). Symantec lämnar inga garantier gällande förmågan hos EIM att fungera tillsammans med andra snabbmeddelandeklienter, inklusive utan att inskränkas till AOL, MSN och Yahoo!.

7. Datalagring gällande endast USA

7.1 KUNDEN UPPMÄRKSAMMAS PÅ ATT ALLA MEDDELANDEN KOMMER ATT LAGRAS I USA OCH ATT SYMANTEC INTE KAN PÅTA SIG NÅGOT ANSVAR FÖR BROTT MOT GÄLLANDE LAGAR OCH FÖRORDNINGAR. KUNDEN ACCEPTERAR ATT KONFIGURERING OCH ANVÄNDANDE AV EIM HELT KONTROLLERAS AV KUNDEN. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av EIM. Kunden bör beakta detta vid konfigureringen av EIM.

8. Loggning och regelefterlevnad

8.1 Kunden kan välja att logga snabbmeddelanden som passerar EIM-tjänsten, förutsatt att motsvarande avgifter för loggningsfunktionen betalas.

8.2 Symantec skickar loggfiler till kunden dagligen så att kunden kan lagra loggarna i ett kompatibelt arkiv om så önskas.

8.3 Symantec sparar loggar under en period på tre (3) år, varefter loggarna raderas permanent. Kundens behöriga firmatecknare kan skriftligen begära (i) en kopia av sådana loggar eller (ii) radering av sådana loggar när som helst före den treåriga (3) arkiveringstidens utgång.

8.4 Kunden bör vara medveten om att administrationskonsolen tillåter kunden att när som helst inaktivera loggning per grupp eller undergrupp och att loggar därför kanske inte utgör en komplett bild av dess användning av EIM-tjänsten.

8.5 Symantec kan sex (6) månader i förväg ge skriftligt besked om sin avsikt att upphöra leverera och ge support för EIM-tjänsten. När denna uppsägningstid är slut ska EIM-tjänsten upphöra.

8.6 När EIM-tjänsten har upphört kan kunden begära att dess loggar återlämnas eller raderas. Om kunden inte meddelar vilket kunden föredrar inom nittio (90) dagar efter att tjänsten har upphört ska Symantec radera loggarna permanent.

8.7 Kunden är medveten om och accepterar att Symantec inte kan agera som tredjepartsnedladdare på något villkor i syfte att efterleva bestämmelserna från SEC (amerikanska finansinspektionen).

9. Programvarulicens

9.1 Beviljande av licens

I den mån det är förenligt med villkoren och bestämmelserna i detta avtal, beviljar Symantec kunden icke överförbar licens utan ensamrätt att enbart för kundens egen interna affärsverksamhet installera och använda programvaran för EIM (med

”programvara” menas var och en av Symantec programvaror för EIM i objektkodformat för vilken Symantec beviljar licens enligt villkoren i avtalet, inklusive men utan att inskränkas till nya upplagor eller uppdateringar i enlighet med vad som anges nedan). Alla immateriella egendomsrätter beträffande programvaran är och skall förbli Symantec (och/eller dess leverantörers) egendom. Symantec beviljar licens för programvaran men säljer den inte. Kunden bekräftar att man är medveten om att programvaran och all relaterad information inklusive men utan att inskränkas till uppdateringar tillhör Symantec och dennes leverantörer. Kunden ansvarar fullständigt för varje slutanvändares följande av eller brott mot villkoren i detta avtal. Kunden skall omedelbart meddela Symantec vid eventuell otillåten användning eller brott mot villkoren för denna licens.

9.2. Restriktioner gällande kopiering och användning

Kunden får ladda ner och installera programvaran på följande villkor:

9.2.1. Kunden får inte ladda ner eller installera programvaran för fler än det antal slutanvändarlicenser kunden beviljats. (Med ”slutanvändare” menas den fysiska dator på vilken programvaran installeras.)

9.2.2. Kunden får kopiera programvaran i enlighet med vad som rimligen är nödvändigt för säkerhetskopiering, arkivering och katastrofåterställning. Tryckt dokumentation får enbart reproduceras av kunden för internt bruk. (Med ”dokumentation” menas Symantec användarhandböcker och/eller bruksanvisningar för användning av programvaran som medföljer den nedladdade programvaran.)

9.2.3 Kunden får inte själv, eller tillåta någon tredje part att: (i) utan föregående skriftligt tillstånd från Symantec demontera, ta isär eller bakåtkompilera programvaran utom i den mån som uttryckligen tillåts enligt gällande lag; (ii) avlägsna någon produktidentifikation eller meddelanden om egendomsrätter; (iii) hyra ut, låna ut eller använda programvaran för timesharing eller servicebyrå; (iv) modifiera, översätta, adaptera eller skapa härledda arbeten från programvaran; eller (v) i övrigt använda eller kopiera programvaran utom enligt vad som uttryckligen anges häri.

9.3. Överföring av rättigheter

Kunden får inte överföra, tilldela eller delegera programvarulicensen i detta avtal utan föregående skriftligt tillstånd från Symantec. Ingen sådan överföring, tilldelning eller delegering i strid med ovanstående skall vara giltig.

9.4. Begränsad garanti och ansvarsbefrielse

9.4.1 Symantec garanterat att programvaran vid nedladdningen i alla materiella avseenden skall motsvara Symantec aktuella dokumentation.

9.4.2 Ovanstående garanti skall inte gälla om: (i) Programvaran inte används i enlighet med detta avtal eller dokumentation; (ii) programvaran eller del därav har modifierats av någon annan än Symantec; eller (iii) ett fel i programvaran har orsakats av kundens utrustning eller en tredje parts programvara.

9.4.3 SYMANTEC GARANTERAR INTE ATT PROGRAMVARAN KOMMER ATT FUNGERA UTAN AVBROTT ELLER FEL. SYMANTEC AVSÄGER SIG UTTRYCKLIGEN ALLA UTTRYCKLIGA, UNDERFÖRSTÅDDA ELLER ÖVRIGA GARANTIER, INKLUSIVE MEN UTAN ATT INSKRÄNKAS TILL GARANTIER GÄLLANDE SÄLJBARHET, TILLFREDSSTÄLLANDE KVALITET ELLER LÄMPLIGHET FÖR VISST ÄNDAMÅL.

9.5. Uppsägning

Vid uppsägning av EIM eller avtalet skall alla kundens häri beviljade rättigheter beträffande rätten att använda programvaran omedelbart upphöra och kunden skall omedelbart till Symantec återlämna eller förstöra alla kopior av programvaran och dokumentationen.

Appendix 10 – Symantec MessageLabs Policy Based Encryption.cloud (PBE)

1. Beskrivning av Tjänsten

1.1 Symantec MessageLabs Policy Based Encryption.cloud (Policy Based Encryption, ”PBE”) gör det möjligt att sända och motta krypterade e-postmeddelanden baserat på kundens riktlinjer för e-postsäkerhet.

1.2 För att erhålla PBE måste kunden även abonnera på följande Tjänster:

- **Symantec MessageLabs Email Boundary Encryption.cloud (”BE**”) enligt beskrivning i Bilaga 2 Appendix 5
- **Symantec MessageLabs Email Content Control.cloud (”e-post CC”)** enligt Bilaga 2 Appendix 4.

1.3 PBE tillhandahåller följande funktioner:

- Möjlighet att använda e-post CC för att definiera utgående krypteringspolicy för e-postmeddelanden.
- Leverans av krypterad e-post till extern mottagares postlåda.
- Åtkomst för mottagaren till den krypterade e-posten via en säker webbportal.
- Åtkomst för mottagaren till den säkra webbportalen för att svara på e-post i krypterat format.

2. PBE-funktioner

2.1 PBE ger kunden möjlighet att sända ett krypterat e-postmeddelande direkt till en mottagares postlåda utan att mottagaren behöver ladda ner någon programvara.

2.2 Kunden kan konfigurera krypteringsmetoden till antingen Push eller Pull. För Symantec MessageLabs Policy Based Encryption.cloud (Z) (”PBE Z”) avgör e-post CC-regeln huruvida Push eller Pull skall användas. För Symantec MessageLabs Policy Based Encryption.cloud (E) (”PBE E”) är standard krypteringsmetod Pull men kan ändras till Push av mottagaren genom nedladdning av funktionen Secure Reader i mottagarens säkra webbportal.

2.2.1 PBE-varianten ”PBE Push” sänder ett meddelande per e-post till mottagaren och sparar originalet av e-postmeddelandet i webbportalen som en krypterad bilaga. Efter registrering online kan mottagaren se det krypterade e-postmeddelandet offline med hjälp av ett Java-program på sin dator.

2.2.2 PBE-varianten ”PBE Pull” sänder ett meddelande per e-post till mottagaren. Mottagaren kan se det krypterade e-postmeddelandet online i sin webbläsare via en säker SSL-session efter att ha loggat in till en säker webbportal med hjälp av sitt lösenord.

2.3 PBE gör det även möjligt för mottagaren att gå in på en säker webbportal och svara på ett krypterat e-postmeddelande i krypterat format.

2.4 Kunden kan lägga till sitt varumärke i portalen som mottagarna använder för att läsa sina krypterade e-postmeddelanden (t.ex. lägga in logo och supportnummer).

2.5 Mottagaren av ett krypterat e-postmeddelande kan också sända helt nya e-postmeddelanden till någon av kundens PBE-användare.

2.6 Om kunden abonnerar på PBE E finns en tredje parts pluginprogram för Outlook tillgängligt som lägger till en ”Ikon för kryptering” i mottagarens verktygsfält för Outlook. Kunden bekräftar att man är medveten om och samtycker till att Symantec inte ansvarar för sådan tredje parts programvara.

2.7 Om kunden abonnerar på PBE E finns följande extrafunktioner tillgängliga:

a) Mottagaren kan välja språk för säker webbportal och meddelanden per e-post från en lista över tillgängliga språk.

b) Mottagaren kan logga in på sina konton utan att öppna ett speciellt meddelande, även om de inte har några aktiva meddelanden.

c) Mottagaren kan se alla sina tidigare meddelanden (som inte slutgiltigt raderats) i sin postlåda, inklusive sända meddelanden.

d) Om Pull-metoden används kan ett meddelande som skapats i webbportalen ha flera mottagare förutsatt att dessa mottagare delar en domän från vilken användaren tidigare mottagit ett säkert e-postmeddelande.

e) Om Push-metoden används kan mottagarna svara till en e-postadress under samma domän.

f) Det första meddelandet till nya användare finns tillgängligt på mer än ett språk.

g) Det går att använda tredje parts certifikat/nyckel för att kryptera ett utgående e-postmeddelande med hjälp av mottagarens offentliga nyckel och dekryptera ett inkommande e-postmeddelande med hjälp av mottagarens privata nyckel i stället för standard certifikat/nycklar som skapas av PBE.

3. Tillhandahållande, Fakturering och begäran om förändringar

3.1. Symantec ska börja debitera för PBE från det datum då Symantec bekräftar att kundens nätverk har teknisk möjlighet att stödja PBE (”datum för tekniskt godkännande”).

3.2 Punkt 5.2 i Bilaga 1 ska inte gälla PBE. Symantec har som mål att leverera PBE-order och begäran om PBE-förändringar inom fyra veckor från datumet för tekniskt godkännande, under förutsättning att all nödvändig informationsinhämtning, så kallad due diligence, har utförts av kunden.

3.3 Kunden samtycker till att tillhandahålla de nödvändiga tekniska resurser, information och tillstånd som behövs och att aktivera eller korrigera sin DNS e-posttjänst för anslutning till PBE.

3.4 Kunden får ändra varumärkningen av portalen högst två gånger per år.

4. Konfigurering

4.1 Kunden ansvarar för att implementera konfigureringen av PBE enligt egna behov. Kunden konfigurerar PBE via ClientNet genom att välja bland de tillgängliga alternativen under e-post CC.

4.2 Symantec betonar att konfigureringen av PBE helt kontrolleras av kunden och att denna konfigurering kommer att avgöra funktionen hos PBE. Därför kan Symantec inte påta sig något ansvar för skada eller förlust som direkt eller indirekt uppstår på grund av att PBE misslyckas med att uppfylla kundens krypteringsförpliktelser.

5. Tjänstens parametrar

5.1 Följande begränsningar gäller för PBE:

5.1.1 Antalet säkra e-postmeddelanden utsända av kunden med hjälp av PBE Z under en månad får inte överskrida trehundra (300) gånger den registrerade användningen för PBE. Antalet säkra e-postmeddelanden utsända av kunden med hjälp av PBE E under en månad får inte överskrida fyrahundraåttio (480) gånger den registrerade användningen för PBE. Vid sändning till flera mottagare kommer varje enskild adress att räknas som ett säkert e-postmeddelande Om kunden överskrider antalet tillåtna säkra e-postmeddelanden under en månad kommer Symantec att öka den registrerade användningen. Om Symantec ökar den registrerade användningen kommer Symantec helt enligt eget gottfinnande att sända ytterligare fakturor och/eller göra justeringar i efterföljande fakturor för att proportionerligt täcka avgifter för den ökade registrerade användningen under kvarstående del av den aktuella faktureringsperioden.

5.1.2 E-postmeddelanden som leds via PBE Z är begränsade till maximalt femtio megabyte (50 MB) per komprimerat e-postmeddelande. E-postmeddelanden som leds via PBE E är begränsade till maximalt femtio megabyte (50 MB per e-postmeddelande efter komprimering.

5.1.3 E-postservicenivån i Servicenivåavtalet gällande svarstid skall inte gälla för PBE.

5.1.4 Minsta antalet användare för PBE Z är 50 användare. Den första och efterföljande beställningar av PBE Z kan göras för block på 50 användare i taget eller i steg om 10 användare för beställningar som överstiger 50 användare.

5.1.5 **PBE FUNGERAR ENBART DÅ DET ANVÄNDS TILLSAMMANS MED BE OCH E-POST CC OCH KAN INTE FUNGERA SOM EN ENSKILD TJÄNST. VARJE ENSKILD PBE-ANVÄNDARE MÅSTE VARA ANVÄNDARE AV E-POST CC.**

6. Amerikansk kryptering

6.1 **KUNDEN BEKRÄFTAR ATT MAN ÄR MEDVETEN OM OCH ACCEPTERAR ATT KRYPTERING AV E-POSTMEDDELANDEN VIA PBE KOMMER ATT SKE I USA OCH ATT SYMANTEC INTE KAN PÅTA SIG NÅGOT ANSVAR FÖR BROTT MOT GÄLLANDE LAGAR OCH FÖRORDNINGAR.**

7. Villkor och bestämmelser

7.1 KUNDEN BEKRÄFTAR ATT MAN ÄR MEDVETEN OM OCH ACCEPTERAR ATT ANVÄNDANDE AV PBE HELT

KONTROLLERAS AV KUNDEN PBE är ämnat att användas enbart för att möjliggöra för kunden att bevaka existerande, verkliga och tillämpade riktlinjer för godtagbar datoranvändning (eller motsvarande). Användandet av krypteringstjänster kan i vissa länder påverkas av lagstiftning. Kunden rekommenderas att alltid kontrollera relevant lagstiftning före användande av PBE. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av PBE.

Appendix 11 – Symantec Email Continuity.cloud (« EC »)

1. Översikt av EC

1.1 EC är ett standby meddelandesystem för Microsoft Exchange- och Lotus Notes-miljöer. EC synkroniserar viktiga system och användarinformation inklusive men inte inskränkt till e-postkatalogen och individuella användares personliga kontakter. Kunden kan även konfigurera EC för att stöda BlackBerry® via trådlös vidarebefordran med hjälp av BlackBerry®s webbklient eller BlackBerry®s Internettjänst och integrerat med Outlook för användare med Outlook 2003 med cachelagrat läge eller Outlook 2007 med cachelagrat läge via en Outlook Extension.

1.2. *Versioner som stöds*: Microsoft Exchange 5.5, Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007, Lotus Notes Version 6, Lotus Notes Version 7.

1.3 *Versioner för Outlook Extension*: Microsoft Outlook 2003 i cachelagrat läge; Microsoft Outlook 2007 i cachelagrat läge.

1.4 Kunden ansvarar för att tillhandahålla och underhålla den nödvändiga maskinvaran och programvaran (enligt beskrivningen i leveransformuläret).

2. Beskrivning av EC

2.1. *Aktivering* Kunden kan begära aktivering av EC per telefon till Symantec supportteam eller via portalen för e-posthantering (Email Management Services, ”EMS”). Efter aktivering av EC kommer kunden att få meddelanden via SMS till utsedda mobiltelefoner och personliga e-postadresser. Därefter kommer EC att börja motta och sortera inkommande e-postmeddelanden, filtrera dem (i enlighet med Klausul 4.4 nedan) enligt alla andra Symantec e-posttjänster som kunden abonnerar på (t.ex. e-post AV), samt leda dem till lämpliga användares postlådor. EC kommer att lagra och spara e-posttrafik som sänds och mottas under aktiveringen i upp till trettio (30) dagar efter avaktivering för att kunden skall kunna överföra dessa e-postmeddelanden till sitt primära e-postsystem om så önskas.

2.2 *Lagring.* Kunden ansvarar för att välja vilka användares e-postmeddelanden som skall sparas och lagringstiden för var och en av dessa användare. De sparade e-postmeddelandena kommer att raderas vid det tillfället som infaller tidigare av antingen (a) då den lagringstid som valts för användaren löpt ut eller (b) då EC sägs upp. Kunden måste köpa tillräckligt med lagringsutrymme för att uppfylla lagringskraven i enlighet med Klausul 5.1 nedan.

2.3 *Autentiseringshanterare.* Kunden kan utöka sina säkerhetsriktlinjer för autentisering i samband med Microsoft Active Directory till EC genom att göra det möjligt för användare att logga in i EC-postlådor med sina Windows-lösenord och därmed eliminera behovet av ett separat EC-lösenord. Windows autentisering kräver en tillgänglig Windows-domänkontrollör som vid tiden för EC-aktiveringen kan nås av en autentiseringshanterare som kan autentisera användare som försöker logga in till EC-postlådor. Versioner som stöds: Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007

2.4 Minsta antalet användare av EC som kan köpas av kunden är det större av (a) ett antal användare som motsvarar antalet postlådor i kundens Microsoft Exchange-organisation eller (b) tio (10) användare.

3. Reserverad.

4. Konfigurering

4.1 *Delvis aktivering*: För vissa e-postsystem/versioner (Microsoft Exchange 2000, 2003 och 2007), kan EC aktiveras för underordnade grupper av kundens miljöer (en eller flera individer, servrar och/eller platser), ”delvis aktivering” för att kunna hantera mer lokala e-postavbrott.

4.2 *Aktivering*: EC-abonnemanget ger kunden rätt till tjugofyra (24) aktiveringar per år, var och en för en period på upp till tolv (12) timmar i följd (”inkluderade aktiveringar”). (Som exempel skulle en enda aktivering som pågår i sex (6) timmar räknas som en (1) aktivering och en aktivering som pågår i nitton (19) timmar skulle räknas som två (2) aktiveringar.) Om kunden har använt sin kvot av inkluderade aktiveringar kan kunden köpa ytterligare aktiveringar (var och en för tolv (12) timmar i följd) till Symantec vid tillfället aktuell taxa.

4.3 Systemtest: Systemtest skall inkludera (a) ett (1) test per kvartal av EC för alla användare, där testet pågår i fyra (4) timmar och (b) obegränsade delvisa test av upp till tio procent (10 %) av användarna för Microsoft Exchange 2000, Microsoft Exchange 2003 och Microsoft Exchange 2007. Kunden måste planera in önskat testdatum med Symantec minst sju (7) vardagar i förväg.

4.4 **KUNDEN BEKRÄFTAR ATT MAN ÄR MEDVETEN OM OCH ACCEPTERAR ATT DÅ KUNDEN BEFINNER SIG I AKTIVERAT TILLSTÅND OCH SKICKAR E-POSTMEDDELANDEN ELLER MOTTAR E-POSTMEDDELANDEN FRÅN ANDRA ORGANISATIONER SOM OCKSÅ BEFINNER SIG I AKTIVERAT TILLSTÅND, KOMMER E-POSTMEDDELANDENA ATT KRINGGÅ SYMANTEC AV KUNDEN ABONNERADE SKANNING AV INKOMMANDE OCH UTGÅENDE E-POST.**.

4.5 Om kunden använder e-post AV, e-post AS, e-post CC, och/eller e-post IC kan Symantec med hjälp av en failover-funktion konfigurera ledande av kundens e-postmeddelanden till EC-miljön inom ClientNet. Denna failover-funktion kommer att användas när EC är aktiverad.

4.6 **OM KUNDEN ANVÄNDER E-POST AV, E-POST AS, E-POST CC ELLER E-POST IC LIGGER DET PÅ KUNDENS ANSVAR ATT KONFIGURERA OCH TESTA FAILOVER-FUNKTIONEN FÖR KUNDENS E-POSTMEDDELANDEN TILL EC-MILJÖN. SÅDANA FAILOVERS MÅSTE ORDNAS I ENLIGHET MED SYMANTEC INSTRUKTIONER VID LEVERANSTILLFÄLLET OCH DÄREFTER UPPRÄTTHÅLLAS. KUNDEN BEKRÄFTAR ATT MAN ÄR MEDVETEN OM OCH ACCEPTERAR ATT E-POST INTE KAN LEDAS TILL EC OM KUNDEN SKULLE UNDERLÅTA ATT ORDNA ELLER UPPRÄTTHÅLLA SÅDANA FAILOVERS**.

5. Alternativ

5.1 *Symantec Email Continuity.cloud Storage Option*

5.1.1 Kunden måste köpa tillräckligt med lagringsutrymme för vid tillfället aktuell taxa.

5.1.2 Om kunden abonnerar på Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email & Web Safeguard.cloud, eller Symantec MessageLabs Ultimate Safeguard.cloud, inkluderar paketen maximalt 0,7 GB lagring av ny e-post per användare per år för EC och Symantec Email Continuity Archive.cloud tillsammans. Om kundens lagring av ny e-post överskrider denna tillåtna mängd lagring måste kunden köpa tillräckligt med lagringsutrymme för Tjänsten till Symantec vid tillfället aktuell taxa.

5.1.3 Om kunden inte abonnerar på ett av paketen angivna i Klausul 5.1.2 ingår ingen lagring i priset per användare och kunden måste köpa tillräckligt med lagringsutrymme för Tjänsten till Symantec vid tillfället aktuell taxa.

5.1.4 Om kunden måste köpa ytterligare lagringsutrymme, kommer Symantec att sända ytterligare fakturor och/eller göra justeringar i efterföljande fakturor för att proportionerligt täcka avgifter för den ytterligare lagringen under kvarstående del av den aktuella faktureringsperioden.

5.2 *Symantec Email Continuity.cloud Wireless Option*

5.2.1 Om kunden abonnerar på Symantec Email Continuity.cloud Wireless Option kan systemadministratörer tillhandahålla speciella BlackBerry®-enheter som hanteras av företagets RIM BlackBerry® Enterprise Servers (BES). När EC är aktiverat kommer de tillhandahållna BlackBerry®-enheterna att fortsätta att sända och motta e-post genom att kommunicera med EMS via en säker kanal som etablerats av BES-servern.

5.2.2. Versioner som stöds: Microsoft Exchange 2000, Microsoft Exchange 2003 och Microsoft Exchange 2007; BlackBerry® Enterprise Server version 4.0 (eller senare); handburna inbyggda BlackBerry®-enheter version 4.1 (eller senare).

6. Villkor och bestämmelser för EC

6.1 INGEN E-POSTKONTINUITETSTJÄNST KAN GARANTERA 100 % SYNKRONISERING OCH DÄRFÖR KAN SYMANTEC INTE PÅTA SIG NÅGOT ANSVAR FÖR SKADA ELLER FÖRLUST SOM DIREKT ELLER INDIREKT UPPSTÅR PÅ GRUND AV ATT EC MISSLYCKATS MED ATT SYNKRONISERA E-POSTSYSTEM.

6.2 Symantec betonar att kunden helt kontrollerar konfigureringen av EC. Symantec rekommenderar att kunden skaffar sig riktlinjer för godtagbar datoranvändning (eller motsvarande). I vissa länder kan det krävas att individuell personal ger sitt samtycke. Symantec rekommenderar att kunden alltid kontrollerar lokal lagstiftning före användande av EC. Symantec kan inte påta sig något ansvar för civilt eller

brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av EC.

7. Programvarulicens för EC

7.1 Beviljande av licens

I den mån det är förenligt med villkoren och bestämmelserna i detta avtal, beviljar Symantec kunden icke överförbar licens utan ensamrätt att enbart för kundens egen interna affärsverksamhet installera och använda programvaran för EC. (med ”programvara” menas var och en av Symantec programvaror för EC i objektkodformat för vilken Symantec beviljar licens enligt villkoren i avtalet, inklusive men utan att inskränkas till nya upplagor eller uppdateringar i enlighet med vad som anges nedan.) Alla immateriella egendomsrätter beträffande programvaran är och skall förbli Symantec (och/eller dess leverantörers) egendom. Symantec beviljar licens för programvaran men säljer den inte. Kunden bekräftar att man är medveten om att programvaran och all relaterad information inklusive men utan att inskränkas till uppdateringar tillhör Symantec och dennes leverantörer. Kunden ansvarar fullständigt för varje användares följande av eller brott mot villkoren i detta avtal. Kunden skall omedelbart meddela Symantec vid eventuell otillåten användning eller brott mot villkoren för denna licens.

7.2. Restriktioner gällande kopiering och användning

Kunden får ladda ner och installera programvaran på följande villkor:

7.2.1. Kunden får inte ladda ner eller installera programvaran för fler än det antal slutanvändarlicenser kunden beviljats. (Med ”slutanvändare” menas den fysiska dator på vilken programvaran installeras.)

7.2.2. Kunden får kopiera programvaran i enlighet med vad som rimligen är nödvändigt för säkerhetskopiering, arkivering och katastrofåterställning. Tryckt dokumentation får enbart reproduceras av kunden för internt bruk. (Med ”dokumentation” menas Symantec användarhandböcker och/eller bruksanvisningar för användning av programvaran som medföljer den nedladdade programvaran).

7.2.3 Kunden får inte själv eller tillåta någon tredje part att: (i) utan föregående skriftligt tillstånd från Symantec demontera, ta isär eller bakåtkompilera programvaran utom i den mån som uttryckligen tillåts enligt gällande lag; (ii) avlägsna någon produktidentifikation eller meddelanden om egendomsrätter; (iii) hyra ut, låna ut eller använda programvaran för timesharing eller servicebyrå; (iv) modifiera, översätta, adaptera eller skapa härledda arbeten från programvaran; eller (v) i övrigt använda eller kopiera programvaran utom enligt vad som uttryckligen anges häri.

7.3. Överföring av rättigheter

Kunden får inte överföra, tilldela eller delegera programvarulicensen i detta avtal utan föregående skriftligt tillstånd från Symantec. Ingen sådan överföring, tilldelning eller delegering i strid med ovanstående skall vara giltig.

7.4. Begränsad garanti och ansvarsbefrielse

7.4.1 Symantec garanterat att programvaran vid nedladdningen i alla materiella avseenden skall motsvara Symantec aktuella dokumentation.

7.4.2 Ovanstående garanti skall inte gälla om: (i) Programvaran inte används i enlighet med detta avtal eller dokumentation; (ii) programvaran eller del därav har modifierats av någon annan än Symantec; eller (iii) ett fel i programvaran har orsakats av kundens utrustning eller en tredje parts programvara.

7.4.3 SYMANTEC GARANTERAR INTE ATT PROGRAMVARAN KOMMER ATT FUNGERA UTAN AVBROTT ELLER FEL. SYMANTEC AVSÄGER SIG UTTRYCKLIGEN ALLA UTTRYCKLIGA, UNDERFÖRSTÅDDA ELLER ÖVRIGA GARANTIER, INKLUSIVE MEN UTAN ATT INSKRÄNKAS TILL GARANTIER GÄLLANDE SÄLJBARHET, TILLFREDSSTÄLLANDE KVALITET ELLER LÄMPLIGHET FÖR VISST ÄNDAMÅL.

7.5. Uppsägning

Vid uppsägning av EC skall alla kundens häri beviljade rättigheter beträffande rätten att använda programvaran omedelbart upphöra och kunden skall omedelbart till Symantec återlämna eller förstöra alla kopior av programvaran och dokumentationen.

Appendix 12 – Schemus-verktyget (Schemus Tool)

1.1 Schemus-verktyget är en programvara som synkroniserar data mellan kundens katalogserver och de av Symantec tjänster som kunden abonnerar på.
1.2 Schemus Limited beviljar kunden licens för Schemus-verktyget via ett separat slutanvändarlicensavtal (”Tredje Parts EULA”)
1.3 Kunden bekräftar att man är medveten om och samtycker till att tillgång till och användning av Schemus-verktyget sker under förutsättning att kunden accepterar och följer villkoren och bestämmelserna i detta tredje parts EULA. (En kopia av detta EULA kan på begäran erhållas från Symantec.)
1.4 Schemus-verktyget är en kontrollerad teknologi som lyder under gällande lagar och bestämmelser för import och export, vilka beskrivs mer specifikt i bestämmelserna för exportkontroll i avsnittet ”Allmänt” i avtalet. Kunden bekräftar att man är medveten om och samtycker till att man måste underteckna ett efterlevnadsintyg (i) före nedladdning av programvaran, (ii) före erhållande av licensnyckel, samt (iii) därefter en gång per år om så begärs av Symantec. (En kopia av efterlevnadsintyget kan på begäran erhållas från Symantec.)
1.5 Symantec lämnar inga (uttryckliga, underförstådda, regelmässiga eller andra) ytterligare garantier gällande Schemus-verktyget. Om fel skulle uppstå i samband med Schemus-verktyget kommer Symantec att vidta kommersiellt rimliga åtgärder för att avgöra källan till problemet och där så är lämpligt vidarebefordra problemet till Schemus Limited.
1.6 Symantec maximala ansvar gentemot kunden i samband med Schemus-verktyget skall begränsas till det större av ett belopp som motsvarar det faktiska belopp som kunden betalt till Symantec för Schemus-verktyget eller 250 brittiska pund (eller 350 euro om kunden betalar i euro).

Appendix 13 – Symantec MessageLabs Instant Messaging Security.cloud (IMSS)

1 Översikt

1.1 Kunden måste synkronisera sin användarkatalog med Symantec för att skapa en lista över användarnamn för Active Directory och motsvarande användarnamn för snabbmeddelanden (IM) inom ClientNet. En ”intern användare” är en användare som finns i kundens katalog och som laddats upp till det administrativa IMSS-gränssnittet. En ”extern användare” är en användare som inte finns i kundens katalog och/eller som inte laddats upp till det administrativa IMSS-gränssnittet.

1.2 Kunden måste även göra grundläggande brandväggsändringar för att leda sina snabbmeddelandekonversationer via Symantec.

1.3 När IMSS har konfigurerats i enlighet med Klausul 1.1 och 1.2 ovan, kommer snabbmeddelanden från interna användare till externa användare och tvärtom att ledas genom IMSS för skanning med hjälp av ledande produkter inklusive Symantec egen heuristiska skanner Skeptic™.

1.4 IMSS kan enbart skanna vissa versioner av offentliga snabbmeddelandeklienter. Symantec kommer att i ClientNet publicera en lista över de versioner av offentliga snabbmeddelandeklienter som stöds. Kunden bekräftar att man är medveten om och accepterar att Symantec med jämna mellanrum samt utan föregående meddelande kan komma att uppdatera och ändra denna lista.

1.5 Om ett **inkommande** snabbmeddelande:
1.5.1 bedöms innehålla virus eller annan skadlig kod kommer det att blockeras;
1.5.2 innehåller en URL-adress för en webbplats där virus eller annan skadlig kod har detekterats, kommer åtkomst till denna webbplats att nekas.

1.6 IMSS erbjuder ett grundläggande nätfiskeskydd som blockerar **inkommande** snabbmeddelanden som bedöms utgöra nätfiskeangrepp.

1.7 IMSS har förmåga att skanna vissa versioner av Word, Excel och PowerPoint dokument men inte andra bilagor.

1.8 IMSS kan inte skanna krypterade snabbmeddelanden.

2. Reserverad.

3. IMSS Innehållskontroll

3.1 IMSS ger kunden möjlighet att konfigurera sina egna regler på basen av en strategi för innehållsfiltrering i samband med inkommande och utgående snabbmeddelanden.

3.2 Kunden ansvarar för att via ClientNet implementera konfigureringsalternativ i enlighet med sina riktlinjer för godtagbar datoranvändning (eller motsvarande). Reglerna kan konfigureras enligt grupp eller individ. Kunden kan ändra reglerna och ändringar kommer att träda i kraft inom fyra (4) timmar.

3.3 Alternativ finns för att ange vilken åtgärd som skall vidtas vid detektering av kontrollerat innehåll i ett snabbmeddelande. Dessa alternativ beskrivs i ClientNet och i aktuell version av administratörhandboken.

3.4 Genom ClientNet kan kunden granska resultatet av sina regler i form av sammandrag för varje dag, vecka, månad och år sorterade efter både regel och användare.

4 Loggning och lagring

4.1 Om kunden har aktiverat loggningsfunktionen kommer Symantec att sammanställa dagliga loggar över skannade snabbmeddelanden. Varje logg kommer att innehålla datum och tidstämpel, innehåll, samt namn på överförda filer. Loggar som inte kan överföras till kunden skall lagras under en period på trettioen (31) dagar och därefter förstöras.

4.2 Kunden kan även konfigurera IMSS så att en kopia av varje snabbmeddelande sänds till kompatibelt arkiv eller annan lagring hos kunden.

5 Meddelanden

5.1 Kunden kan konfigurera IMSS så att ett automatiskt meddelande sänds:
5.1.1 till avsändaren och mottagaren om ett snabbmeddelande blockeras på grund av att det bedöms innehålla virus, nätfiskeangrepp eller kontrollerat innehåll; eller
5.1.2 till mottagaren om åtkomst till en webbplats nekas på grund av att den bedöms innehålla virus eller skadligt innehåll.

5.2 Kunden kan aktivera, anpassa och avaktivera meddelanden genom ClientNet.

6 Support

6.1 Support inkluderar:

6.1.1 Genomgång av IMSS-gränssnittet inklusive en beskrivning av tjänsten samt frågor och svar (Detta inkluderar inte hjälp med upplägg av regler eller analys av reglernas effektivitet);
6.1.2 Administratörhandbok
6.1.3 Användarhandbok

7 Villkor och bestämmelser för IMSS

7.1 Symantec tillhandahåller listor och exempel på regler med ord som kan ses som stötande. Kunden accepterar och samtycker till att Symantec får sammanställa och publicera listor med standardord hämtade från kundens egna ordlistor.

7.2 Kunden bekräftar att man är medveten om att snabbmeddelanden kan innehålla personligen identifierbar information och att loggning och inhämtning av snabbmeddelanden därmed medför bearbetning av personlig information. Vidare bekräftar kunden att man är medveten om att IMSS är en tjänst som går att konfigurera och att kunden ensam ansvarar för konfigureringen av IMSS i enlighet med sina riktlinjer för godtagbar datoranvändning (eller motsvarande), liksom alla gällande lagar och bestämmelser. Symantec rekommenderar att kunden alltid kontrollerar lokal lagstiftning före användande av IMSS samt ser till att kunden själv liksom alla kundens anställda då kunden använder IMSS är medvetna om och handlar i enlighet med alla förpliktelser i samband med gällande lagar och/eller förordningar rörande dataskydd och sekretess. I vissa länder kan det krävas att individuell personal ger sitt samtycke före uppfångning och loggning av snabbmeddelanden. ~~Som~~ ett minimum bör kunden, med rimlig och minimal anpassning till egna förhållanden, implementera Symantec standardmeddelande gällande IMSS för dem som använder kommunikationssystem som täcks av IMSS och som (i) anger att kommunikation som sänds över systemet kommer att loggas och kan komma att fångas upp, (ii) anger syftet med denna loggning och uppfångning, samt (iii) erhåller användarens tillåtelse att utföra denna loggning och uppfångning. Som en del av anpassningen av standardmeddelandet för IMSS till egna förhållanden får kunden översätta men bör inte i övrigt modifiera formuleringarna gällande punkt (i), (ii) och (iii) i föregående mening. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig på grund av användningen av IMSS. Kunden skall hålla Symantec skadeslöst beträffande alla anspråk från sina anställda, tredje parter och/eller statliga myndigheter i samband med Symantec uppfångning eller loggning av snabbmeddelanden eller kundens underlåtande att följa lagar och/eller bestämmelser.

7.3 **KUNDEN UPPMÄRKSAMMAS PÅ ATT ALLA SNABBMEDDELANDEN SOM PASSERAR GENOM IMSS KAN KOMMA ATT SKANNAS OCH LAGRAS PÅ HÅRDVARA SOM BEFINNER SIG I USA. DÄRFÖR SAMTYCKER KUNDEN TILL ATT FÖRE ELLER SAMTIDIGT SOM IMSS TAS I BRUK, VIDTA ALLA NÖDVÄNDIGA ÅTGÄRDER (I) FÖR ATT INFORMERA ALLA SINA ANSTÄLLDA, REPRESENTANTER OCH UNDERLEVERANTÖRER, LIKSOM TREDJE PARTER SOM ANVÄNDER KOMMUNIKATIONSSYSTEM SOM TÄCKS AV IMSS OM ATT ALL INFORMATION SOM PASSERAR GENOM IMSS, INKLUSIVE INDIVIDERS MÖJLIGA PERSONLIGA IDENTIFIERBARA INFORMATION, KAN KOMMA ATT BEARBETAS I USA; SAMT (II) FÖR ATT SKAFFA SIG DESSA ANSTÄLLDAS, REPRESENTANTERS, UNDERLEVERANTÖRERS OCH TREDJE PARTERS SAMTYCKE TILL DENNA BEARBETNING. VIDARE KAN ALL PERSONLIG INFORMATION SOM KUNDEN GÖR TILLGÄNGLIG FÖR SYMANTEC KOMMA ATT ÖVERFÖRAS TILL SYMANTEC NÄRSTÅENDE BOLAG OCH/ELLER UNDERLEVERANTÖRER SOM HANDLAR Å SYMANTEC VÄGNAR. DESSA NÄRSTÅENDE BOLAG ELLER UNDERLEVERANTÖRER KAN BEFINNA SIG I USA ELLER I ANDRA LÄNDER SOM EVENTUELLT HAR EN MINDRE OMFATTANDE DATASKYDDSLAGSTIFTNING ÄN DEN REGION DÄR KUNDEN BEFINNER SIG. I SÅDANA FALL KOMMER SYMANTEC ATT HA VIDTAGIT ÅTGÄRDER FÖR ATT INSAMLADE DATA SOM ÖVERFÖRS BEHANDLAS MED**

EN ADEKVAT NIVÅ AV SKYDD. KUNDEN SAMTYCKER TILL ATT VIDTA ALLA NÖDVÄNDIGA ÅTGÄRDER FÖR ATT (I) INFORMERA ALLA SINA ANSTÄLLDA, REPRESENTANTER OCH UNDERLEVERANTÖRER, LIKSOM TREDJE PARTER VARS PERSONLIGA INFORMATION KUNDEN GÖR TILLGÄNGLIG FÖR SYMANTEC OM ATT DERAS INFORMATION KAN KOMMA ATT BEARBETAS I DESSA LÄNDER; SAMT SKALL (II) ERHÅLLA DESSA ANSTÄLLDAS, REPRESENTANTERS, UNDERLEVERANTÖRERS OCH TREDJE PARTERS SAMTYCKE TILL DENNA BEARBETNING. SYMANTEC KAN INTE PÅTA SIG NÅGOT ANSVAR FÖR BROTT MOT GÄLLANDE LAGAR OCH FÖRORDNINGAR I SAMBAND MED DETTA.

7.4 **INGEN PROGRAMVARA ELLER TJÄNST KAN GARANTERA 100 % DETEKTERING OCH DÄRFÖR KAN SYMANTEC INTE PÅTA SIG NÅGOT ANSVAR FÖR SKADA ELLER FÖRLUST SOM DIREKT ELLER INDIREKT UPPSTÅR PÅ GRUND AV ATT IMSS MISSLYCKATS MED ATT DETEKTERA SKRÄPMEDDELANDEN, VIRUS NÄTFISKEANGREPP, SKADLIG KOD, BLOCKERADE URL-ADRESSER ELLER KONTROLLERAT INNEHÅLL ELLER FELAKTIGT IDENTIFIERAT ETT SNABBMEDDELANDE SOM INNEHÅLLANDE SKRÄPMEDDELANDEN, VIRUS, NÄTFISKEANGREPP, SKADLIG KOD, BLOCKERADE URL-ADRESSER ELLER KONTROLLERAT INNEHÅLL VILKET SENARE VISAR SIG INTE HA NÅGOT SÅDANT INNEHÅLL.** Vidare kontrollerar kunden helt konfigureringen av reglerna för innehållskontroll i IMSS och denna konfigurering kommer att avgöra funktionen hos IMSS.

Appendix 14 – Symantec Email Continuity Archive.cloud; Symantec Email Continuity Archive Lite.cloud

1. Översikt

1.1 Symantec Email Continuity Archive.cloud och Symantec Email Continuity Archive Lite.cloud är värdtjänster med lagringssystem för e-post som gör att kundens systemadministratörer kan lägga upp specifika riktlinjer för sparande av e-post för lagring av e-posthistorik för ett antal utsedda e-postlådor.

2. Kundens förpliktelser

2.1 Kunden ansvarar för följande åtgärder i samband med Tjänsten:
2.1.1 att tillhandahålla och upprätthålla nödvändig hårdvara och programvara (enligt beskrivning i formuläret gällande tillhandahållandet av Tjänsten)
2.1.2 att se till att utsedda tekniska resurser med administrativa rättigheter finns tillgängliga för tillhandahållandet av Tjänsten
2.1.3 att välja ut de användare som skall ha rätt att använda Tjänsten och den specifika lagringstiden för var och en av dessa användare
2.1.4 att dela ut och skydda åtkomstprivilegier beträffande arkivet via kundgränssnittet
2.1.5 att lägga upp och hantera riktlinjer för lagring i arkiv
2.1.6 att utföra sökning för att hämta arkiverade data.
2.2 Om kunden har underlåtit att inom trettio (30) dagar efter beställningen utföra någon av de åtgärder som krävs för tillhandahållande av Tjänsten har Symantec rätt att börja ta ut avgift för Tjänsten.

3. Funktioner

3.1 *Symantec Email Continuity Archive.cloud* inkluderar följande funktioner:
3.1.1 *Hämtning och lagring av e-post* – e-postmeddelanden hämtas då de levereras till kundens primära e-postmiljö och överförs till ett e-postarkiv för katalogisering och lagring. E-postmeddelandena krypteras och lagras inom Tjänsten. Riktlinjer för lagring av e-post kan ställas in så att användare kan välja när e-postmeddelanden skall tömmas från Tjänsten.
3.1.2 *Återställning* – ger möjlighet att återställa e-postmeddelanden från e-postarkivet tillbaka till kundens Exchange meddelandelagring.
3.1.3 *Elektronisk utredning* – ger kundens systemadministratörer möjlighet att utse vissa användare som ”granskare” och ge dem möjlighet att granska e-postmeddelanden i andra postlådor än sina egna för elektroniska utredningar och andra syften. Granskare kan skapa ett utredningsarkiv med resultaten av sökningar i användarnas postlådor. Utredningsarkivet kan exporteras till en enda postlåda.
3.1.4 *Windows-autentisering* – ger en kund som använder Microsoft Exchange 2000, Microsoft Exchange 2003 och/eller Microsoft Exchange 2007 möjlighet att utöka riktlinjer för säkerhet beträffande autentisering i samband med Microsoft Active Directory för användare av Tjänsten genom att möjliggöra för användare att logga in i Tjänsten med sitt lösenord för Active Directory.
3.1.5 *Slutanvändararkiv* – ger de användare för vilka vissa riktlinjer beträffande lagring gäller, möjlighet att från den egna postlådan komma åt personliga e-postarkiv via ett webbaserat gränssnitt. Kundens e-postadministratörer kan även specificera huruvida användare kan vidarebefordra e-postmeddelanden från sina personliga arkiv.
3.1.6 *Lagringshantering* – kundens systemadministratör kan definiera riktlinjer för lagringshantering som flyttar bilagor från kundens Exchange meddelandelagring till Tjänsten i syfte att minska lagringsbehoven.
3.2 *Symantec Email Continuity Archive Lite.cloud* inkluderar följande funktioner (enligt ovanstående beskrivning av var och en av tjänsterna):
3.2.1 *hämtning och lagring av e-post*
3.2.2 *återställning*
3.2.3 *elektronisk utredning*
3.2.4 *Windows-autentisering*
Symantec Email Continuity Archive Lite.cloud inkluderar inte slutanvändararkivering och lagringshantering. Kunden kan uppgradera för att inkludera slutanvändararkivering genom att abonnera på *Symantec Email Continuity Archive Lite.cloud End User Pack*.
3.3 *Import* – kunden kan mot en importavgift baserad på mängden data, importera äldre data till Tjänsten från PST-filer genom att ladda ner och använda ett importverktyg. Om den faktiska mängden äldre data överskrider den mängd dataimport som köpts förbehåller sig Symantec rätten att ta ut en avgift för denna ytterligare mängd data till den standardtaxa som gäller vid tillfället.

4. Symantec Email Continuity.cloud Storage Option

4.1 Kundens lagring skall mätas enligt den mängd obearbetad e-post som överförts till Tjänsten och för tillfället lagras.
4.2 Om kunden abonnerar på Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email & Web Safeguard.cloud, eller Symantec MessageLabs Ultimate Safeguard.cloud:
4.2.1 Paketet inkluderar maximalt 0,7 GB lagring av ny e-post per användare per år för EC och Symantec Email Continuity Archive.cloud tillsammans. Om kundens lagring av ny e-post överskrider denna tillåtna mängd lagring måste kunden köpa tillräckligt med lagringsutrymme för Tjänsten till Symantec vid tillfället aktuell taxa.
4.2.2 Paketet inkluderar ingen lagring av äldre data som importeras enligt Klausul 3.3 ovan och kunden måste köpa tillräckligt med lagringsutrymme för att uppfylla dessa behov till Symantec vid tillfället aktuell taxa.
4.3 Om kunden inte abonnerar på ett av paketen angivna i Klausul 4.2 ingår ingen lagring i priset per användare och kunden måste köpa tillräckligt med lagringsutrymme för Tjänsten till Symantec vid tillfället aktuell taxa.
4.4 Om kunden måste köpa ytterligare lagringsutrymme, kommer Symantec att sända ytterligare fakturor och/eller göra justeringar i efterföljande fakturor för att proportionerligt täcka avgifter för den ytterligare lagringen under kvarstående del av den aktuella faktureringsperioden.

5. Villkor och bestämmelser

5.1 INGEN E-POSTARKIVERINGSTJÄNST KAN GARANTERA 100 % KORREKTHET OCH DÄRFÖR KAN SYMANTEC, MED UNDANTAG FÖR VAD SOM UTTRYCKLIGEN ANGES I TJÄNSTENIVÅAVTALET, INTE PÅTA SIG NÅGOT ANSVAR FÖR SKADA ELLER FÖRLUST SOM DIREKT ELLER INDIREKT UPPSTÅR PÅ GRUND AV ATT TJÄNSTEN MISSLYCKATS MED ATT UTFÖRA SIN FUNKTION.
5.2 Symantec skall inte ansvara för oförmåga att tillhandahålla Tjänsten enligt beskrivningen häri om detta beror på (a) att Symantec inte kan tillämpa sina standardmetoder beträffande tillhandahållande och hantering av Tjänsten för kunden, (b) att kunden inte följer Symantec riktlinjer som anges i användarhandboken eller formuläret gällande tillhandahållande av Tjänsten, eller (c) att kunden inte aktiverar eller använder Tjänsten.
5.3 Symantec betonar att kunden helt kontrollerar konfigureringen av Tjänsten. Symantec rekommenderar att kunden skaffar sig riktlinjer för godtagbar datoranvändning (eller motsvarande). I vissa länder kan det krävas att individuell personal ger sitt samtycke. Symantec rekommenderar att kunden alltid kontrollerar lokal lagstiftning före användande av Tjänsten. Symantec kan inte påta sig något ansvar för civilt eller brottsligt ansvar som kunden kan komma att ådra sig genom användande av Tjänsten.
5.4 KUNDEN BEKRÄFTAR ATT MAN ÄR MEDVETEN OM OCH SAMTYCKER TILL ATT EN DEL AV ELLER HELA TJÄNSTEN KAN KOMMA ATT UTFÖRAS I USA OCH ATT KUNDEN ANSVARAR FÖR ATT SKAFFA SIG ALLA TILLSTÅND OCH GODKÄNNANDEN SOM KRÄVS FÖR ATT UTFÖRA ÖVERFÖRINGEN AV DATA. KUNDEN BEKRÄFTAR VIDARE OCH SAMTYCKER TILL ATT SYMANTEC INTE KAN PÅTA SIG NÅGOT ANSVAR FÖR BROTT MOT GÄLLANDE LAGAR OCH FÖRORDNINGAR I SAMBAND MED DETTA.
5.5 Kunden bekräftar att man är medveten om och samtycker till (i) att Symantec skanningstjänster (e-post AV, e-post AS, e-post IC och e-post CC) inte skannar alla e-postmeddelanden när de förs in i arkivet och (ii) att Symantec skanningstjänster (e-post AV, e-post AS, e-post IC och e-post CC) inte skannar e-postmeddelanden som släpps från arkivet för återinförande i användarens postlåda. Därför kan Symantec inte hållas ansvarigt för virus, skräppost, bilder eller olämpligt innehåll i sådana återinförda e-postmeddelanden och Servicenivåavtalet skall inte heller gälla sådana återinförda e-postmeddelanden.

5.6 Kunden är medveten om och accepterar att Symantec inte kan agera som tredjepartsnedladdare på något villkor i syfte att efterleva SEC:s bestämmelser.

6. Programvarulicens

6.1 Beviljande av licens

I den mån det är förenligt med villkoren och bestämmelserna i detta avtal, beviljar Symantec kunden icke överförbar licens utan ensamrätt att enbart för kundens egen interna affärsverksamhet installera och använda programvaran för Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud. (med ”programvara” menas var och en av Symantec programvaror för Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud i objektkodformat för vilken Symantec beviljar licens enligt villkoren i avtalet, inklusive men utan att inskränkas till nya upplagor eller uppdateringar i enlighet med vad som anges nedan.) Alla immateriella egendomsrätter beträffande programvaran är och skall förbli Symantec (och/eller dess leverantörers) egendom. Symantec beviljar licens för programvaran men säljer den inte. Kunden bekräftar att man är medveten om att programvaran och all relaterad information inklusive men utan att inskränkas till uppdateringar tillhör Symantec och dennes leverantörer. Kunden ansvarar fullständigt för varje användares följande av eller brott mot villkoren i detta avtal. Kunden skall omedelbart meddela Symantec vid eventuell otillåten användning eller brott mot villkoren för denna licens.

6.2. Restriktioner gällande kopiering och användning

Kunden får ladda ner och installera programvaran på följande villkor:

6.2.1. Kunden får inte ladda ner eller installera programvaran för fler än det antal slutanvändarlicenser kunden beviljats. (Med ”slutanvändare” menas den fysiska dator på vilken programvaran installeras.)

6.2.2. Kunden får kopiera programvaran i enlighet med vad som rimligen är nödvändigt för säkerhetskopiering, arkivering och katastrofåterställning. Tryckt dokumentation får enbart reproduceras av kunden för internt bruk. (Med ”dokumentation” menas Symantec användarhandböcker och/eller bruksanvisningar för användning av programvaran som medföljer den nedladdade programvaran).

6.2.3 Kunden får inte själv eller tillåta någon tredje part att: (i) utan föregående skriftligt tillstånd från Symantec demontera, ta isär eller bakåtkompilera programvaran utom i den mån som uttryckligen tillåts enligt gällande lag; (ii) avlägsna någon produktidentifikation eller meddelanden om egendomsrätter; (iii) hyra ut, låna ut eller använda programvaran för timesharing eller servicebyrå; (iv) modifiera, översätta, adaptera eller skapa härledda arbeten från programvaran; eller (v) i övrigt använda eller kopiera programvaran utom enligt vad som uttryckligen anges häri.

6.3. Överföring av rättigheter

Kunden får inte överföra, tilldela eller delegera programvarulicensen i detta avtal utan föregående skriftligt tillstånd från Symantec. Ingen sådan överföring, tilldelning eller delegering i strid med ovanstående skall vara giltig.

6.4. Begränsad garanti och ansvarsbefrielse

6.4.1 Symantec garanterat att programvaran vid nedladdningen i alla materiella avseenden skall motsvara Symantec aktuella dokumentation.

6.4.2 Ovanstående garanti skall inte gälla om: (i) Programvaran inte används i enlighet med detta avtal eller dokumentation; (ii) programvaran eller del därav har modifierats av någon annan än Symantec; eller (iii) ett fel i programvaran har orsakats av kundens utrustning eller en tredje parts programvara.

6.4.3 SYMANTEC GARANTERAR INTE ATT PROGRAMVARAN KOMMER ATT FUNGERA UTAN AVBROTT ELLER FEL. SYMANTEC AVSÄGER SIG UTTRYCKLIGEN ALLA UTTRYCKLIGA, UNDERFÖRSTÅDDA ELLER ÖVRIGA GARANTIER, INKLUSIVE MEN UTAN ATT INSKRÄNKAS TILL GARANTIER GÄLLANDE SÄLJBARHET, TILLFREDSSTÄLLANDE KVALITET ELLER LÄMPLIGHET FÖR VISST ÄNDAMÅL.

6.5. Uppsägning

Vid uppsägning av Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud skall alla kundens häri beviljade rättigheter beträffande rätten att använda programvaran omedelbart upphöra och kunden skall omedelbart till Symantec återlämna eller förstöra alla kopior av programvaran och dokumentationen.

7. Uppsägning av Tjänst och dataextrahering

7.1 Vid uppsägning av Tjänsten Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud ska Symantec ta bort Kundens data från arkivet.

7.2 Kunden kan när som helst före uppsägningen hämta sina data från arkivet.

Appendix 15 – Symantec MessageLabs Volume Mail Service (Massutskickshantering)

1. Om kunden abonnerar på massutskickshantering kan kunden sända och motta massutskick på följande villkor:

1.1 Massutskicket måste bestå enbart av bekräftade mottagare som valt att inkluderas på utskickslistan. Kunden måste på Symantec begäran och i enlighet med gällande lagstiftning lämna bevis på sådana bekräftelser.

1.2 Storleken på varje enskilt massutskick inklusive bilagor får inte överskrida 500 kilobyte.

1.3 ”Mottagarfältet” i varje enskilt massutskick får inte innehålla mer än femhundra (500) e-postadresser.

1.4 Kunden måste ha ett effektivt listhanteringssystem som omfattar snabb borttagning av ogiltiga e-postadresser och e-postadresser där abonnemang på utskicket sagts upp.

1.5 Kunden måste ha Symantec MessageLabs Email Anti-Virus.cloud för sin allmänna e-post.

1.6 Kundens massutskick måste komma från eller sändas till en separat domän till dennas allmänna e-post för att massutskicket därmed skall kunna riktas mot ett speciellt tillhandahållet kontrolltorn.

1.7 Standard utgående banderoll kommer att meddela mottagaren att massutskick har skannats för virus men det kommer inte att innehålla Symantec logo.

1.8 Om kunden abonnerar på Band F eller G i massutskickshantering i Avsnitt B ”Tjänst och avgifter” får kunden sända eller motta massutskick i grupper om högst 250 000 mottagare per dag.

1.9 Kunden bekräftar att man är medveten om och accepterar att sändande av massutskick troligtvis kommer att ha varierande inverkan på flödet av e-posttrafik. Sådan inverkan ligger utom Symantec kontroll och därför skall Servicenivåer som beskrivs i Servicenivåavtalet inte gälla för massutskick.

1.10 Om det vid något tillfälle förekommer att (i) kundens e-postsystem svartlistas, eller (ii) kunden medverkar till att Symantec system svartlistas på grund av utsändande av skräppost, eller (iii) kunden underlåter att uppfylla någon av de förpliktelser som anges i detta Appendix, kommer Symantec att informera kunden om detta och förbehåller sig rätten att omedelbart helt enligt eget gottfinnande undanhålla, avbryta eller säga upp en del av eller alla Tjänsterna.

1.11 Vart och ett av massutskickshanteringens band har en maximal kvot av tillåtna mottagare per månad. Dessa kvoter kan inte överföras eller ackumuleras och därmed kan oanvända mottagare inte föras över till efterföljande månader.

1.12 Kunden skall meddela Symantec om den faktiska användningen av massutskick vid något tillfälle överskrider antalet mottagare per månad som tillåts för kundens aktuella band och Symantec kommer att höja avgiften för motsvarande band i enlighet med Symantec vid tillfället aktuell taxa. Symantec kommer även att bevaka kundens faktiska användning av massutskick och om antalet mottagare per månad överskrider antalet som är tillåtet för kundens aktuella band, kommer Symantec att höja avgiften i enlighet med Symantec vid tillfället aktuell taxa. Symantec kommer helt enligt eget gottfinnande att sända ytterligare fakturor och/eller göra justeringar i efterföljande kvartalsfakturor för att täcka dessa höjda avgifter.

Appendix 16 – Symantec Enterprise Vault.cloud

1. Översikt

1.1 Symantec EV.cloud är samlingsnamnet för ett antal arkiveringstjänster (som alla beskrivs i punkterna 1.1 till 1.10 nedan) som kunden kan prenumerera på. Alla tjänster i Symantec EV.cloud-serien är kompatibla med godkända versioner av lokala Exchange-servrar och värdbaserade Exchange-tjänster.

1.2 Följande gäller för både Tjänsten Symantec Enterprise Vault Personal.cloud och Tjänsten Symantec Enterprise Vault Discovery.cloud:

1.2.1 Maximal storlek för e-postmeddelanden i Tjänsten Symantec Enterprise Vault Personal.cloud och Tjänsten Symantec Enterprise Vault Discovery.cloud är 50 MB.

1.2 Följande gäller för både Tjänsten Symantec Enterprise Vault Personal.cloud och Tjänsten Symantec Enterprise Vault Discovery.cloud:

1.2.3 Kunderna kan direkt besvara eller vidarebefordra meddelanden som finns i arkivet som skapats i någon av de båda Tjänsterna, vilket innebär att Kunderna regelbundet kan skapa backuper av filerna som kan användas om Kundens e-post slutar fungera.

1.2.4 Kunderna måste även fortsättningsvis göra backup på innehållet på sina e-postservrar lokalt. Om en Kund måste återskapa sin e-postserver bör Kunden göra det från lokalt hanterade data och inte från arkivet

1.1. Symantec Enterprise Vault Personal.cloud

Tjänsten Symantec Enterprise Vault Personal.cloud är Symantec Internetbaserade e-postarkiveringstjänst, utformad för att ge kundens individuella användare tillgång till sina egna personliga e-postarkiv direkt från Microsoft Outlook eller Outlook Web Access (där detta stöds) för att hitta och återställa förlorade eller raderade e-postmeddelanden.

1.1.1 Kundens inkommande och utgående e-postmeddelanden, med bilagor, lagras i ett sökbart arkiv på Internet (”Personal Archive” – personligt arkiv), där användare kan söka efter förlorade eller raderade e-postmeddelanden.

1.1.2 Användare har också tillgång till sitt personliga arkiv från Microsoft Outlook, Outlook Web Access (där detta stöds), IBM Lotus Notes, BlackBerry®-enheter och via en webbläsarbaserad och säker webbplats.

1.1.3 Användare kan söka i det personliga arkivet efter specifika e-postmeddelanden och bilagor på två olika sätt: Snabbsökning och avancerad sökning. Det avancerade sökalternativet ger användare möjlighet att anpassa sina sökningar enligt olika kriterier, som nyckelord i meddelanden, till, från, ämne, datum och typ av bilaga.

1.1.4 Om detta är aktiverat kan användare skriva, svara på och vidarebefordra meddelanden direkt från Symantec Enterprise Vault Personal.cloud, precis som i Outlook eller Notes.

1.1.5 Användare kan skapa anpassade sökningar, enligt olika kriterier (t ex datumintervall, avsändare eller typ av bilaga) och sedan spara dem så att användare kan köra dem igen vid behov.

1.1.6 Genom att flytta kundens e-post till det personliga arkivet och ta bort lokala arkiv återvinns plats på kundens delade diskar och e-postservrar.

1.1.7 Kundens personliga arkiv kan användas för att återställa gammal e-post om en dator kommer bort eller blir stulen.

1.1.8 Kunder kan lägga till PST-filer i Symantec Enterprise Vault Personal.cloud, där mappstrukturen kan behållas som den var första gången filerna lades till.

1.2. Symantec Enterprise Vault Discovery.cloud

Tjänsten Symantec Enterprise Vault Discovery.cloud är Symantec Internetbaserade e-postarkiveringstjänst avsedd för att påskynda begäranden om information i juridiskt syfte (e-discovery), upprätthålla användningspolicyer för e-post och lindra effekterna av dataförluster. Symantec Enterprise Vault Discovery.cloud hjälper kunder att bevara e-post i samband med domstolsprocesser/juridiska beslut och gör det enklare att skydda kommunikation mellan advokat och klient.

1.2.1 Symantec Enterprise Vault Discovery.cloud lagrar och indexerar e-postmeddelanden, bilagor och BlackBerry®-meddelanden (SMS, PIN-to-PIN, samtalsloggar) i ett centrallager på Internet.

1.2.2 Kunder kan lägga juridiska spärrar på specifik kommunikation (enligt sökvillkor) för att underlätta skydd av kunders personal eller automatiserade raderingsprinciper för att inte av misstag radera e-postmeddelanden relevanta för fallet. Administratörer och granskare kan flagga kommunikation mellan advokat och klient, som kan uteslutas från begäranden om e-posthämtning.

1.2.3 Symantec Enterprise Vault Discovery.cloud har en söklogg som lagrar aktiviteter för granskare, så att administratörer kan utföra lämpliga granskningar.

1.2.4 Administratörer har möjlighet att gruppera användare enligt anpassade villkor. Granskare kan sedan söka i dessa grupper.

1.2.5 Kunder kan söka igenom innehållet i arkiverade e-postmeddelanden och bilagor med olika sökvillkor, som till, från, datum, ämne, meddelandets brödtext, meddelandets bilagor och andra meddelandeegenskaper.

1.2.6 Kundens granskare kan effektivt navigera genom sökresultat, identifiera markerade ord och märka potentiellt skadliga e-postmeddelanden så att de enkelt kan hämtas och granskas ytterligare.

1.2.7 Kunder kan märka e-postmeddelanden som tillhör ett specifikt fall eller juridiskt ärende och sedan exportera e-postmeddelanden till en fallhanteringslösning från tredje man eller annat program för vidare granskning och analys.

1.2.8 Kundens granskare kan skapa och spara anpassade e-postsökningar enligt kundens e-postpolicyer och köra dem igen efter behov.

1.2.9 Kundens granskare kan skapa policymeddelanden som varnar dem när ett e-postmeddelande uppfyller villkoren i en ”sparad sökning” (t ex innehåller specifika ord eller fraser).

1.3. Symantec Enterprise Vault.cloud BlackBerry® Option

Tjänsten Symantec Enterprise Vault.cloud BlackBerry® Option är Symantec Internetbaserade tjänst som är utformad för att ge kundens individuella användare tillgång till och sökning i arkiverade e-postmeddelanden, bilagor, SMS, PIN-to-PIN-meddelanden och samtalsloggfiler via sina BlackBerry®-enheter. Användare kan söka upp och återställa förlorade eller raderade e-postmeddelanden och fortsätta använda sin BlackBerry®-enhet för att skriva, besvara och skicka meddelanden i realtid, även när kundens primära e-postserver är nere. Symantec Enterprise Vault.cloud BlackBerry® Option är en frivillig tilläggstjänst till tjänsten Symantec Enterprise Vault Personal.cloud.

1.3.1 Symantec Enterprise Vault.cloud BlackBerry® Option kan distribueras av administratörer till användare från en BES (BlackBerry® Enterprise Server) eller av användare via BlackBerry® Desktop Manager.

1.3.2 Användare kan logga in i sitt Symantec Enterprise Vault.cloud BlackBerry® Option genom att klicka på ikonen som visas på enhetens startskärm.

1.3.3 När användaren klickar på ett program visas en startbild i tre sekunder och sedan uppmanas användaren att ange sina inloggningsuppgifter.

1.3.4 Efter lyckad inloggning kommer användaren till startskärmen (dvs. listvyskärmen) i det personliga arkivet.

1.3.5 Från listvyskärmen (inkorgen) kan användare utföra ett antal olika åtgärder, t ex skriva nya meddelanden, besvara eller vidarebefordra meddelanden samt göra enkla eller avancerade sökningar.

1.3.6 Användare kan söka upp gamla, förlorade eller raderade e-postmeddelanden med enkla eller avancerade sökningar i alla meddelanden och samtalsloggfiler lagrade i det personliga arkivet och sedan återställa dessa meddelanden till sin inkorg.

1.3.7 Användaren kan ange text i sökrutan och trycka på sökikonen för att starta sökningen. Sökresultaten kan filtreras på ”Datum”, ”Från” och ”Till”.

1.3.8 Användaren kan använda sitt personliga arkiv för att skriva, besvara och skicka meddelanden även om kundens primära e-postplattform (t ex Microsoft Exchange) inte är tillgänglig.

1.4 AdvisorMail on Symantec.cloud™

Tjänsten AdvisorMail on Symantec.cloud™ (AdvisorMail) är Symantec Internetbaserade e-postarkiveringstjänst som strävar efter att påskynda e-postgranskningsprocessen som krävs enligt vissa tillsynskrav. Tjänsten AdvisorMail arkiverar e-postmeddelanden i ett enskilt arkiv. Meddelanden söks automatiskt igenom och flaggas enligt kundens specifika

policyer. Meddelanden eller bilagor som innehåller specifika nyckelord eller fraser kan sedan granskas av regelefterlevnadsexperter så att de uppfyller gällande policyer.
1.4.1 AdvisorMail samlar in skickade och mottagna meddelanden utan att kunden behöver göra något och skickar dem säkert till flera datacenter för bevarande, med TLS- eller VPN-kryptering.
1.4.2 AdvisorMails administrations- och rapportverktyg har lägen för granskning i förväg eller i efterhand, slumpmässiga tester, anpassningsbara regler för specifika domäner eller e-postadresser och sammanfattande rapporter.
1.4.3 AdvisorMail har två distinkta behörighetsnivåer för e-postgranskning: Administrator (fullständig behörighet) och Auditors (övervakningsbehörigheter för utvalda inkorgar).
1.4.4 AdvisorMail har ett antal verktyg för att strömlinjeforma övervakningsprocessen, bland annat automatisk flaggning av misstänkt e-post för granskning.
1.4.5 Kunder kan göra ett förval av startmapp (t ex granskat), datumintervall och meddelandevy (t ex List- eller Snippet-vy).
1.4.6 Kunder kan använda funktionen Next Click (nästa klick) för att hoppa till nästa överträdelse i e-postmeddelanden och bilagor med ett enda musklick medan högerklicksåtgärder gör att kunden kan välja kommandon genom att högerklicka med musen (t ex lägga till nyckelord i lexikonet).
1.4.7 AdvisorMails skiktade övervakningsfunktion gör att kunder kan skicka ut ett företagslexikon (lista över nyckelord och fraser som indikerar överträdelser) till fjärranslutna kontor med ett enskilt kommando.
1.4.8 Med AdvisorMails whitelist-editor kan kunder vitlista nyckelord och fraser som ofta finns i ansvarsfriskrivningar (t ex juridiska friskrivningar som finns i e-postmeddelandens sidfötter) för att minska antalet felaktigt rapporterade överträdelser.
1.4.9 Med AdvisorMail kan kunder lägga till e-postadresser, flytta användare till andra kontor, ändra regler och granska flera e-postmeddelanden.
1.4.10 AdvisorMails söklogg samlar in de granskningsaktiviteter som företagets granskare utför, vilket hjälper administratörer att uppfylla bestämmelser.
1.4.11 Granskare kan lägga till anteckningar i meddelanden vid behov.

1.5 AdvisorMail IM Option on Symantec.cloud™
Tjänsten AdvisorMail IM Option on Symantec.cloud™ är Symantec Internetbaserade arkiveringstjänst för snabbmeddelandeplattformar som stöds. Snabbmeddelanden samlas in, lagras och indexeras i AdvisorMail och övervakas sedan enligt kundens specifika policyer för att uppfylla bestämmelser. Snabbmeddelanden som innehåller angivna nyckelord eller fraser kan sedan granskas av regelefterlevnadsexperter så att de uppfyller gällande policyer. Tjänsten AdvisorMail IM Option on Symantec.cloud™ är en frivillig tillvalstjänst till AdvisorMail.
1.5.1 Tjänsten AdvisorMail IM Option on Symantec.cloud™ samverkar med snabbmeddelandenätverk och -klienter som stöds, vilka för tillfället omfattar offentliga snabbmeddelandenätverk, t ex AOL, MSN, Yahoo och Google Talk, privata nätverk (Reuters) och företagssnabbmeddelandeklienter (Microsoft Office Communicator, Lotus Sametime och Jabber).
1.5.2 Snabbmeddelanden indexeras och kopieras i sin ursprungliga form till media där de enkelt kan sökas igenom.
1.5.3 Kunden kan söka upp och hämta specifika snabbmeddelandekonversationer enligt olika sökvillkor, som datumintervall, nyckelord eller fraser samt avsändare/mottagare.
1.5.3 Det finns en loggningshistorik för granskningssyften.

1.6 AdvisorMail Bloomberg Option on Symantec.cloud™
Tjänsten AdvisorMail Bloomberg Option on Symantec.cloud™ är Symantec Internetbaserade arkiveringstjänst för Instant Bloomberg (snabbmeddelanden) och Bloomberg-e-post. Bloomberg-meddelanden samlas in, lagras och indexeras i AdvisorMail och övervakas sedan enligt kundens specifika policyer. Bloomberg-meddelanden som innehåller angivna nyckelord eller fraser kan sedan granskas av sakkunnig. Tjänsten AdvisorMail Bloomberg Option on Symantec.cloud™ är en frivillig tillvalstjänst till AdvisorMail.
1.6.1 Tjänsten AdvisorMail Bloomberg Option on Symantec.cloud™ samlar in Instant Bloomberg och Bloomberg-e-post till AdvisorMail i ursprungsformatet.
1.6.2 Bloomberg-meddelanden indexeras och kopieras i sin ursprungliga form till lagringsmedia där de enkelt kan sökas igenom.
1.6.3 Kunden kan söka upp och hämta specifika Bloomberg-meddelanden enligt olika sökvillkor, som datumintervall, nyckelord eller fraser samt avsändare/mottagare.
1.6.4 Det finns en loggningshistorik för granskningssyften.

1.7 Reserverat

1.8 Symantec Enterprise Vault.cloud Data Import Option
Symantec Enterprise Vault.cloud Data Import Option är SymantecInternetbaserade tjänst för migrering och införlivande av befintliga e-postdata i kundens arkivlager. Med importtjänsten kan kunden sedan söka i sitt e-postarkiv (t ex Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud eller AdvisorMail) med både införlivad e-post och nya e-postströmmar.
1.8.1 Symantec Enterprise Vault.cloud Data Import Option kräver att en kund levererar via S-FTP eller säkra bud-e-postdata i PST- eller EML-filformat.
1.8.2 Kunden kan extrahera data manuellt och tillhandahålla den i PST- eller EML-format eller använda professionella tjänster för automatiserad extrahering från arkiv som stöds.
1.8.3 Under kundens ledning tilldelar Symantec Enterprise Vault.cloud Data Import Option ägande för varje meddelande som har hittats. Meddelanden som inte direkt kan tilldelas en specifik individ arkiveras i en ”allround”-inkorg i e-postarkivet.
1.8.4 All migreringsaktivitet kan loggas och granskas för att ge integritet åt kundens e-postmeddelanden och behålla ”beviskedjan”.
1.8.5 Symantec Enterprise Vault.cloud Data Import Option kräver kundens aktiva deltagande för att planera, analysera och utföra en införlivandeplan med minimala driftstörningar.
1.8.6 Maximal storlek för e-postmeddelanden är 40 MB.

1.9 Symantec Enterprise Vault Mailbox Continuity.cloud
OM SYMANTEC INTE KAN UPPRÄTTA EN SMTP-ANSLUTNING TILL KUNDEN OMDIRIGERAS KUNDENS E-POSTMEDDELANDEN TILL TJÄNSTEN SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD FÖR KUNDENS RÄKNING (”KONTINUITETSHÄNDELSE”). KLARGÖRANDE: (I) OM KUNDENS BRANDVÄGG FUNGERAR SOM PROXY OCH SVARAR I E-POSTSERVERNS STÄLLE ELLER (II) OM KUNDENS E-POSTSERVER SVARAR PÅ NÅGOT SÄTT (INKLUSIVE, MEN INTE BEGRÄNSAT TILL, I FORM AV FELKODER) UTGÖR DETTA EN SMTP-ANSLUTNING OCH INTE EN KONTINUITETSHÄNDELSE.
1.9.1 Under en Kontinuitetshändelse kan Kundens enskilda Användare komma åt sin e-post via en särskild mapp i Microsoft Outlook® eller ett webbaserat användargränssnitt. Användaren kan (i) visa högst nittio (90) dagar gamla historiska e-postmeddelanden, inklusive nya e-postmeddelanden som skickats eller tagits emot under Kontinuitetshändelsen, (ii) skapa, besvara och vidarebefordra e-postmeddelanden och (iii) använda vanliga e-postverktyg som stavningskontroll, bilagor och formatering.
1.9.2 Om kunden enbart prenumererar på Symantec Enterprise Vault Mailbox Continuity.cloud lagras Kontinuitets-e-postmeddelanden i Tjänsten under en period på nittio (90) dagar. Om Kunden har köpt en ytterligare arkiveringstjänst enligt denna Bilaga 17 sparas Kontinuitets-e-postmeddelanden i Tjänsten under den lagringsperiod som kunden valt.
1.9.3 Kontinuitets-e-postmeddelanden levereras till Kundens primära e-postserver när servern åter börjar ta emot e-postmeddelande, med undantag för e-postmeddelanden som stått i kö under mer än sju (7) dagar. Sådana e-postmeddelanden måste Kunden istället hämta från kontinuitetsarkivet som beskrivs i punkt 1.9.2 ovan.
1.9.4 Tjänsten Symantec Enterprise Vault Mailbox Continuity.cloud använder en opportunistisk TLS-anslutning (Transport Layer Security), snarare än en forcerad, vid försök att leverera e-post. TLS är ett förbättrat säkerhetsprotokoll för att skydda/kryptera e-post under överföring över Internet.
ALLA KUNDER MED GRÄNSKRYPTERING OCH POLICYBASERAD KRYPTERING SOM ÄVEN VÄLJER TJÄNSTEN SYMANTEC ENTERPRISE VAULT MAILBOX

CONTINUITY.CLOUD ÄR INFÖRSTÅDDA MED OCH ACCEPTERAR ATT FÖRSÖK ATT UPPRÄTTA EN TLS-ANSLUTNING KOMMER ATT GÖRAS, MEN KANSKE INTE LYCKAS, OCH ATT E-POSTMEDDELANDEN DÄRFÖR EVENTUELLT INTE BLIR KRYPTERADE. KUNDEN ÄR ÄVEN INFÖRSTÅDD MED OCH ACCEPTERAR ATT DENNE INTE BÖR SKICKA ELLER TA EMOT KÄNSLIG INFORMATION VIA TJÄNSTEN EMAIL CONTINUITY.CLOUD (L) OCH ATT KUNDEN, OM DENNE ÄNDÅ VÄLJER ATT GÖRA DET, I SÅ FALL GÖR DET HELT PÅ EGEN RISK.

1.9.5 Förpliktelser i samband med Symantec Enterprise Vault Mailbox Continuity.cloud

Tjänsten Symantec Enterprise Vault Mailbox Continuity.cloud levererar bara e-post till en särskilt utsedd server per angiven domän och ”per användardirigering”. Kunden accepterar härmed denna aspekt av Tjänsten. Kunden accepterar att konfigurera Tjänsten Symantec Enterprise Vault Mailbox Continuity.cloud som en redundansleveransväg med ClientNet-gränssnittet och att informera Symantec om leveransplatsen (namn på e-postvärd eller IP-adress) efter domänen för sina e-postservrar när Tjänsten tas i bruk. Kunden är införstådd med och accepterar att denne har en fortlöpande förpliktelse att informera Symantec om eventuella ändringar av leveransplatsen så länge Tjänsten Symantec Enterprise Vault Mailbox Continuity.cloud nyttjas. Kunden är införstådd med och accepterar att Kundens underlåtenhet att genomföra sådana konfigurationer eller att ge Symantec sådan leveransinformation har negativ inverkan på funktionaliteten hos Tjänsten Symantec Enterprise Vault Mailbox Continuity.cloud.

1.10 Symantec Enterprise Vault.cloud Folder Sync Option

1.10.1 Symantec Enterprise Vault.cloud Folder Sync Option är en tilläggstjänst till Tjänsten Symantec Enterprise Vault Personal .cloud som beskrivs i avsnitt 1.1 i den här Bilagan. Med hjälp av Tjänsten Symantec Enterprise Vault.cloud Folder Sync Option kan en Kund visa e-postmeddelanden i Tjänsten Symantec Enterprise Vault Personal .cloud på i stort sett samma sätt som i e-poststrukturen i Kundens Outlook-mappar. Med Symantec Enterprise Vault.cloud Folder Sync Option kan en administratör synkronisera Kundens Outlook-mappstrukturer i Symantec Enterprise Vault Personal.cloud. När en Kund flyttar e-postmeddelanden mellan olika Outlook-mappar och skapar och flyttar Outlook-mappar replikerar synkroniseringstjänsten mapparnas struktur i Symantec Enterprise Vault Personal .cloud.

1.10.2 Tjänsten Symantec Enterprise Vault.cloud Folder Sync Option distribueras av Kundens administratörer via en lokal Tjänst som spårar flyttningar av mappar och objekt.

1.10.3 Efter den inledande synkroniseringen med Symantec Enterprise Vault.cloud Folder Sync Option utförs synkroniseringar stegvis mellan Outlook-mapparna och Symantec Enterprise Vault Personal .cloud.

1.10.4 Kunden kan välja att schemalägga synkroniseringarna i intervall uppdelade på timmar, dagar eller veckor.

1.10.5 Kunden kan filtrera resultaten från en arkivsökning genom att aktivera filterfunktionen och välja en mapp från listan som visas i sökfiltren.

Tjänsten stöds bara på plattformarna Microsoft Exchange Server 2003, 2007 och 2010.

2. Ytterligare villkor.

2.1 Symantec betonar att konfiguration och användning av tjänsten helt står under kundens kontroll. Symantec rekommenderar att kunden har en acceptabel datoranvändningspolicy (eller motsvarande). I vissa fall kan det vara nödvändigt att erhålla medgivande från enskilda anställda. Symantec råder kunden att alltid kontrollera den lokala lagstiftningen innan tjänsten distribueras. Symantec kan inte ta något ansvar för eventuellt civilrättsligt eller straffrättsligt ansvar som kunden kan ådra sig som ett resultat av användning av tjänsten.

2.2 **KUNDEN ÄR MEDVETEN OM OCH ACCEPTERAR ATT EN DEL AV ELLER HELA TJÄNSTEN KAN UTFÖRAS I USA OCH ATT KUNDEN ANSVARAR FÖR ATT ALLA NÖDVÄNDIGA MEDGIVANDEN OCH GODKÄNNANDEN FÖR ÖVERFÖRINGEN AV DATA ERHÅLLS. KUNDEN ÄR VIDARE MEDVETEN OM OCH ACCEPTERAR ATT SYMANTEC INTE KAN HÅLLAS ANSVARIGT FÖR NÅGRA MOTSVARANDE BROTT MOT TILLÄMPLIG LAGSTIFTNING ELLER FÖRESKRIFTER.**

2.3 Kunden är medveten om och accepterar att (i) Symantec genomsökningstjänster (Email AV, Email AS, Email IC och Email CC) inte söker igenom all e-post som ursprungligen kommer till arkivet och att (ii) Symantec genomsökningstjänster (Email AV, Email AS, Email IC och Email CC) inte söker igenom e-postmeddelanden som återställs från arkivet till användarens inkorg. Symantec kan därför inte heller hållas ansvarigt för virus, skräppost, bilder eller olämpligt innehåll som sådana återställda e-postmeddelanden kan innehålla, och vidare ska SLA (Service Level Agreement) inte heller gälla återställda e-postmeddelanden.

2.4 Enligt villkoren i detta avtal beviljar Symantec kunden en icke-exklusiv, ej överförbar rätt att installera och använda programvara som hör till nämnda tjänster där så är tillämpligt endast för kundens egen interna affärsverksamhet. Alla immateriella rättigheter till denna programvara tillhör och ska fortsättningsvis tillhöra Symantec (och/eller dess leverantörer). Sådan programvara säljs inte av Symantec, den licensieras. Kunden bekräftar att programvaran och all relaterad information, inklusive, men inte begränsat till, uppdateringar, tillhör Symantec och dess leverantörer. Kunden ska ansvara och vara fullständigt ersättningsskyldig för att varje användare följer villkoren i detta avtal. Kunden ska omedelbart meddela Symantec om obehörig användning eller brott mot villkoren i denna licens upptäcks.

2.5 Kunden är medveten om och accepterar att Symantec inte kan agera som tredjepartsnedladdare på något villkor i syfte att efterleva SEC:s bestämmelser.

2.6 Alla Kunddata som finns lagrade eller arkiverade enligt denna bilaga av Symantec eller dess leverantörer är uteslutande Kundens egendom (”Kunddata”), och ingenting häri ger Symantec eller dess leverantörer någon juridisk eller sedvanerättslig rätt eller äganderätt till Kunddata eller rätt att göra anspråk på dessa.

2.7 Kunddata ska lagras eller arkiveras under Prenumerationsperioden för Tjänsten och under en period på etthundratjugo (120) dagar efter dess upphörande, eller etthundratjugo (120) dagar efter uppsägningsdatumet om Tjänsten sägs upp innan Prenumerationsperioden löpt ut (benämns gemensamt ”Lagringsperiod efter uppsägning”). Under eller före Lagringsperioden efter uppsägning ska Kunden ge Symantec skriftliga instruktioner om att (i) kostnadsfritt radera Kundens data (såvida det inte är förbjudet i lag eller enligt domstolsbeslut) eller (ii) tillhandahålla en offlinekopia i PST-format via hårddiskmedia till Symantecs vid tidpunkten gällande priser och i en takt på inte mer än två (2) terabyte som levereras per månad tills alla Kunddata har returnerats till Kunden. Om Kunden underlåter att ge Symantec skriftliga instruktioner enligt ovan raderar Symantec Kunddata (såvida det inte är förbjudet i lag eller enligt domstolsbeslut) när Lagringsperioden efter uppsägning löper ut

Appendix 17 – Symantec Endpoint Protection.cloud

1. Översikt

1.1 För att kunden ska kunna använda Symantec Endpoint Protection.cloud måste vederbörande installera en agent på alla slutanvändardatorer och tilldela lämplig policy för användning av tjänsten. Hanteringsportalen för Symantec Endpoint Protection.cloud är en administratörsportal som används för hantering av datorer, policyer, meddelanden och rapporter (”Hanteringsportal”).

1.2 Kunden kan behöva ändra några grundläggande brandväggsinställningar för att agenten ska kunna kommunicera och fungera med Symantecs infrastruktur för molntjänster.

1.3 När tjänsten har konfigurerats i enlighet med punkterna 1.1 och 1.2 används Hanteringsportalen för att hantera agenten/agenterna.

1.4 Symantec ska publicera en lista över vilka operativsystem som stöds för agenten och vilka webbläsare som stöds för Hanteringsportalen. Kunden accepterar att Symantec med jämna mellanrum kan komma att uppdatera och ändra den här listan utan föregående meddelande.

1.5 Agenten på datorn:

1.5.1 ska skydda datorn mot skadlig kod utifrån kända metoder för tjänsten.

1.5.2 ska blockera kända angrepp med skadlig kod från nätverket på datorn.

1.5.3 ska syfta till att tillhandahålla funktioner för skydd mot nätfiske (s k phishing) för de webbläsare som stöds och blockera nätfiskeangrepp.

2. Hanteringsportal

2.1. På Hanteringsportalen kan kunden konfigurera sin egen policybaserade säkerhet för agenterna.

2.2 Kunden ansvarar för att implementera de konfigurationsalternativ som ligger i linje med kundens policy för godtagbar datoranvändning (eller motsvarande) via Hanteringsportalen. Policyer konfigureras för datorgruppen.

2.3 Ändringar i policyn visas omedelbart i Hanteringsportalen och batchas ned till agenterna. Tillämplig policyinställning för en viss agent kan visas på Hanteringsportalen eller på den agent som körs på slutanvändardatorn.

3. Loggar och rapporter

3.1 Alla loggar och rapporter som rapporteras av agenten lagras och kan visas på och hämtas från Hanteringsportalen i tolv (12) månader. Därefter tas loggarna bort.

4. Meddelanden

4.1 Kunden kan konfigurera Symantec Endpoint Protection.cloud Service så att ett automatiskt meddelande skickas till konfigurerade e-postmottagare utifrån regeln för meddelanden, som kan konfigureras i Hanteringsportalen.

4.2 Kunden kan skapa, ta bort och anpassa meddelanden med Hanteringsportalen.

5. Support

5.1 Supporten omfattar:

5.1.1 genomgång av Hanteringsportalen inklusive en tjänstbeskrivning och en session med frågor och svar. (Detta omfattar inte hjälp med att konfigurera policyer och analyser av policyernas effektivitet.)

5.1.2 administratörsvägledning

5.1.3. användarvägledning.

6. Dataintegritet för Symantec Endpoint Protection.cloud

6.1 Kunden accepterar att loggar kan innehålla personligt identifierbar information och att loggningen och övervakningen av loggar därför kan utgöra behandling av personuppgifter. Kunden accepterar vidare att Symantec Endpoint Protection.cloud är en tjänst som kan konfigureras och att kunden är ensam ansvarig för att konfigurera Symantec Endpoint Protection.cloud i enlighet med kundens policy för godtagbar datoranvändning (eller motsvarande) och alla tillämpliga lagar och regler. Symantec rekommenderar följaktligen att kunden alltid kontrollerar lokal lagstiftning innan vederbörande distribuerar Symantec Endpoint Protection.cloud och alltid ser till att kunden, och alla dess anställda, är medvetna om och efterlever alla skyldigheter som åligger dem med avseende på lagar och/eller bestämmelser om dataskydd och integritet i samband med kundens användning av Symantec Endpoint Protection.cloud. I vissa länder kan det vara nödvändigt att inhämta medgivande från var och en i personalen innan övervakning och loggning kan ske. Kunden skall installera agenter för Symantec Endpoint Protection.cloud med skälig och minimal anpassning. Kunden samtycker till att enheter som täcks av Symantec Endpoint Protection.cloud (i) loggar information med avseende på driften av Symantec Endpoint Protection.cloud Service, (ii) att denna information överförs till Symantec i syfte att ge hanteringsinformation och rapportera till Kunden och (iii) Kunden tillåter att sådan loggning och överföring sker.

7. Konfiguration

7.1 Om Kunden har köpt Tjänsten via en Symantec-återförsäljare ger Kunden uttryckligen Symantec-återförsäljaren befogenhet att (i) ändra Tjänstens konfiguration i syfte att optimera dess funktionalitet och (ii) skicka in supportärenden för Kundens räkning.

Appendix 18 – Symantec MessageLabs Smart Connect.cloud Service ("Smart Connect.cloud")

1. **Översikt**

1.1. När roamingagenten är installerad och nödvändiga konfigurationer gjorts dirigeras förfrågningar om webbsidor och bilagor elektroniskt via användaragenten till Symantec MessageLabs Web v2 URL.cloud Service ("Web v2 URL") där de granskas digitalt med Symantec MessageLabs Web v2 Protect.cloud Service ("Web v2 Protect").

2. **Beskrivning av tjänst**

2.1. När användaren ansluter till Internet i länder där tjänsterna tillhandahålls dirigeras Kundens externa HTTP- och FTP-over-HTTP-förfrågningar direkt genom Web v2 URL- och Web v2 Protect-tjänsterna, inklusive alla bilagor, makron och körbara filer.

3. **Konfiguration**

3.1. Konfigurationsinställningarna som krävs för att dirigera extern webbtrafik till roamingagentprogramvaran, samt för att vidarebefordra utgående trafik till Web v2 URL- och Web v2 Protect-tjänsterna, skapas och underhålls av Kunden och är beroende av Kundens tekniska infrastruktur. Kunden måste installera en PAC-fil på användarens dator så att webbläsaren riktas mot Symantec roamingagent när den startas. En PAC-filmall kan hämtas på ClientNet och modifieras av Kunden. Kunden ska se till att intern HTTP/FTP-over-HTTP-trafik (t ex företagets intranät) inte dirigeras till roamingagentprogramvaran.

3.2. Åtkomsten till Web v2 URL och Web v2 Protect är begränsad till auktoriserade system som innehåller en giltig version av roamingagentprogramvaran, samt till auktoriserade användare som aktiveras för de här tjänsterna i ClientNet. Roamingprogramagenten och information om auktoriserad användare används för att identifiera Kunden och dynamiskt välja kundspecifika inställningar.

3.3. Policyregler för Web v2 URL-tjänsten och genomsökning av innehåll för Web v2 Protect-tjänsten är samma vare sig en användare använder roamingagenttjänsten eller om användaren ansluter via ett konfigurerat nät, dvs ett företags-LAN.

3.4. Kunden godkänner att roamingagenten levereras med Symantec standardinställningar, vilka bland annat innefattar rimliga åtgärder för att dirigera användarens webbtrafik till en "optimal" åtkomstpunkt för tjänstinfrastruktur. Dirigeringen baseras på en tolkning av roaminganvändarens plats baserad på IP-adressen och på användning av en geolokaliseringsdatabas från tredje part för att identifiera det land som användaren sannolikt ansluter från. Symantec dirigerar användare efter landsbeteckning till den förmodat bästa tjänståtkomstpunkten för det specificerade landet. Detta görs oberoende av eventuella bedömningar av den sannolika prestandan hos enskilda användares anslutningar, och endast för de länder som Symantec anser vara kapabla att hålla en acceptabel tjänstnivå.

Kunden accepterar att Symantec inte kan tillhandahålla Web v2 URL- och Web v2 Protect-tjänsterna i länder som inte anses kapabla att hålla en acceptabel tjänstnivå. I situationer där användaren bedöms befinna sig i ett land där tjänster inte kan tillhandahållas kommer roamingagenten att gå till "fail open"-läge, så att användaren kan ansluta till Internet utan de förmåner som Symantec ger i länder där dess tjänster kan tillhandahållas.

KUNDEN GODKÄNNER ATT ANVÄNDARENS WEBBTRAFIK KAN DIRIGERAS TILL INFRASTRUKTUR PÅ EN GEOGRAFISK PLATS UTANFÖR EU I SYFTE ATT BEARBETAS ENLIGT DENNA KLAUSUL 3.4. KUNDEN ANSVARAR FÖR ATT INHÄMTA ALLA MEDGIVANDEN OCH GODKÄNNANDEN SOM KRÄVS FÖR ÖVERFÖRING AV SÅDAN WEBBTRAFIK. KUNDEN ÄR VIDARE MEDVETEN OM OCH ACCEPTERAR ATT SYMANTEC INTE PÅTAR SIG NÅGOT ANSVAR FÖR EVENTUELLA BROTT MOT TILLÄMPLIGA LAGAR ELLER FÖRESKRIFTER I DETTA HÄNSEENDE.

4. **Ytterligare exportvillkor för Smart Connect.cloud**

4.1 Kund eller Partner får inte, och får inte tillåta tredje part att, sälja, återförsälja, exportera, reexportera, överföra, sprida, distribuera, avhända, röja eller på annat sätt hantera reglerad teknik, direkt eller indirekt, till något av följande länder: Afghanistan, Angola, Armenien, Azerbajdzjan, Bosnien och Herzegovina, Burundi, Demokratiska republiken Kongo, Eritrea, Etiopien, Iran, Irak, Kina, Kuba, Liberia, Libyen, Myanmar, Nigeria, Nordkorea, Rwanda, Sierra Leone, Somalia, Sudan, Syrien, Tanzania, Uganda och Zimbabwe.

4.2 Kund eller partner får inte överföra webbroamingagenten till något annat företag, eller till någon enskild person som inte är anställd hos kund eller partner, med följande undantag: (i) Kund eller Partner kan överföra till eller aktivera hämtningen av webbroamingagenten via sina oberoende underleverantörer för användning å Kundens eller Partnerns vägnar, och/eller (ii) Kund eller Partner kan överföra till eller aktivera hämtningen av webbroamingagenten via sina oberoende slutkunder som de återförsäljer Symantec Service till, förutsatt att Kund eller Partner gör dem medvetna om förpliktelserna i den här klausulen.

Bilaga 3
Servicenivåavtal

1. Definitioner

1.1. Följande ord skall i samband med detta Servicenivåavtal ha följande innebörd:

Med "**kreditbegäran**" menas det meddelande som kunden via e-post till **support.cloud@symantec.com** med ämnesrubriken "Kreditbegäran" måste sända till Symantec (om inte annat meddelats av Symantec).

Med "**utsedd torngrupp**" menas två (2) eller flera torn fördelade över minst två (2) platser och som utsetts att tillhandahålla Tjänsten för kunden.

Med "falskt positiv e-postvirusvarning" menas att ett legitimt e-postmeddelande felaktigt markeras/fångas upp som innehållande virus.

Med "**e-posttjänster**" menas e-post AV, e-post AS, e-post IC, e-post CC, policybaserad kryptering och gränskryptering.

Med "känt virus" menas ett virus som vid tillfället då innehållet mottas av Symantec: (i) redan i en (1) timme funnits offentligt tillgängligt för konfigurering genom en av de tredje parters kommersiella skanners som används av Symantec; eller (ii) finns med på den "Wild List" som publiceras på http://www.wildlist.org och har identifierats som "In the wild" av minst två deltagare i Wild List-programmet.

Med "Symantec Spårare" menas ett av Symantec verktyg som mäter tillgång till Tjänsten och svarstid.

Med "**månadsavgift**" menas månadsavgiften för berörda Tjänster enligt beskrivning i avtalet.

Med "**servicenivå**" menas var och en av de parametrar för Tjänsten som beskrivs i detta Servicenivåavtal.

Med "falskt negativ uppfångning av skräppost" menas ett skräppostmeddelande som inte identifierats som skräppost.

Med "falskt positiv uppfångning av skräppost" menas att ett legitimt e-postmeddelande felaktigt markeras/fångas upp som skräppost.

Med "rekommenderade skräppostinställningar" menas Symantec bästa metoder för riktlinjer beträffande konfigurering för e-post AS.

Med "torn" menas att antal belastningsbalanserade servrar.

Med "**webbtjänster**" menas Web v2 Protect och Web v2 URL tillsammans.

2. Allmänt

2.1. Om kunden skulle anse sig vara berättigad till ersättning i enlighet med detta Servicenivåavtal måste kunden sända in en kreditbegäran inom tio (10) arbetsdagar efter slutet av ifrågavarande kalendermånad. Kunden bekräftar att man är medveten om att loggar enbart behålls i ett visst antal dagar och att kreditbegäran som lämnas in efter att denna tidsbegränsning löpt ut kommer att bedömas som ogiltig.

2.2. All kreditbegäran kommer att verifieras av Symantec i enlighet med gällande bestämmelser i detta Servicenivåavtal.

2.3. Detta Servicenivåavtal kommer inte att gälla: (i) under perioder av planerat underhåll eller nödfallsunderhåll, perioder utan tillgång som beror på force majeure eller kundens eller en tredje parts handlingar eller underlåtanden; (ii) under perioder då Symantec avbrutit tjänsten i enlighet med villkor i avtalet; (iii) då kunden brutit mot avtalet (inklusive, men inte begränsat till, om kunden har några fakturor som förfallit till betalning); (iv) gällande e-postmeddelanden som inte har passerat igenom tjänsten (inklusive, men inte begränsat till, om kunden inte har låst sin egen router för att skicka all e-posttrafik till Symantec); eller (v) avseende ingående eller utgående e-postmeddelanden som först skickades till Symantec och innehöll mer än 500 mottagare per SMTP-session.

2.4. Ersättningarna som beskrivs i detta Servicenivåavtal skall utgöra kundens hela och enda ersättning beträffande kontrakt, brott (inklusive men utan att inskränkas till vårdslöshet) eller i övrig gällande Servicenivå.

2.5. Symantec maximala ackumulerade förpliktelser enligt detta Servicenivåavtal under en viss kalendermånad skall inte överstiga etthundra procent (100 %) av den månadsavgift som kunden är skyldig att betala för berörd(a) Tjänst(er).

2.6 Om den berörda Tjänsten är en del av ett ej uppdelningsbart tjänstepaket:

a) skall månadsavgift för berörd Tjänst vid uträkning av kredit för Tjänsten räknas ut som den totala månadsavgiften för det ej uppdelningsbara tjänstepaketet, dividerat med antalet Tjänster som ingår i paketet

b) skall den reviderade avgiften för det ej uppdelningsbara tjänstepaketet, om kunden säger upp den berörda Tjänsten i enlighet med detta Servicenivåavtal, räknas ut som den ursprungliga totala månadsavgiften för det ej uppdelningsbara tjänstepaketet, dividerat med det ursprungliga antalet Tjänster som ingår i paketet, multiplicerat med antalet kvarstående Tjänster som ingår i paketet.

2.7 Servicenivåerna för e-posttjänsterna gäller inte för kundens EC och därför skall tjänstenivåerna för e-posttjänsterna i Klausul 3 till och med 5 nedan inte gälla under de perioder då EC är aktiverade.

3. 100 % Tillgång till Tjänsten

3.1 Denna tillgång till Tjänsten enligt Servicenivå skall enbart gälla om kunden använder en eller flera av e-posttjänsterna eller webbtjänsterna.

3.2 I samband med e-posttjänsterna avser denna tillgång till Tjänsten enligt Servicenivå, förmågan att etablera en SMTP-session via port 25 i utsedd torngrupp uppmätt av Symantec Spårare. Denna Servicenivå skall enbart gälla om utsedd torngrupp kan:

3.2.1 ta emot kundens inkommande e-post för kundens domän 24 timmar om dygnet, 7 dagar i veckan

3.2.2 ta emot kundens utgående e-post från en korrekt konfigurerad SMTP-värd tillhörande kunden å kundens domäns/domäners vägnar 24 timmar om dygnet, 7 dagar i veckan.

3.3 I samband med webbtjänsterna avser denna tillgång till Tjänsten gällande Servicenivå webbtjänsternas förmåga att ta emot kundens utgående webbegäran och skall enbart gälla om kundens värd, portalenheter eller proxy(er) är korrekt konfigurerade 24 timmar om dygnet, 7 dagar i veckan.

3.4 Om tillgång till Tjänsten under en kalendermånad är mindre än hundra procent (100 %) kan kunden ha rätt till följande procentbaserade krediter:

Procent tillgång till Tjänsten per kalendermånad	Procent kredit av månadsavgift
< 100 % men > = 99 %	25
< 99 % men > = 98,0 %	50
< 98,0 %	100 samt uppsägning av berörd Tjänst enligt kundens eget gottfinnande

3.5 Om tillgång till Tjänsten under en kalendermånad faller under nittioåtta procent (98 %) skall kunden ha rätt att säga upp den berörda Tjänsten med omedelbar verkan och återfå den del av avgifterna som i förskott betalats för den berörda Tjänsten gällande perioden efter uppsägningen.

4. 100 % leverans av e-post

4.1 Denna Servicenivå gällande leverans av e-post kommer enbart att gälla om kunden använder en eller flera av e-posttjänsterna.

4.2 Symantec kommer att leverera 100 % av all e-post som sänds till eller från kunden, på följande villkor:

4.2.1 E-posten måste mottas av kundens utsedda torngrupp

4.2.2 E-post får inte innehålla virus, skräppost eller annat innehåll som gör att den blockeras av e-posttjänsterna.

4.3 Förutsatt att detta stämmer överens med bestämmelserna i Klausul 4.1 och 4.2 ovan, har kunden om Symantec misslyckas med att leverera ett e-postmeddelande till eller från kunden och kunden inte brutit mot några villkor i avtalet, rätt att säga upp e-posttjänsterna efter meddelande trettio (30) dagar i förväg.

5. E-postsvarstid på 60 sekunder

5.1. Förutsatt att detta stämmer överens med bestämmelserna i Klausul 5.2, kommer denna Servicenivå gällande e-postsvarstid enbart att gälla om kunden använder en eller flera av e-posttjänsterna.

5.2. Denna Servicenivå gällande e-postsvarstid skall **inte** gälla policybaserad kryptering.

5.3. Om den genomsnittliga tiden tur och retur för e-postmeddelanden som sänds var 5 minuter till och från vart och ett av e-posttjänsttornen inom kundens utsedda torngrupp (uppmätt av

Symantec Spårare) under en kalendermånad överskrider de fördröjningar som anges i nedanstående tabell, kan kunden lämna in en kreditbegäran i enlighet med nedanstående tabell:

Genomsnittlig tid tur och retur för 100 % av mätningarna (i minuter och sekunder)	Procent kredit av månadsavgift
> 1 min men < = 1 min 30 sek	25
> 1 min 30 sek men < = 2 min	50
> 2 min men < = 2 min 30 sek	75
> 2 min 30 sek	100

5.4. Denna Servicenivå gällande e-postsvarstid kommer inte att gälla:
5.4.1. Om kunden inte har försett Symantec med en lista över specifika e-postadresser som skall erhålla Tjänsten (”godkännandelistan”) och kunden drabbas av ett angrepp med nekande av Tjänst
5.4.2. Under perioder av fördröjningar som orsakas av e-postrundgång från/till kundens system.

6. Webbsvarstid på 0,1 sekunder

6.1 Denna Servicenivå gällande webbsvarstid kommer enbart att gälla om kunden använder en eller flera av webbtjänsterna.
6.2. Om genomsnittlig skanningstid för webbinnehåll, uppmätt från det ögonblick då Symantec mottar innehållet till det ögonblick då Symantec försöker överföra innehållet, räknat över en kalendermånad, understiger 100 % enligt nedanstående tabell, kan kunden lämna in en kreditbegäran:

Genomsnittlig andel webbinnehåll som skannas inom 100 millisekunder	Procent kredit av månadsavgift
< 100 % men > = 99 %	25
< 99 % men > = 98 %	50
< 98 % men > = 97 %	75
< 97 %	100 samt uppsägning av berörd Tjänst enligt kundens eget gottfinnande

6.3 Denna Servicenivå gällande webbsvarstid skall enbart gälla objekt på upp till 1 MB.

7. 0,0003 % falskt positiv uppfångning av skräppost

7.1. Denna Servicenivå gällande falskt positiv uppfångning av skräppost gäller enbart om kunden använder skräppostskydd och tillämpar Symantec rekommenderade skräppostinställningar.
7.2. Om genomsnittligt antal falskt positiv uppfångning av skräppost överstiger 0,0003 % av hela kundens e-posttrafik under en kalendermånad, kan kunden ha rätt till kredit enligt nedanstående tabell:

Andel falskt positiv uppfångning av skräppost under kalendermånaden	Procent kredit av månadsavgift
> 0,0003 men < = 0,003	25
> 0,003 men < = 0,03	50
> 0,03 men < = 0,3	75
> 0,3	100

7.3. I samband med denna Servicenivå kommer följande e-postmeddelanden inte att anses utgöra falskt positiv uppfångning av skräppost:
7.3.1. E-postmeddelanden som inte är legitimt affärsmässiga
7.3.2. E-postmeddelanden med över 20 mottagare
7.3.3. E-post där avsändaren ingår på kundens lista över blockerade avsändare inklusive men utan att inskränkas till sådana som angetts av individuella användare om kunden har aktiverat inställning på användarnivå
7.3.4. E-postmeddelanden som sänds från en komprometterad maskin
7.3.5. E-postmeddelanden som sänds från en maskin som finns på en tredje parts lista över blockerade avsändare
7.3.6. E-postmeddelanden som har sänts till över 20 mottagare (under en enda manöver eller en serie av manövrar) och har minst 80 % samma innehåll.

8. 99 % uppfångning av skräppost

8.1. Denna Servicenivå gällande uppfångning av skräppost gäller enbart om kunden använder skräppostskydd och tillämpar de rekommenderade skräppostinställningarna. Bestämmelserna i denna Klausul 8 motsvarar antalet falska negativa uppfångningar av skräppost som uppmäts under en månad.
8.2. Kunden kan ha rätt till kredit i enlighet med nedanstående tabell:

Andel uppfångning av skräppost under kalendermånaden	Procent kredit av månadsavgift
> 98 % – < = 99 %	25
> 97 % – < = 98 %	50
> 96 % – < = 97 %	75
< 96 %	100

8.3. Denna Servicenivå gällande uppfångning av skräppost kommer inte att gälla om e-postmeddelandet inte sändes till en legitim adress.
8.4 En lägre andel uppfångning av skräppost på 95 % skall gälla för e-postmeddelanden som innehåller asiatiska skrivtecken. Om denna andel uppfångning av skräppost faller under 95 % skall kunden ha rätt till 25 % kredit på månadsavgiften. Om andelen uppfångning av skräppost faller under 90 % skall kunden ha rätt till 100 % kredit på månadsavgiften.

9. Begäran om kredit gällande skräppostskydd

9.1. För att bli berättigad till kredit enligt Klausul 7 och 8 måste kunden sända in misstänkta falskt positivt eller falskt negativt uppfångade e-postmeddelanden till **support.cloud@symantec.com** inom 5 dagar efter att e-postmeddelandet mottagits. Symantec kommer att undersöka och bekräfta huruvida e-postmeddelandet utgör en falskt positiv eller falskt negativ uppfångning av skräppost och kommer att registrera resultatet av undersökningen. Om kunden i slutet av kalendermånaden anser att antalet bekräftade falskt positiva och falskt negativa uppfångningar av skräppost berättigar till kredit enligt ovanstående tabell, måste kunden sända in en kreditbegäran till Symantec i enlighet med Klausul 2.1 i denna Bilaga.

10. 100 % Virusskydd för e-post

10.1. Denna Servicenivå för virusskydd för e-post gäller enbart om kunden använder virusskyddet för e-post.
10.2. Om kundens system skulle infekteras av ett eller flera virus under en kalendermånad och Symantec informerats om detta genom ett inloggat och verifierat supportsamtal under vilket det bekräftats att viruset har överförts till kunden via e-post AV, har kunden rätt att fakturera Symantec för likvida skador motsvarande det lägre av 100 % av den vid tillfället kvarstående månadsavgiften eller 5 000 brittiska pund/10 000 euro (beroende på vilken valuta kunden faktureras i). Ersättningen som beskrivs i denna Klausul 10.2 skall utgöra den enda och hela ersättningen beträffande kontrakt, brott (inklusive men utan att inskränkas till vårdslöshet) eller i övrigt gällande eventuell infektion med virus som överförts till kunden eller en tredje part via Tjänsten. För att undvika tveksamhet, skall ersättningen beskriven i denna Klausul 10.2 inte gälla i fall av medveten självinfektion.
10.3. Kundens system skall anses som infekterade om ett virus i ett e-postmeddelande som mottagits via e-post AV har aktiverats i kundens system, antingen automatiskt eller genom manuellt ingrepp.
10.4. Om Symantec detekterar men inte stoppar ett virusinfekterat e-postmeddelande, kommer Symantec snarast att meddela kunden och förse kunden med tillräcklig information för att denna skall kunna radera det virusinfekterade e-postmeddelandet. Om ett sådant meddelande resulterar i att infektion förhindras skall ersättningen beskriven i Klausul 10.2 ovan inte gälla. Om kunden underlåter att snabbt agera efter att ha erhållit sådan information kommer detta att ogiltiggöra bestämmelserna om Servicenivå i Klausul 10.2 ovan.
10.5. E-post AV kommer att skanna så mycket som möjligt av e-posten och dess bilagor. Det kan hända att det inte är möjligt att skanna bilagor med innehåll som direkt kontrolleras av avsändaren (t.ex. lösenordsskyddade och/eller krypterade bilagor). Sådana e-postmeddelanden och/eller bilagor utesluts från bestämmelserna om Servicenivå i Klausul 10.2 ovan.
10.6. Denna Servicenivå gällande virusskydd gäller inte i samband med virus som medvetet har släppts ut av kunden.

11. 0,0001 % a e-postvirusvarningar

11.1 Denna Servicenivå för falskt positiv e-postvirusvarning gäller enbart om kunden använder virusskydd för e-post.
11.2. Om falskt positiva e-postvirusvarningar under en kalendermånad överstiger 0,0003 % av kundens totala e-posttrafik, kan kunden ha rätt till kredit enligt nedanstående tabell:

Andel falskt positiva e-postvirusvarningar under kalendermånaden	Procent kredit av månadsavgift
> 0,0001 men < = 0,001	25
> 0,001 men < = 0,01	50
> 0,01 men < = 0,1	75
> 0,1	100

12. 100 % skydd mot kända webbvirus

12.1 Denna Servicenivå för skydd mot webbvirus gäller enbart om kunden använder Web v2 Protect.

12.2. Om kundens system skulle infekteras av ett eller flera kända virus under en kalendermånad och Symantec informerats om detta genom ett inloggat och verifierat supportsamtal där information om den URL-adress från vilket objektet laddades ner lämnats och vid vilket det bekräftats att viruset har överförts till kunden via Web v2 Protect, har kunden rätt att fakturera Symantec för likvida skador motsvarande det lägre av 100 % av den vid tillfället kvarstående månadsavgiften eller 5 000 brittiska pund/10 000 euro (beroende på vilken valuta kunden faktureras i). Ersättningarna som beskrivs i denna Klausul 12.2 skall utgöra kundens enda och hela ersättning beträffande kontrakt, brott (inklusive men utan att inskränkas till vårdslöshet) eller i övrig gällande infektion av känt virus som överförts till kunden eller en tredje part via Web v2 Protect. För att undvika tveksamhet, skall ersättningen beskriven i denna Klausul 12.2 inte gälla i fall av medveten självinfektion eller medveten nedladdning av känd skadlig kod utförd av kunden.

12.3 Kundens system skall anses som infekterade om ett känt virus i en webbtransaktion som mottagits via Web v2 Protect har aktiverats i kundens system, antingen automatiskt eller genom manuellt ingrepp.

12.4 Om Symantec detekterar men inte stoppar ett känt virus som utgör en del av en webbtransaktion via Symantec Web v2 Protect, kommer Symantec snarast att meddela kunden och förse kunden med tillräcklig information för att denna skall kunna identifiera och radera objektet. Om ett sådant meddelande resulterar i att infektion förhindras skall ersättningen beskriven i Klausul 12.2 ovan inte gälla. Om kunden underlåter att snabbt agera efter att ha erhållit sådan information kommer detta att ogiltiggöra bestämmelserna om Servicenivå i Klausul 12.2 ovan.

12.5. Web v2 Protect kommer att skanna så mycket som möjligt av alla nedladdningar från webben. Det kan hända att det inte går att skanna vissa objekt som i kommunikationssyfte är inkapslade eller i tunnel via de stödda webbprotokollen (HTTP och FTP över HTTP); som överförs via HTTPS; som komprimerats eller modifierats från sin ursprungliga form för distribution; som skyddas av produktlicens; eller som utgör nedladdning, uppdatering eller innehåll som direkt kontrolleras av avsändaren (t.ex. om de är lösenordsskyddade och/eller krypterade). Sådana objekt och/eller bilagor utesluts från bestämmelserna om Servicenivå i Klausul 12.2 ovan.

13. Teknisk support och felrespons 24 timmar om dygnet, 7 dagar i veckan

13.1 Symantec kommer tjugofyra (24) timmar per dygn och sju (7) dagar i veckan att:

a) erbjuda kunden teknisk support när det gäller problem med Tjänsten

b) samarbeta med kunden för att lösa sådana problem.

13.2 Om en kund kontaktar Symantec via telefon eller e-post för att påtala ett problem eller fel, eller begära information om en tjänst, kommer prioritering och respons att ske enligt nedanstående tabell:

Prioritet	Definition	Responsmålsättning
Högsta	Förlust av Tjänst	95 % besvarade inom 2 timmar
Stor	Delvis förlust eller nedsättning av Tjänst	85 % besvarade inom 4 timmar
Låg	Begäran om information om potentiell påverkan av Tjänst eller frånvaro av Tjänst	75 % besvarade inom 8 timmar

13.3 Fel som uppstår på grund av kundens handlingar eller som kräver åtgärder från andra tjänsteföretag ligger utanför Symantec kontroll och utesluts därför från responstiderna i Klausul 13.2 ovan.

13.4 I den mån detta överensstämmer med Klausul 13.3, kan kunder som anser att en fördröjning av Symantec respons på en begäran förekommit (som överskrider de parametrar som beskrivs i Klausul 13.2 ovan) ha rätt till kredit. Begäran om kredit måste ange händelsens tid, datum och loggnummer. Om kunden är berättigad kommer en kredit att beviljas enligt nedanstående tabell:

Prioritet	Misslyckande att uppfylla målsättning	Procent kredit av månadsavgift
Högsta	Mer än en gång under en kalendermånad	15
Stor	Mer än två gånger under en kalendermånad	10
Låg	Mer än tre gånger under en kalendermånad	5

14. E-postarkivering (P)

14.1 Bestämmelserna i Klausul 14 skall gälla enbart för Tjänsten e-postarkivering (P).

14.1 Tillgång till e-postarkivering (P)

14.1.1 E-postarkivering (P) skall finnas tillgänglig 99,9 % av tiden under varje kalendermånad, med undantag för perioder av planerat underhåll och nödfallsunderhåll. I detta sammanhang avser ”tillgänglig” att Symantec värdinfrastruktur finns redo att ta emot och arkivera e-post. Vid uträkning av otillgänglighet kommer följande kriterier att användas: a) mätningen kommer att utföras av Symantec bevakningssystem (kunden kan få dessa mätningsresultat på skriftlig begäran); b) bevakning kommer att ske i intervaller om 5 minuter och två efter varandra följande misslyckanden skall anses utgöra ett avbrott; c) enbart Symantec värdinfrastruktur kommer att mätas och mätningarna utesluter all otillgänglighet som beror på att en enhet för e-postarkivering inte fungerar eller avbrott hos ett av kundens nätverk eller Internet.

14.1.2 För varje en (1) procents eller del av procents otillgänglighet utöver tillgänglighetsmålsättningen i denna Klausul 14.1 på 99,9 % under den ifrågavarande kalendermånaden, skall kunden ha rätt till en kredit motsvarande tio procent (10 %) av den månadsavgift som kunden är skyldig att betala till Symantec i samband med e-postarkivering (P), upp till 100 % av månadsavgiften för e-postarkivering (P) för en viss kalendermånad. Kunden får helt enligt eget gottfinnande säga upp e-postarkivering (P) om denna tillgänglighet vid något tillfälle understiger nittio procent (90 %) under en viss kalendermånad.

14.2 Servicenivå gällande enhet för e-postarkivering (P)

14.2.1 Om en enhet för e-postarkivering upphör att fungera under garantiperioden på grund av en av de orsaker som täcks av Symantec begränsade garanti (enligt definition i dokumentation som medföljer enheten för e-postarkivering), skall Symantec utan någon kostnad för kunden, samt i samarbete med kunden, inom fyra (4) timmar efter att kunden under normal arbetstid meddelat Symantec om problemet samt inom åtta (8) timmar efter att kunden meddelat Symantec om problemet utanför normal arbetstid, utföra felsökning på enheten för e-postarkivering (vilket kan kräva VPN-åtkomst till enheten för e-postarkivering). Inom tjugo (20) timmar av normal arbetstid efter att Symantec informerats om problemet, skall Symantec göra något av följande:

14.2.1.1 meddela kunden om att enheten för e-postarkivering fungera korrekt och problemet inte beror på enheten för e-postarkivering eller programvaran

14.2.1.2 reparera enheten för e-postarkivering med hjälp av hårdvara och/eller programvara

14.2.1.3 meddela kunden om att enheten för e-postarkivering måste bytas ut

14.2.1.4 återbetala månadsavgiften för e-postarkivering (P) gällande den aktuella avtalstiden och säga upp e-postarkivering (P), om Symantec inte kan reparera eller ersätta enheten för e-postarkivering.

14.2.2 Om Symantec enligt Klausul 14.2.1.3 ovan skulle erfordras tillhandahålla en ny enhet för e-postarkivering som ersättning för den gamla, skall Symantec inom fyrtioåtta (48) timmar av normal arbetstid från och med det tillfälle då Symantec meddelar kunden om att en ny enhet för e-postarkivering krävs, leverera denna nya enhet för e-postarkivering till kundens lokal.

14.2.3 Om Symantec enligt Klausul 14.2.1.2 och 14.2.1.3 ovan skulle erfordras reparera eller byta ut enheten för e-postarkivering eller programvaran men inte gör det inom den tids ram som anges i Klausul 14.2.1 och 14.2.2, skall Symantec till kunden återbetala fem procent (5 %) av månadsavgiften för e-postarkivering (P) för var dag av dröjsmål utanför denna tidsram.

14.2.4 Föregående villkor i denna Klausul 14.2 skall vara kundens enda och hela ersättning i samband med defekt eller brott mot garanti gällande enheten för e-postarkivering.

15. EC

15.1 Bestämmelserna i denna Klausul 15 skall gälla enbart för EC.

15.1.1 EC skall finnas tillgänglig 99,9 % av tiden under varje kalendermånad, med undantag för perioder av planerat underhåll och nödfallsunderhåll. I detta sammanhang avser ”tillgänglig” att Symantec värdinfrastruktur finns redo att synkronisera nyckelsystem och Användarinformation. Vid uträkning av otillgänglighet kommer följande kriterier att användas: a) mätningen kommer att utföras av Symantec bevakningssystem (kunden kan få dessa mätningsresultat på skriftlig begäran); b) enbart Symantec värdinfrastruktur kommer att mätas och mätningarna utesluter all otillgänglighet som beror på

avbrott hos ett av kundens nätverk eller en tredje parts tjänst, liksom problem med DNS som ligger utanför Symantec direkta kontroll.
15.1.2 För varje en (1) procents eller del av procents otillgänglighet utöver tillgänglighetsmålsättningen i denna Klausul 15.1 på 99,9 % under den ifrågavarande kalendermånaden, skall kunden ha rätt till en kredit motsvarande tio procent (10 %) av den månadsavgift som kunden är skyldig att betala till Symantec för EC, upp till 100 % av månadsavgiften för EC för en viss kalendermånad. Kunden får helt enligt eget gottfinnande säga upp EC om denna tillgänglighet vid något tillfälle understiger nittio procent (90 %) under en viss kalendermånad.

16. Symantec Email Continuity Archive.cloud; Symantec Email Continuity Archive Lite.cloud

16.1 Bestämmelserna i denna Klausul 16 skall enbart gälla för Symantec Email Continuity Archive.cloud och Symantec Email Continuity Archive Lite.cloud.
16.1.1 Symantec Email Continuity Archive.cloud och Symantec Email Continuity Archive Lite.cloud skall finnas tillgängliga 99,95 % av tiden under varje kalendermånad. Tillgängligheten skall räknas ut genom att det totala antalet timmar som Symantec Email Continuity Archive.cloud och Symantec Email Continuity Archive Lite.cloud (enligt vad som är tillämpligt) under den ifrågavarande kalendermånaden var otillgänglig (med undantag för perioder av avbrott hos kundens nätverk, underhåll, liksom problem med DNS som ligger utanför Symantec direkta kontroll) divideras med det totala antalet timmar som Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud (enligt vad som är tillämpligt) enligt planen skulle ha varit tillgängligt.
16.1.2 För varje en (1) procents eller del av procents otillgänglighet utöver tillgänglighetsmålsättningen i denna Klausul 16 på 99,95 % under den ifrågavarande kalendermånaden, skall kunden ha rätt till en kredit motsvarande den avgift som kunden betalt till Symantec för Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud (enligt vad som är tillämpligt) för en dag av Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud.

17. Symantec EV.cloud

17.1 Symantec ska tillhandahålla 99,99 % servertillgänglighet för Symantec EV.cloud. Om servertillgängligheten för en hel kalendermånad faller under 99,99 % kommer Symantec att kreditera kunden enligt nedan:

Servertillgänglighet	Kreditering som andel av månadsavgift
99,9 % till 99,98 %	5 % av månadsavgiften
98,0 % till 99,8 %	10 % av månadsavgiften
95,0 % till 97,9 %	15 % av månadsavgiften
90,0 % till 94,9 %	25 % av månadsavgiften
89,9 % eller mindre	2,5 % av månadsavgiften för varje 1 % av förlorad tillgänglighet upp till maximalt 100 % av månadsavgiften

17.2 Begäran om kreditering måste innehålla datum och klockslag då servern inte varit tillgänglig. Symantec kommer att jämföra informationen om serverns otillgänglighet från kunden med de övervakningsdata för servertillgänglighet som Symantec samlar in. En kreditering ska göras om servern inte är tillgänglig i den utsträckning som visas i tabellen i punkt 17.1 ovan. Den kreditering som beskrivs i punkt 17.2 ska vara kundens enda ersättning i samband med att en server inte är tillgänglig. En server som inte är tillgänglig i samband med underhåll tas inte med i beräkningarna av servertillgänglighet.

18. Symantec Endpoint Protection.cloud

18.1 Bestämmelserna i den här punkten 18 skall endast gälla för Symantec Endpoint Protection.cloud Service.
18.1.1 Symantec Endpoint Protection.cloud kommer att vara tillgänglig 100 procent av varje kalendermånad, utom vid schemalagt underhåll och akut underhåll. Med ”Tillgänglig” avses i detta fall då Symantec molnbaserade infrastruktur kan synkronisera policyinformation. Följande kriterier gäller för mätning av när tjänsten inte är tillgänglig: a) mätningen utförs av Symantec övervakningssystem (mätningen kan efter skriftlig begäran tillhandahållas kunden), b) endast Symantec värdbaserade infrastruktur kommer att mätas och mätningen tar inte hänsyn till tillgänglighetsproblem som beror på nätverksfel hos kunden, fel hos tredje man eller ett DNS-problem som faller utanför Symantec direkta kontroll.
18.1.2 För varje (1) procent eller del därav av tillgänglighetsbortfall utanför tillgänglighetsmålsättningen på 99,9 procent, enligt den här punkten 18.1 under ifrågavarande kalendermånad, är kunden berättigad till en kreditering motsvarande tio (10) procent av månadsavgiften till Symantec för Symantec Endpoint Protection.cloud Service, och maximalt 100 procent av månadsavgiften för Symantec Endpoint Protection.cloud Service under varje kalendermånad. Kunden kan säga upp Symantec Endpoint Protection.cloud Service efter eget gottfinnande om tillgängligheten någon gång faller under nittio (90) procent under en kalendermånad.
18.1.3 Den kreditering som beskrivs i punkt 18.1.2 ska vara Kundens enda ersättning i samband med att en server inte är tillgänglig för Tjänsten Symantec Endpoint Protection.cloud. Servicenivåerna i avsnitten 3.1, 3.4 och 11.1 i det här Servicenivåavtalet gäller inte för Tjänsten Symantec Endpoint Protection.cloud.