Vedlegg 1
Generell Tjeneste Beskrivelse

TJENESTE BESKRIVELSER OG/ELLER SERVICE LEVEL ("SLAs") SOM ER ANGITT I VEDLEGG 2 OG 3 NEDENFOR OG IKKE ER BESTILT AV KUNDEN I DEL B AV AVTALEN, SKAL IKKE GJELDE FOR KUNDEN.

1. Definisjoner

Uttrykkene med stor forbokstav nedenfor, skal ha den betydning som er angitt i denne Avtale:

"Volum Email"	betyr en gruppe på mer en fem tusen (5000) e-mail beskjeder med i det vesentlige samme innhold sendt eller mottatt ved en arbeidsoperasjon eller en serie relaterte arbeidsoperasjoner;
"Email"	betyr enhver SMTP-beskjed sendt eller mottatt via Tjenesten;
"Non-Severable Tjeneste Bundle"	betyr et knippe Tjenester som angitt i Del B "Tjenester og Pris" i Avtalen og klausul 7 nedenfor, som er underlagt bestemmelsene i Klausul 3.6 i Avtalen;
"Medlem"	betyr Kunden og organisasjoner som Kunden lager et kryptert nettverk med ved å anvende Boundary Krypterings Tjenesten;
"Normale Arbeidstimer"	betyr mellom 8:30am og 5:30pm UK tid, mandag til fredag bortsett fra offisielle fridager i Storbritannia;
"Åpen Proxy"	betyr en proxy server konfigurert til å tillate ukjente eller uautoriserte tredjeparter tilgang, lagring eller videresending DNS, web sider eller annen data;
"Åpen Relay"	betyr en Email server konfigurert til å motta Email fra en ukjent eller uautorisert tredjepart og videresende Emailen til en eller flere mottakere som ikke er brukere av Emailsystemet som Emailserveren er knyttet til. Open Relay kan også betegnes som "Spam relay" eller "offentlig relay";
"Spam"	Betyr uoppfordret kommersiell kommunikasjon;
"Tårn"	betyr en gruppe av balansert belastning Emailservere;
"Bruker"	betyr en person, mailboks eller maskin som bruker Tjenesten; og
"Virus"	betyr en del av en programkode, inkludert et selvgenererende element, vanligvis skjult som noe annet som er designet på en måte som kan angripe andre computersystemer.

2. Introduksjon

2.1 Symantec er en administrert tjenesteleverandør som spesialiserer seg på Internett-nivå Email, Instant Messaging og Websikkerhet.

2.2 Tjenestene administreres på tjuefire (24) timer/dag, sju (7) dager/uke basis fra Symantecs Globale Operasjons Senter. Tjenestene overvåkes for hardwaretilgjengelighet, tjenestekapasitet og nettverk resurs utnytting.

2.3. Hvis Symantec ikke er i stand til å levere Email til en Kundes mailserver, skal Symantec lagre Kundens innkommende Email for inntil sju (7) dager i påvente av levering.

2.4. Tjenesten er tilgjengelig til Kunder som er fast tilknyttet Internett med en fast IP-adresse. Den kan ikke tilbys Kunder med systemer som er tilknyttet Internett via dial-up eller ISDN linjer eller som har dynamisk allokert IP-adresse.

2.5. For alle innkommende Email vil IP-omdømmet til avsender bli forsikret. Email som stammer fra en beryktet kilde (som for eksempel en "spammer") vil bli forsinket for å minimere innvirkningen på nettverkskapasiteten.

2.6 Kunden skal konfigurere e-postserverne til å begrense antallet mottakere per utgående SMTP-tilkobling til mindre enn 500. En mottaker er en individuell e-postadresse. En e-postgruppe kan inneholde én eller flere mottakere. Hvis en inngående eller utgående e-postmelding inkluderer mer enn 500 mottakere i en SMTP-tilkobling, vil Symantec behandle de første 500 mottakerne og sende en SMTP-svarkode til den sendende e-postserveren for å kreve at den sender e-postmeldingen på nytt til de resterende mottakerne.

3. Planlagt Vedlikehold

3.1. I anledning denne Klausul 3, skal "Planlagt Vedlikehold" bety perioder med vedlikehold hvor Kunden har fått sju (7) dagers forhåndsvarsel fra Symantec og som kan forårsake avbrudd i Tjenesten på grunn av ikke tilgjengelig Tårn. Planlagt Vedlikehold skal ikke utgjøre mer enn åtte (8) timer pr. kalendermåned og skal ikke finne sted mellom kl 0800 og 1800 (i tidssonen hvor Tårnet er lokalisert).

3.2. Når det er mulig, skal Planlagt Vedlikehold utføres uten at Tjenesten blir berørt. Dette vil normalt oppnås ved å utføre Planlagt Vedlikehold i perioder med forventet lav trafikk og ved å utføre Planlagt Vedlikehold på deler av nettverket om gangen. I løpet av perioder med Planlagt Vedlikehold kan trafikken bli omdirigert rundt på deler av nettverket hvor det ikke pågår vedlikehold for å minimere avbrudd av Tjenesten.

3.3. I tillfelle vedlikehold blir nødvendig på grunn av uforutsette hendelser, og det er sannsynlig at slikt vedlikehold vil påvirke Tjenesten, skal Symantec bestrebe seg etter å informere berørte parter og vil legge ut en beskjed på ClientNet så snart som mulig og senest innen en (1) time etter påbegynt uforutsett vedlikehold.

4. ClientNet

4.1. En integrert del av Tjenesten er Symantecs internettbaserte konfigurasjon, administrasjons- og rapporteringsverktøy benevnt ClientNet. ClientNet gjøres tilgjengelig for Kunden gjennom en passordbeskyttet innlogging, og hvor passordet ikke må deles med utenforstående tredjepart. ClientNet gir mulighet for Kunden til å se data og statistikk for deres bruk av Tjenesten og tilbyr en rekke konfigurasjons- og administrasjonsmuligheter.

5. Teknisk Support

5.1. Symantec vil på tjuefire (24) timer/dag, sju (7) dager/uke basis:

a) besørge Teknisk Support til Kunden i anledning problemer med Tjenesten; og
b) samarbeide med Kunden for å løse slike problemer.

6. Kundetjenester

6.1. Symantec vil besørge kundetjenester i Normale Arbeidstimer for:

a) å motta og behandle bestillinger knyttet til Tjenesten;
b) å motta og behandle anmodninger om tilpassing av de operasjonelle aspekter ved Tjenesten; og
c) besvare forespørsler knyttet til fakturering.

6.2. Med mindre annet er avtalt i angjeldende Tjeneste Beskrivelse, på kvittering for ferdig utfylt og komplett bestilling av Tjenesten eller en Tjeneste Endringsordre, vil Symantec Global Anskaffelse Team bestrebe seg på å besørge Tjenesten innen tjuesju (27) Normale Arbeidstimer, forutsatt at alle faser av teknisk due diligence er gjennomført.

7. Non-Severable Tjeneste Bundle

7.1 Non-Severable Tjeneste Bundle (dersom valgt i Del B "Tjenester og Pris" i Avtalen) omfatter mulighet for følgende Tjenester:

Navn på nåværende ikke-delbare tjenestepakke	Constituent Services (Legacy Constituent Service)	Navn på eldre ikke-delbare tjenestepakke
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 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 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 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. Navn på eldre tjenester

8.1 For kunder som kjøpte tjenester før 11. juni 2011, henvises det til andre tjenestenavn i dette dokumentet enn de opprinnelige navnene til de eldre tjenestene. Diagrammet nedenfor viser tilsvarende eldre begreper for den nye nomenklaturen, slik at kundene kan se hvilke deler av dokumentet som gjelder for tjenester de kjøpte under den forrige nomenklaturen.

Gammelt navn på tjenesten	Nåværende navn på tjenesten
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	AdvisorMail IM Option on Symantec.cloud™

MessageLabs Email Premium Archiving.cloud for IM (L)	
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

Vedlegg 2
Tjeneste Beskrivelse

Bilag 1 – Symantec MessageLabs Email Anti-Virus.cloud Tjeneste

1. Oversikt

1.1. Symantec MessageLabs Email Anti-Virus.cloud Tjeneste ("Email AV") er Symantecs Internett-nivå Email Virus skanning Tjeneste. Kundens innkommende og utgående Email inklusiv alle vedlegg, macros eller maskinkommandoer blir dirigert gjennom Email AV ved DNS og MX registreringsinnstillinger.

1.2 Email og vedlegg blir skannet av flere industriledende anti-virus produkter inklusiv Symantecs egen heuristisk skanner, Skeptic™.

2. Varsling Beskjeder

2.1 Hvis Kundens innkommende Email eller vedlegg finnes å inneholde Virus, vil et automatisk varsel, dersom valgt av Kunden, bli sendt til avsender og tilsiktet mottaker i form av en notifikasjon. I anledning Kundens utgående Email kan man velge at Tjenesten bare varsler avsender og ikke tilsiktet mottaker. Brukeridentifikasjon kan også sendes til en Email-administrator i begge tilfeller. Den infiserte Emailen videresendes til en sikker server i påvente av automatisk destruksjon etter sju (7) dager, forutsatt at det ikke er sendt som en massemailvirus, i hvilket tilfelle det vil bli slettet umiddelbart.

2.2 I tilfelle et alvorlig utbrudd av et nytt Virus, vil en varselmelding bli lagt ut på ClientNet.

3. Konfigurering

3.1 ClientNet kan anvendes tilpassing av fane-tekst, håndtering av Virus-infisert Email og bestemme maksimum Emailstørrelse.

4. Håndtering av Virus-Infisert Email

4.1 Hvor en virusinfisert Email viser seg å kunne frigjøres, kan den frigjøres fra sikker server ved å anvende ClientNet. Emailen vil bli sluppet enten til første adresse på original mottagerliste eller til en spesifisert adresse som allerede er notifisert til Symantec, og logget av Symantec i ClientNet (Merk: disse adresser kan være gruppe Email navn eller kortnavn, og i så tilfelle vil Emailen kunne bli frigjort til alle adressatene i gruppen eller til kortnavn). Alternativt kan den virusinfiserte Emailen bli frigjort til en alternativ adresse av Symantec etter mottak av relevant "Frigi Authorization Form". Symantec vil bare kunne handle på basis av anmodninger godkjent av Kunden vedrørende videresending av Virusinfisert Email. Symantec vil ikke returnere Virusinfisert Email til avsender. Symantec vil ikke videresende Virus-infisert Email til tredjeparter. Visse Virusinfiserte Emailer sendt til Kunden vil ikke kunne frigjøres på grunn av at de inneholder et Virus som er særlig infisert eller ødeleggende. Disse vil bli vist på ClientNet som ikke frigjørbare.

5. Email AV Vilkår og Betingelser

5.1 Hvis anmodet om å frigjøre en virusinfisert Email, vil Symantec frigjøre den innen åtte (8) Normale Arbeidstimer etter mottak av korrekt autorisert anmodning om frigjøring.

Bilag 2 – Symantec MessageLabs Email Image Control.cloud Tjeneste

1. Oversikt

1.1 Symantec MessageLabs Email Image Control.cloud tjeneste ("Email IC") er Symantecs Internett-nivå Email bilde kontroll tjeneste som er designet for å oppdage innhold av pornografiske bilder i bildefiler.

2. Tjeneste Beskrivelse

2.1 Kundens innkommende og utgående Email kan skannes ved å bruke en Image Composition Analysis (ICA) for pornografiske bilder som finnes i bildefiler vedlagt Email.

2.2 Hvis Kundens innkommende eller utgående Email mistenkes å inneholde et pornografisk bilde, vil en av flere mulige handlinger bli foretatt avhengig av konfigureringsalternativene som er valgt av Kunden.

3. Konfigurering

3.1 Når Symantec har mottatt ferdig utfylt og akseptert bestilling, vil Symantec gjøre Email IC tilgjengelig for Kunden. Oppstart Email IC vil bli gjort tilgjengelig for hvert av Kundens domener. Kunden er ansvarlig for å tilpasse konfigureringen for Email IC for hvert domene iht Kundens behov. Kunden konfigurerer Email IC ved å anvende ClientNet.

3.2 Det er mulig å spesifisere sensitivitetsnivå for ICA-filteret, som styrer muligheten for oppdagelse av uønskede bilder. Sensitiviteten kan settes til High, Medium eller Low. Disse innstillinger er svært subjektive, men til veiledning. Flere bilder vil bli mistenkt å være pornografisk ved High sensitivitet og færre bilder vil bli mistenkt å være pornografisk ved Low sensitivitet.

3.3 Muligheter er tilgjengelig for å definere handlinger som skal skje ved oppdagelse av bilder som mistenkes å være pornografiske. Disse omfatter mulighet for å innstille uavhengig for innkommende og utgående Email og bør innstilles iht Kundens eksisterende og akseptabel computer bruker policy (eller tilsvarende). Disse muligheter er:

3.3.1logge mistenkelig Email (besørger statistikk som er tilgjengelig via ClientNet);

3.3.2 tagge mistenkelig Email på headeren (kun for innkommende Email);

3.3.3 kopiere mistenkelig Email til en forhåndsdefinert Email adresse;

3.3.4 omdirigere mistenkelig Email til en forhåndsdefinert Email adresse;

3.3.5 slette mistenkelig Email;

3.3.6 tagge mistenkelig Email i subjekt (overskrift) feltet.

3.4. Når Kunden har identifisert klarerte Email-avsendere eller mottakere for administrering av Email IC, vil Email fra slike avsendere og mottakere ikke bli skannet av Email IC.

4. Rapportering

4.1 Hvis valgt alternativ i Klausul 3.3 i dette Bilag er å omdirigere eller slette Email som inneholder et bilde som mistenkes å være pornografisk, kan en automatisk varsling bli sendt avsender. Hvis Emailen er innkommende til Kunden, kan en automatisk varsling også sendes påtenkt mottaker. Slik automatisk varsling kan aktiveres og deaktiveres av Kunden gjennom ClientNet.

4.2 Rapportering av effektivitet for Email IC besørges gjennom ClientNet hvor statstikk er tilgjengelig for antall innkommende og utgående Email som mistenkes å inneholde pornografiske bilder. ClientNet kan konfigureres til å lage rapporter som sendes pr. Email til Kunden på ukentlig eller månedlig basis.

5. Email IC Vilkår og Betingelser

5.1 INTET SOFTWARE FOR PÅVISNING AV PORNOGRAFISK BILDE KAN GARANTERE 100 % OPPDAGELSESRATE, OG PÅ DENNE BAKGRUNN KAN SYMANTEC IKKE AKSEPTERE ANSVAR FOR SKADE ELLER TAP SOM DIREKTE ELLER INDIREKTE RESULTERER I EN FEIL VED TJENESTEN KNYTTET TIL MANGLENDE PÅVISNING AV PORNOGRAFISK BILDE ELLER FOR FEILAKTIG Å HA PÅVIST ET BILDE SOM PORNOGRAFISK, TIL TROSS FOR AT DET SENERE VISER SEG Å IKKE VÆRE DET.

5.2 Det kan være umulig å skanne vedlegg med innhold som er under direkte kontroll av avsender (for eksempel, passordbeskyttet og/eller kryptert vedlegg).

5.3 Email IC kan skanne for pornografiske bilder innlagt i visse versjoner av Word, Excel, PowerPoint og pdf-dokumenter, men ikke i andre dokumenter.

5.4 Symantec fremhever at konfigureringen av Email IC er fullstendig underlagt Kundens kontroll. Email IC er påtenkt å anvendes kun for å gjøre Kunden i stand til å håndheve en eksisterende, effektivt implementert og akseptabel computer bruker policy (eller tilsvarende). I visse land kan det være nødvendig å innhente samtykke fra den individuelle bruker/ansatt. Symantec råder Kunden til alltid å sjekke lokal lovgivning før implementering av Email IC. Symantec aksepterer ikke ansvar for noe sivilt krav eller strafferettslig ansvar som Kunden kan bli påført som følge av driften av Email IC. Kunden aksepterer at definisjonen av hva som er og hva som ikke er et pornografisk bilde er subjektiv. Kunden må hensynta dette når Tjenesten konfigureres.

5.5 Hvis Kunden frigjør eller ber om frigivelse av en virus-infisert Email, vil den frigjorte Emailen ikke bli skannet av Email IC forut for frigivelsen.

Bilag 3 – Symantec MessageLabs Email Anti-Spam.cloud Tjenesten

1. Oversikt

1.1 Symantec MessageLabs Email Anti-Spam.cloud tjeneste ("Email AS") er Symantecs Internett-nivå Email Anti-Spam tjeneste som er designet for å beskytte Kunden mot uoppfordret eller uønsket Email.

2. Tjeneste Beskrivelse

2.1 Kundens innkommende Email kan skannes ved hjelp av en rekke ulike påvisningsmetoder for å avgjøre hvorvidt det er Spam. Hvis en innkommende Email mistenkes å være Spam, vil en av flere mulige handlinger bli foretatt avhengig av konfigureringsalternativene som er valgt av Kunden i Klausul 3.2 nedenfor.

2.2 En liste for privat godkjente avsendere kan settes sammen av Kunden, og av en individuell Bruker hvis Kunden har muliggjort Brukernivåinnstillinger. Hvis påvisningsmetoden er valgt og en innkommende Email er mottatt fra en avsender listet som godkjent domene, vil den automatisk passere mulige andre valgte Spam påvisningsmetoder.

2.3 En liste for privatblokkerte avsendere kan settes sammen av Kunden, og av en individuell Bruker hvis Kunden har muliggjort Brukernivåinnstillinger. Hvis denne påvisningsmetode er valgt og en innkommende Email mottas fra en avsender på listen over blokkert avsender domener, vil en handling bli foretatt iht. det som er definert av konfigureringsmulighetene i Klausul 3.2 nedenfor.

2.4 En rekke offentlige blokkert avsenderlister kan anvendes. Hvis en av disse påvisningsmetoder er valgt og en innkommende Email er mottatt fra et domene som er listet på en av de valgte offentlige blokkeringslistene, vil en handling bli foretatt iht. det som er definert av konfigureringsmulighetene i Klausul 3.2 nedenfor.

2.5 Hvis Emailen ikke har blitt slettet som følge av at den er blokkert som beskrevet ovenfor og signatursystem er valgt og handlingen som ville blitt foretatt som følge av påvisning av Emailen siden Spam, som er mer alvorlig enn det som allerede er valgt som følge av påvisning som blokkert avsender, vil Kundens innkommende Email bli skannet ved hjelp av signatur-systemet. Hvis en Email er påvist ved denne metoden som Spam, vil aksjon bli tatt som definert av konfigureringsmulighetene i klausul 3.2 nedenfor. Denne handlingen vil overstyre enhver mindre alvorlig handling som allerede er utløst av en metode fra listen over blokkerte avsendere.

2.6 Hvis Emailen ikke har blitt slettet som følge av de foregående prosesser og heuristikk påvisning er valgt og handlingen som ville blitt foretatt som følge av påvisning av Emailen som Spam som konfigurert av Kunden er mer alvorlig enn det som allerede er valgt, som følge av påvisning ved de foregående prosesser, vil Kundens innkommende Email bli skannet ved hjelp av heuristikk skanning. Hvis en innkommende Email er heuristisk oppdaget som Spam, vil handling bli foretatt som definert i konfigureringsmulighetene i klausul 3.2 nedenfor. Denne handlingen vil overstyre enhver mindre alvorlig handling som allerede er utløst av en av de foregående metoder.

2.7 Blokkert avsender/godkjent avsenderlister som besørges av Symantec er kun gitt som eksempler.

3. Konfigurering

3.1 Når Symantec har mottatt ferdig utfylt og akseptert bestilling, vil Symantec gjøre Email AS tilgjengelig for Kunden. Oppstart Email AS vil bli gjort tilgjengelig for hvert av Kundens domener. KUNDEN ERKJENNER AT EMAIL AS VIL BLI ANSKAFFET MED SYMANTECS DEFAULT INNSTILLINGER ANVENDT FRA OPPSTART OG AT DET ER KUNDENS ANSVAR ALENE Å KONFIGURERE EMAIL AS GJENNOM CLIENTNET IHT. KUNDENS EGNE KRAV. Default innstillinger som anvendes for Email AS inkluderer følgende handlinger:

3.1.1. Blokkere og slette Email; eller
3.1.2. Sette Email i karantene; og
3.1.3. Bruk av en godkjent avsenderliste for IP-adresser, domener og emailadresser; og
3.1.4. Bruk av forutsiende Spam påvisning (Skeptic).

3.2 Muligheter er tilgjengelig for å spesifisere hvilken handling som skal foretas hvis en Email mistenkes å være Spam. Disse muligheter, listet nedenfor, kan velges for hver av de tilgjengelige påvisningsmetoder:

3.2.1 Tagge mistenkelig Email innen headeren;

3.2.2 Tagge mistenkelig Email i subjekt feltet;

3.2.3 Omdirigere mistenkelig Email til en forhåndsdefinert Email adresse (som må være på et domene som skannes av Tjenesten);

3.2.4 Slette mistenkelig Email;

3.2.5 Sette i Spam Karantene (Spam Quarantine).

4. Spam Quarantine Tjeneste Beskrivelse

4.1 Hvis Kunden konfigurerer Spam Quarantine for et domene, vil hver Brukers Spam Quarantine konto bli satt opp automatisk første gang en mistenkelig Spam er identifisert av Email AS og Brukeren vil automatisk motta en Email varsling.

4.2 Spam Quarantine er tilgjengelig for Brukeren via Spam Manager interface.

4.3 Mistenkelig Spam kan lagres for en maksimal periode på fjorten (14) dager, og vil deretter automatisk bli slettet. Kunden kan kjøpe utvidet lagring utover slik fjorten (14) dagers periode ved å betale en tilleggsavgift som kalkuleres pr. bruker pr. dag basis ("Symantec MessageLabs Extended Spam Quarantine").

4.4 Hvis Spam Quarantine ikke er i stand til å akseptere Email som mistenkes som Spam, vil Emailen bli tagget og sendt til mottakeren.

5. Spam Quarantine Konfigurering

5.1 Kunden konfigurerer Spam Quarantine via ClientNet.

5.2 Default Bruker varsling er iht 0 nedenfor. Brukeren kan til enhver tid velge en av de følgende varslingsmuligheter:

5.2.1 Varslinger mottas daglig;

5.2.2 Varslinger mottas med varierende hyppighet;

5.2.3 Varslinger mottas ikke.

5.3 Følgende frigivelses muligheter er tilgjengelig gjennom Spam Manager: (i) slette Email; (ii) frigi Email til original mottaker adresse; (iii) gjennomgå Email tekst.

5.4 For å benytte Spam Quarantine må Kunden ha registrert en Validation Liste hos Symantec. Validation Listen omfatter alle gyldige Email adresser som anvendes av Kunden. En hver mottakeradresse som ikke er på Validation Liste ansees å være ugyldig og Email vil ikke kunne leveres til slik adresse.

5.5 Gjennom ClientNet kan Kunden kontrollere andre aspekter ved Spam Manager: (a) automatisk eller manuell varslings policy; (b) oppsett av oppsummering varslinger; (c) default språk innstillinger; (d) brukernivå innstillinger; (e) forhåndsinnstilt kortnavn Email og (f) spesialiserte Brukere (for eksempel Quarantine Administratorer).

5.6 Kunden kan etablere grupper av email adresser for Spam Quarantine. Dette for å knytte en rekke individuelle email adresser til en "eier" email adresse, med formål å kunne gi email kortnavn og delegert tilgang. Største antall email adresser som kan knyttes til en single email adresse er femti (50). Symantec forbeholder seg retten til å fjerne Kundens konto gruppe eller kortnavn- linker, dersom maksimumsgrensen overskrides.

6. Rapportering

6.1 Rapportering av effektivitet av Email AS besørges gjennom ClientNet. ClientNet kan konfigureres til å produsere rapporter som sendes pr Email til Kunden på ukentlig eller månedlig basis.

7. Email AS Vilkår og Betingelser

7.1 INTET ANTI-SPAM SOFTWARE KAN GARANTERE 100% OPPDAGELSESRATE OG PÅ DENNE BAKGRUNN KAN SYMANTEC IKKE AKSEPTERE ANSVAR FOR SKADE ELLER TAP SOM DIREKTE ELLER INDIREKTE RESULTERER FRA EN FEIL VED TJENESTEN KNYTTET TIL MANGLENDE PÅVISNING AV SPAM ELLER FOR FEILAKTIG Å HA PÅVIST EN EMAIL SOM SPAM, TIL TROSS FOR AT DET SENERE VISER SEG Å IKKE VÆRE DET.

7.2 Symantec fremhever at konfigureringen av Email AS er fullstendig underlagt Kundens kontroll. Symantec anbefaler at Kunden har en akseptabel computer bruker policy (eller

tilsvarende)Email IC er påtenkt å anvendes kun for å gjøre Kunden i stand til å håndheve en eksisterende, effektivt implementert og akseptabel computer bruker policy (eller tilsvarende). I visse land kan det være nødvendig å innhente samtykke fra den individuelle bruker/ansatt. Symantec tilråder Kunden alltid å sjekke lokal lovgivning før implementering av Email AS. Symantec aksepterer ikke ansvar for noe sivilt krav eller strafferettslig ansvar som Kunden kan bli påført som følge av driften av Email AS.

Bilag 4 – Symantec MessageLabs Email Content Control.cloud Tjeneste

1. Oversikt

1.1 Symantec MessageLabs Email Content Control.cloud ("Email CC") er Symantecs innholds kontroll tjeneste designet for å sette Kunden i stand til å konfigurere sine egne regler basert på filter strategi i samsvar med akseptabel computer bruker policy (eller tilsvarende) relatert til Email.

2. Tjeneste Beskrivelse

2.1 Email CC tillater Kunden å bygge en samling regler som skal filtrere innkommende og utgående Email i samsvar med dette Bilag 4. En regel er en instruksjon laget av Kunden og som anvendes til å identifisere et bestemt format av beskjed/vedlegg eller innhold, og som forordner en bestemt handling i tilknytning til Emailen.

3. Konfigurering

3.1 Når Symantec har mottatt ferdig utfylt og akseptert bestilling, vil Symantec gjøre Email CC tilgjengelig for hvert av Kundens gjeldende domener. Kunden er ansvarlig for å implementere konfigureringsmulighetene for Email CC for hvert domene iht Kundens behov. Kunden konfigurerer Email CC via ClientNet.

3.2 Kunden kan konfigurere regler på et 'pr. domene', 'pr. gruppe' eller 'individuell' basis.

3.3 Endringer kan gjøres av Kunden i reglene. Endringer vil bli effektive innen 24 timer.

3.4 Muligheter er tilgjengelig for å definere handlinger som skal foretas når mistenkelig Email påvises. Disse muligheter kan innstilles selvstendig for innkommende og utgående Email og bør settes iht Kundens eksisterende og akseptabel computer bruker policy (eller tilsvarende). Disse muligheter er:

3.4.1 Blokkere og slette mistenkelig Email;

3.4.2 Tagge (hvis innkommende) og omdirigere mistenkelig Email til en spesifisert administrator;

3.4.3 Tagge (hvis innkommende) og kopiere mistenkelig Email til en spesifisert administrator;

3.4.4 Tagge (hvis innkommende) header av mistenkelig Email;

3.4.5 Komprimere Email vedlegg;

3.4.6 Kun logge til ClientNet statstikk;

3.4.7 Tagge i subjekt feltet.

4. Rapportering

4.1 Gjennom ClientNet kan Kunden gjennomgå resultatene av deres regler i form av daglig, ukentlig, månedlig og årlig sammendrag organisert både etter regel og etter Bruker.

4.2 Rapporter som inneholder tjeneste aktivitets logger kan produseres på ukentlig eller månedlig basis og bli emailet til Kunden etter anmodning.

4.3 Gjennom ClientNet kan Kunden aktivere og deaktivere varslinger konfigurert av Kunden på en pr. regel basis.

5. Innhold Kontroll Support

5.1 Support inkluderer Gjennomgang av Emailen CC interface inklusiv Tjeneste beskrivelsen og Q&A sesjon.

6. Wildcarding

6.1. Email CC fungerer iht Kundens konfigurerte regler. Men med det særlige unntak at wildcarding tillater Kunden å konfigurere Email CC gjennom ClientNet til å identifisere visse alfanumeriske formler som følger et særlig mønster (for eksempel Social Security nummer, personnummer og kredittkort informasjon).

7. Innhold Kontroll Vilkår og Betingelser

7.1 Veiledende ordlister og template regler levert av Symantec inneholder ord som kan ansees å være støtende.

7.2 Kunden aksepterer og er enig i at Symantec kan samle og publisere default ordlister som inneholder ord ervervet fra Kundens tilpassede ordliste.

7.3 Kunden aksepterer at dersom Email CC er anvendt i forbindelse med karantene behandling av Emailen Anti-Spam Tjenesten, kan dette resultere i at mistenkelig Spam blir satt i karantene før den har blitt filteret av Email CC.

7.4 Email CC kan skanne for innhold innlagt i visse versjoner av Word, Excel PowerPoint og pdf dokumenter, men ikke andre dokumenter.

7.5 Symantec fremhever at konfigureringen av Email CC er fullstendig underlagt Kundens kontroll, og at presisjonen i slik konfigurering vil avgjøre presisjonen i Email CC Tjenesten. Symantec aksepterer ikke ansvar for tap eller skade som resulterer direkte eller indirekte fra feil ved Tjenesten i forhold til å oppdage eller feilaktig identifisere at en Email inneholder mistenkelig innhold, som senere viser seg ikke å inneholde det.

7.6 Symantec anbefaler at Kunden har en akseptabel computer bruker policy (eller tilsvarende) i kraft som regulerer Brukernes bruk av Email og at template regler tilført av Symantec supporterer slik policy. I visse land vil det være nødvendig å innhente samtykke fra individuelle brukere/ansatte. Symantec råder Kunden til alltid å undersøke lokal lovgivning før implementering Email CC. Symantec aksepterer ikke ansvar for strafferettslig eller sivilt ansvar som kan pådras av Kunden som følge av bruk av Email CC.

Bilag 5 – Symantec MessageLabs Email Boundary Encryption.cloud Tjeneste

1. Oversikt

1.1. Symantec MessageLabs Email Boundary Encryption.cloud Tjeneste ("BE") besørger krypterte kommunikasjons som gjør Kunden i stand til å lage et sikkert privat Email nettverk (SPA) med nominerte partner organisasjoner ("SPEN Partners"). Slik konfigurering betegnes "Enforced" kryptering.

1.2. I tillegg har Kunden mulighet til å motta opportunistisk kryptert Email som sendes fra organisasjoner som har TLS-capable mail servere, som det ikke finnes Enforced kryptering for hos Kunden. Slik konfigurering kalles "Opportunistic" kryptering.

1.3. Hvis Kunden abonnerer på BE, men ikke uttrykkelig har identifisert noen SPEN Partnere, kan Kunden motta Email sendt opportunistisk innkommende over TLS, og sende Email kryptert opportunistsk utgående til non-SPEN Partner organisasjoner.

1.4. Kunden kan også konfigurere sine email servere for "Sikker Kobling" modell av BE, i hvilket tilfelle:

1.4.1 Email utveksling mellom Symantecs og Kundens Sikker Kobling mail servere skal sikres av TLS kryptering. Hvorvidt videresending vil bli utført i ukryptert eller kryptert format vil bero på (i) Kundens spesifiserte TLS håndheving og (ii) destinasjon server kapasitet til å motta Email over Opportunistic TLS.

1.4.2 KUNDEN FORSTÅR OG AKSEPTERER AT DERSOM SIKKER KOBLING MODEL IKKE ANVENDES FOR EN BESTEMT MAIL SERVER, VIL KUNDENS INNKOMMENDE OG UTGÅENDE EMAIL SOM KOMMER FRA ELLER MOTTAS AV SLIK MAIL SERVER, IKKE SIKRES AV TLS KRYPTERING. FØLGELIG FORSTÅR OG AKSEPTERER KUNDEN AT MAN IKKE SKAL SENDE ELLER MOTTA SENSITIVE DATA VIA SLIK MAIL SERVERE OG GJØR DETTE EVENTUELT FULLSTENDIG FOR EGEN RISIKO.

1.5 Hvis Kunden anvender BE i forbindelse med PBE Tjenesten, er Symantecs anbefalte "best practice" for Kunden å implementere Sikker Kobling smodell av BE på alle mail servere.

1.6 **BE FUNGERER KUN NÅR ANVENDES SAMMEN MED EN AV DE FØLGENDE TJENESTER OG KAN IKKE BENYTTES SOM EN SELVSTENDIG TJENESTE: EMAIL AV, EMAIL AS, EMAIL IC OG/ELLER EMAIL CC.**

2. Levering og fakturering

2.1. Symantec vil belaste for BE fra datoen Symantec bekrefter at kundens nettverk er teknisk i stand til å støtte BE ("dato for teknisk godkjenning").

2.2 Paragraf 5.2 i Vedlegg 1 gjelder ikke for BE. Symantec vil søke å levere BE-bestillinger og BE-endringsanmodninger innen 4 uker etter dato for teknisk godkjenning, forutsatt at kunden har utført alle nødvendige forberedelser.

2.3 Dersom Symantec må allokere ytterligere tekniske resurser for å besørge Kundens anskaffelsen av BE, fordi Kunden ikke har utført nødvendig teknisk due diligence, skal Symantec ha rett til å kreve et tilleggsvederlag på £1500/€1500 (avhengig av valutaen som Kunden faktureres i) pr. person pr. dag.

3. Konfigurering

3.1. Kunden skal definere SPEN Partners som Kunden ønsker å kommunisere sikkert med fra domene. SPEN Partners kan være kunder eller ikke – kunder av BE, men Symantec vil ikke gi direkte support til SPEN Partners. Non-SPEN Partner organisasjoner kan motta Email over Opportunistic Outbound TLS som beskrevet i Klausul 1 ovenfor, dersom deres mail servere supporterer mottakelse av kryptert mail.

3.2. BE er basert på standard 'SMTP over TLS' (Simple Mail Overfører Protocol over Transport Layer Sikkehet) ("STARTTLS").

3.3. Både Kundens og SPEN Partneres mail servere må supportere STARTTLS for å muliggjøre bruk av BE.

3.4. BE er supportert av valgte Tårn, som alle STARTTLS Email vil bli formidlet igjennom. Dette innebærer at Kunden utpeker hvilke av dets domener som skal anvende BE.

3.5. Når BE anvendes i forbindelse med signaturing system funksjonalitet for Email AS, anbefaler Symantec at Kunden inkluderer i sin Email AS en godkjent avsender liste for alle dets SPEN Partner domener. Dersom slik anbefalt "best practice" ikke er fulgt, forstår og godtar Kunden at lokalt signaturing system i visse tilfeller ikke vil være tilgjengelig. Email kan bli omdirigert til et remote signaturing system via et offentlig nettverk.

4. Sertifikater og Autentisering

4.1. Når Kunden starter en STARTTLS kobling må aksepterende mail server besørge sertifikat for autentisering. Hvis aksepterende mail server ønsker å autentisere Tjenesten vil Symantec besørge klient sertifikat for autentisering. Hvis aksepterende mail server ikke kan autentisere, vil Emailen bli returnert til Kunden.

4.2. Når en ekstern mail server starter en STARTTLS kobling, vil Tjenesten besørge server sertifikat for autentisering, men vil ikke insistere på at ekstern mail server gir klient sertifikat for autentisering.

4.3. Validering av sertifikat er basert på Sertifikat Myndighet som har signert sertifikatet. For hvert sertifikat som inngis av en remote mail server som del av en STARTTLS kobling, vil Tjenesten validere at anerkjent Sertifikat Myndighet har signert sertifikatet. Hvis et sertifikat ikke kan valideres mot anerkjent Sertifikat Myndighet, vil koblingen bli brutt og Emailen vil bli returnert til avsender.

5. Krypteringsvilkår og Betingelser

5.1. Symantec tar ikke ansvar for Kundens eller tredjeparts (inklusiv en SPEN Partner) manglende oppfyllelse av plikten til å registrere sertifikater eller for nøyaktighet og rettidighet av slik informasjon.

5.2. BE er påtenkt å anvendes kun for å besørge at Kunden kan håndheve en eksisterende, effektivt implementert og akseptabel computer bruker policy (eller tilsvarende). Bruk av kryptert tjenester kan i noen land være underlagt særlig lovgivning. Kunden rådes til alltid å sjekke relevant lovgivning før man anvender BE Tjenesten. Symantec aksepterer ikke ansvar for sivile krav eller straffeansvar som følge av bruken av BE.

Bilag 6 – Symantec MessageLabs Web v2 Protect.cloud Tjenesten

1. Oversikt

1.1. Når relevante konfigureringsendringer er gjort for Web sider og vedlegg, vil disse bli dirigert elektronisk via Symantec MessageLabs Web v2 Protect.cloud Tjenesten ("Web v2 Protect") og bli digitalt undersøkt for virus.

2. Tjeneste Beskrivelse

2.1. Kundens eksterne HTTP og FTP-over-HTTP anmodninger inklusiv alle vedlegg, macros eller kommandoer dirigeres gjennom Web v2 Protect.

3. Konfigurering

3.1. Konfigureringsinnstillinger som er påkrevd for å dirigere slik eksterne trafikk via Web v2 Protect gjøres og vedlikeholdes av Kunden og er avhengig av Kundens tekniske infrastruktur. Kunden bør påse at intern HTTP/FTP-over-HTTP trafikk (f.eks. til selskaps intranett) ikke dirigeres via Web v2 Protect. Hvor Kunden har Internett tjenester som krever en direkte kobling isteden for via proxy, er det Kundens ansvar at nødvendige endringer gjøres i egen infrastruktur for å fasilitere dette.

3.2. Tilgang til Web v2 Protect er begrenset via Skanning IP dvs. IP adressen(e) som Kundens web trafikk genereres fra. Skanning IP blir også brukt til å identifisere Kundens og dynamisk valgte Kunde-spesifikke innstillinger.

3.3. Web v2 Protect vil skanne passende deler av Web side og vedlegg som kan inneholde virus, ødeleggende koder, spyware eller adware. Det er ikke mulig å skanne visse Web sider, innhold eller vedlegg (for eksempel, passord beskyttet). Vedlegg som uttrykkelig er identifisert som uskannbare vil ikke bli blokkert. Streamed og kryptert trafikk (dvs. streaming Media og/eller HTTPS/SSL) kan ikke skannes og vil bli sendt gjennom Web v2 Protect uskannet.

3.4 Roaming Bruker Support er en tilleggsmulighet som utvider Web v2 Protect Tjenesten til bruker som ikke er innen selskapets nettverk (for eksempel til en Bruker som jobber hjemmefra). Kunden må installere en PAC file på Brukerens PC slik at Brukeren er vist til Symantecs web portal når søker startes opp. For tilgang til web portalen, må Brukeren oppgi passord og brukernavn. PAC fil template kan lastes ned fra ClientNet og modifiseres av Kunden.

4. Varsel

4.1. Hvis en av Kundens Web sider eller vedlegg finnes å inneholde en enhet som identifiseres som et Virus, Spyware eller Adware, vil tilgangen til slik Web side eller vedlegg nektes og internettbrukeren vil se en automatisk varslings Web side. I sjeldne tilfeller, og hvor en eller flere deler av anmodet innhold er blokkert, vil det ikke være mulig å vise varslings Web side og varslings Web side kan erstatte innholdet av den anmodede enheten, men tilgang til den infiserte siden eller vedlegg vil fortsatt bli nektet.

4.2. Der finnes en seksjon innen automatisk varslings Web sider som Kunden kan tilpasse via ClientNet.

5. Rapportering

5.1 Rapportering av effektivitet av Web v2 Protect besørges gjennom ClientNet.

5.2 For å muliggjøre pr. Bruker eller gruppe rapportering, vil Kunden måtte installere relevant software applikasjon ("Client Site Proxy") i samsvar med installasjonsveiledningen. Bruk av Client Site Proxy er underlagt End User Lisens Avtalen og besørges med Client Site Proxy.

5.3 Kunden anerkjenner at ClientNets detaljerte rapporterings data kun lagres for en maksimums periode på førti (40) dager og vil ikke være tilgjengelig for Kunden etter utløp av denne perioden. ClientNet oppsummeringsdata er tilgjengelig for en maksimum periode på tolv (12) måneder.

5.4 Kunden kan anmode om en utvidet rapporteringsperiode for ClientNets detaljerte rapport for en maksimumsperiode på inntil seks (6) måneder ved å abonnere på WSS Enhanced Data Retensjon.

6. Generelle Vilkår og Betingelser

6.1. INTET WEB SKANNING SOFTWARE KAN GARANTERE 100% PÅVISNINGSRATE OG DERFOR KAN SYMANTEC IKKE AKSEPTERE ANSVAR FOR SKADE ELLER TAP SOM RESULTERER DIREKTE ELLER INDIREKTE FRA MANGEL VED Web v2 Protect I FORHOLD TIL Å OPPDAGE VIRUS, ØDELEGGENDE KODE, SPYWARE ELLER ADWARE.

6.2. Symantec fremhever at konfigurering av Web v2 Protect kontrolleres utelukkende av Kunden. Web v2 Protect er påtenkt å anvendes kun for å gjøre Kunden i stand til å håndheve en eksisterende, effektivt implementert og akseptabel computer bruker policy (eller tilsvarende). I visse land kan det være nødvendig å innhente samtykke fra de individuelle brukerne. Symantec råder Kunden til alltid å undersøke lokal lovgivning før implementering Web v2 Protect. Symantec kan ikke akseptere ansvar for sivile krav eller straffeansvar som Kunden kan pådra seg som følge av anvendelsen av Web v2 Protect.

6.3 Kundens web trafikk når Web v2 Protect anvendes, skal ikke overskride tretti megabytes (30MB) pr. Bruker pr. dag (beregnet som et gjennomsnitt pr. Bruker for Kundens totale registrerte bruk for Web v2 Protect). I tilfelle den daglige grensen overskrides, forbeholder Symantec sin rett til å:

6.3.1 umiddelbart stanse besørgelsen av eller suspendere hele eller deler av Web v2 Protect frem til slik overskridende bruk er avhjulpet; eller

6.3.2 kreve at Kunden kjøper ytterligere Bruker kapasitet for å reflektere virkelig web trafikk bruk og øke fakturabeløp og/eller gjøre justeringer i senere fakturer for å dekke prisen for økt registrert bruk på pro-rata basis for den gjenstående del av inneværende faktureringsperiode.

Bilag 7 – Symantec MessageLabs Web v2 URL.cloud Tjenesten

1. Oversikt

1.1. Når relevante konfigureringsendringer er gjort for Web sider og vedlegg, vil disse bli dirigert elektronisk via Symantec MessageLabs Web v2 URL.cloud Tjeneste ("Web v2 URL") og bli digitalt undersøkt for virus.

2. Tjeneste Beskrivelse

2.1. Kundens eksterne HTTP og FTP-over-HTTP anmodninger inklusiv alle vedlegg, macros eller kommandoer dirigeres gjennom Web v2 URL.

3. Konfigurering

3.1. Konfigureringsinnstillinger som er nødvendig for å dirigere slik eksterne trafikk via Web v2 URL gjøres og vedlikeholdes av Kunden og er avhengig av Kundens tekniske infrastruktur. Kunden bør påse at intern HTTP/FTP-over-HTTP trafikk (f.eks. til selskaps intranett) ikke dirigeres via Web v2 URL. Hvor Kunden har Internett tjeneste som krever en direkte kobling istedenfor via en proxy, er det Kundens ansvar å besørge de nødvendige endringer i egen infrastruktur for å fasilitere dette.

3.2. Tilgang til Web v2 URL er begrenset via Skanning IP dvs. IP adressen(e) som Kundens web trafikk genereres fra. Skanning IPs brukes også til å identifisere Kunden og dynamisk velge Kunde-spesifikke innstillinger.

3.3. Kunden kan konfigurere Web v2 URL for å lage tilgangsbegrensning policy regler via ClientNet (basert både på kategorier og type innhold) og anvende disse til spesifikke tider for spesifikke Brukere eller grupper av Brukere ved å anvende Client Site Proxy beskrevet i Klausul 5.1.

3.4. KUNDEN AKSEPTERER AT Web v2 URL VIL BLI BESØRGET MED SYMANTECS DEFAULT INNSTILLINGER FRA UTGANGSPUNKTET OG AT DET ER KUNDENS ANSVAR ALENE Å KONFIGURERE Web v2 URL GJENNOM CLIENTNET IHT. EGNE KRAV. Default innstillingene omfatter en "Blokkere og Logg" funksjon for følgende URL Kategorier:

3.4.1 Adult / Sexually Explicit; og
3.4.2 Spyware; og
3.4.3 Spam URLs; og
3.4.4 Kriminell aktivitet.

3.5 Roaming Bruker Support er en tilleggsfunksjon som utvider Web v2 URL Tjenesten til brukere som ikke er innen selskapets nettverk (for eksempel til en Bruker som jobber hjemmefra). Kunden må installere en PAC file på Brukerens PC slik at Brukeren vises til Symantecs web portal når søkemotoren startes opp. For tilgang til web portalen, må Brukeren oppgi passord og brukernavn. PAC file template kan lastes ned fra ClientNet og tilpasses av Kunden.

4. Varsel

4.1. Hvis en Bruker anmoder om en Web side eller et vedlegg hvor en tilgangsbegrensnings policy gjelder, vil tilgang til slik Web side eller vedlegg nektes og Brukeren vil se en automatisk varslings Web side. I sjeldne tilfeller, og hvor en eller flere deler av anmodet innhold er blokkert, vil det ikke være mulig å vise varslings Web side og varslings Web side kan erstatte innholdet av den anmodede delen, men tilgang til den relevante siden vil fortsatt bli nektet.

4.2. Der finnes en seksjon innen automatisk varslings Web sider som Kunden kan tilpasse via ClientNet.

5. Rapportering

5.1. Rapportering av resultatene fra en av Kundens tilgangs begrensning policy regler som lages iht Klausul 3.3 ovenfor besørges gjennom Client Net.

5.2 For å muliggjøre pr. Bruker eller gruppe administrasjon og rapportering, vil Kunden måtte installere relevant software applikasjon ("Client Site Proxy") iht. installasjonsveiledningen. Bruk av Client Site Proxy er underlagt End User Lisens Avtalen og besørges med Client Site Proxy.

5.3 Kunden anerkjenner at ClientNet detaljert rapportering data kun lagres av Symantec for en maksimum periode på førti (40) dager og vil bli ikke bli tilgjengelig for Kunden etter utløpet av slik periode. ClientNet oppsummeringsdata er tilgjengelig for en maksimum periode av tolv (12) måneder.

5.4 Kunden kan anmode om en utvidet rapporteringsperiode for ClientNets detaljert rapport på inntil seks (6) måneder ved å abonnerer på WSS Enhanced Data Retensjon.

6. Generelle Vilkår og Betingelser

6.1. INTET WEB FILTERINGS SOFTWARE KAN GARANTERE 100% PÅVISNING RATE OG DERFOR KAN MESSAGELAB IKKE AKSEPTERE ANSVAR FOR NOEN SKADE ELLER TAP SOM RESULTERER DIREKTE ELLER INDIREKTE FRA MANGLER VED Web v2 URL I FORHOLD TIL Å OPPDAGE BLOKKERT URLs ELLER INNHOLD.

6.2. Symantec fremhever at konfigurering av Web v2 URL alene er Kundens ansvar og underlagt Kundens kontroll. Web v2 URL er påtenkt å anvendes alene for å gjøre Kunden i stand til å håndheve en eksisterende, effektivt implementert og akseptabel computer bruker policy (eller tilsvarende). I visse land vil det være nødvendig å innhente samtykke fra individuell personell. Symantec råder Kunden til alltid å undersøke lokal lovgivning før implementering Web v2 URL. Symantec kan ikke akseptere ansvar for sivile krav eller straffeansvar som Kunden kan pådra seg som følge av anvendelsen av Web v2 URL.

6.3 Kundens web trafikk når Web v2 URL anvendes skal ikke overskride tretti megabytes (30MB) pr. bruker pr. dag (beregnet som et gjennomsnitt pr. bruker på kryss av Kundens totale Registeret Usage for Web v2 URL). I tilfelle slik daglig grense overskrides, forbeholder Symantec sin rett til å:

6.3.1 umiddelbart holde tilbake besørgelsen av eller suspendere hele eller deler Web v2 URL og inntil slik overskridende bruk er avhjulpet; eller
6.3.2 kreve at Kunden kjøper ytterligere Bruker kapasitet for å reflektere virkelig web trafikk bruk og øke fakturabeløp og/eller gjøre justeringer i senere fakturer for å dekke prisen for økt registrert bruk på pro-rata basis for den gjenstående del av inneværende faktureringsperiode.

Bilag 8 – Symantec MessageLabs Email Archiving.cloud (P) Tjenesten

1. Tjeneste Oversikt

1.1 Symantec MessageLabs Email Archiving.cloud (P), Symantec MessageLabs Email Archiving.cloud Lite (P) og Symantec MessageLabs Email Archiving.cloud Premium (P) Tjenester (sammen benevnt "Arkivering (P) Tjenesten") er en hybrid administrert arkiveringstjeneste for arkivering, lagring og gjenfinning av Email.

1.2 For Kunder med *500 Brukere eller færre*, vil *Symantec MessageLabs Email Archiving.cloud Lite (P)* inkluderer følgende:

(i) Standard funksjoner som beskrevet i klausul 3 nedenfor;

(ii) 3 års lagringsperiode;

(iii) Maksimum lagring av 3GB pr. Bruker (beregnet som et gjennomsnitt pr. Bruker basert på totalt antall Brukere).

For Kunder med *flere enn 500 Brukere*, vil *Symantec MessageLabs Email Archiving.cloud Lite (P)* inkludere følgende:

(i) Standard funksjoner som beskrevet i klausul 3 nedenfor;

(ii) 1 år lagringsperiode;

(iii) Maksimum lagring av 1.5GB pr. Bruker (beregnet som et gjennomsnitt pr. Bruker basert på totalt antall Brukere).

1.3 For Kunder med *500 Brukere eller færre*, vil *Symantec MessageLabs Email Archiving.cloud (P)* inkludere følgende:

(i) Standard funksjoner som beskrevet i klausul 3 nedenfor;

(ii) 10 års lagringsperiode;

(iii) Maksimum lagring av 10GB pr. Bruker (beregnet som et gjennomsnitt pr. Bruker basert på totalt antall Brukere).

For Kunder med *flere enn 500 Brukere*, vil *Symantec MessageLabs Email Archiving.cloud (P)* inkludere følgende:

(i) Standard funksjoner som beskrevet i klausul 3 nedenfor;

(ii) Ubegrenset lagringsperiode;

(iii) Maksimum lagring av 6GB pr. Bruker (beregnet som et gjennomsnitt pr. Bruker basert på totalt antall Brukere).

1.4 For Kunder med 500 Brukere eller færre, vil *Symantec MessageLabs Email Archiving.cloud Premium (P)* inkludere følgende:

(i) Standard funksjoner som beskrevet i klausul 3 nedenfor;

(ii) Premium funksjoner som beskrevet i klausul 4 nedenfor;

(iii) 10 års lagringsperiode;

(iv) Maksimum lagring av 10GB pr. Bruker (beregnet som et gjennomsnitt pr. Bruker basert på totalt antall Brukere).

For Kunder med flere enn 500 Brukere, vil *Symantec MessageLabs Email Archiving.cloud Premium (P)* inkludere følgende:

(i) Standard funksjoner som beskrevet i klausul 3 nedenfor;

(ii) Premium funksjoner som beskrevet i klausul 4 nedenfor;

(iii) Ubegrenset lagringsperiode;

(iv) Maksimum lagring av 6GB pr. Bruker (beregnet som et gjennomsnitt pr. Bruker basert på totalt antall Brukere).

1.5 Kunden må konfigurere journal-funksjonen til Exchange til å legge igjen en kopi av interne og eksterne Email på en lokal mailboks på Exchange server. Applikasjonen som finnes bak brannmurer innen Kundens selskapsnettverk ("Email Arkivering Appliance(s)") kan da anvendes til å trekke data fra slik mailboks for inngivelse til Arkivering (P) Tjenesten. Email som ikke er slettet, vil lagres i daglig mailboks inntil lagring med Arkivering (P) Tjenesten er bekreftet.

1.6 Symantec skal kontrollere Kundens virkelige bruk av Arkivering (P) Tjenesten og om hvorvidt den aktuelle lagring overskrides i forhold til mengden av kjøpt lagring, i hvilket tilfelle Kunden vil måtte kjøpe ytterligere kapasitet for lagring til Symantecs gjeldende priser. Symantec vil sende ytterligere faktura og/eller gjøre tilpasninger i senere faktura for å dekke vederlag for økt lagring på en pro-rata basis for gjenstående del avgjeldende fakturaperiode.

1.7 Kunden anerkjenner og godtar at så snart en Email har blitt arkivert, så kan den ikke slettes før den avtalte lagringsperiode utløper. Dette betyr at det ikke er mulig å slette individuelt utvalgte Email.

1.8 Kunden forstår og godtar at Symantec ikke er i stand til å opptre som en tredjeparts nedlaster. I tilfelle Kunden får krav på å nominere en tredjepart nedlaster for compliance formål, skal Symantec bruke rimelige anstrengelser for å besørge fasilitering av en direkte og uavhengig Avtale mellom Kunden og Symantecs tredjepart tjeneste besørger for dette formål. Kunden anerkjenner at tredjepart tjenestebesørger kan kreve vederlag for slik tjeneste.

2. Tjeneste Aktivering

2.1 Kunden må utfylle Symantecs Anskaffelse skjema nøyaktig.
2.2 Det kreves at Kunden kjøper Email Arkivering Appliance(s) for å motta Arkivering (P) Tjenesten. Email Arkivering Appliance(s) som er kjøpt (og medfølgende dokumentasjon) vil bli sendt til Kunden for installasjon og konfigurering. Kunden er ansvarlig for all frakt, avgifter, forsikring og skatter i anledning Email Arkivering Appliance.
2.3 Symantec vil kontakte Kunden for å tilslutte en første klient anrop.
2.4 Handlinger vist i Symantecs Klient Oppsett Dokument må ferdigstilles av Kunden før første klient anrop og inkludere, men ikke begrenset til:
2.4.1 Lage ny aktiv katalog bruker konto;
2.4.2 Lage tilleggs aktiv katalog grupper;
2.4.3 Legge til brukere til Exchange grupper;
2.4.4 Brannmur konfigurering (hvis påkrevd);
2.4.5 Muliggjøre Microsoft Exchange Journaling (ikke tidligere enn 48 timer før installering av Emailen Arkivering Appliance);
2.4.6 Installere Email Arkivering Appliance (i rack og oppstartet);
2.4.7 Sikre at alle mailbokser som er påkrevd for arkivering er "mail enabled";
2.4.8 Konfigurere remote tilgang for Symantec.
Kunden kan ringe en Symantec Kunde Tjenesten Manager hvis man trenger assistanse i anledning ovenstående handlinger.
2.5 Første klient anrop skal bli utført via WebEx. I denne samtalen skal Partene:
2.5.1 Verifisere at alle handlinger i Klient Oppsett Dokument har blitt fullført;
2.5.2 Installere arkivering og annet software ved å anvende Symantecs Arkivering Installasjon Prosedyre Dokument;
2.5.3 Gjennomgå Active katalog oppsett;
2.5.4 Aktivere tjeneste;
2.5.5 Verifisere bruker interface tilgjengelighet;
2.5.6 Verifisere arkivering (site-til-site);
2.5.7 Generere kopier av krypteringsnøkler i henhold til Symantecs Nøkkel Back-up Prosedyre Dokument.
2.6 En opplæringssesjon er tilgjengelig under eller etter første klient anrop og omfatter sesjoner fokusert på: (i) DEN, (ii) Policy, (iii) Tilsyn, (iv) End User.
2.7 En etterfølgende telefon gjennomgang vil finne sted ca. en (1) uke etter aktivering. Etter tilfredsstillende gjennomføring av etterfølgende telefon anrop, kan Kunden følge standard support prosedyre dersom ytterligere assistanse er påkrevd.

3. Standard Funksjoner

3.1 *Adresse Oppløsning og Distribusjons Liste/Gruppe Ekspansjon*. Alle email adresser merket av Exchange som interne adresser vil bli oppløst til korresponderende Bruker mailbokser. For hver distribusjonsliste som er mottaker av en beskjed, vil en liste over til enhver tid gjeldende medlemskap bli fanget opp som tilleggs metadata vedrørende Emailen beskjeden.
3.2 *Full-tekst Indeks*. Email Arkivering Appliance kan trekke ut tekst innhold fra forskjellige typer av vedlegg så vel som alminnelige felt i beskjeden for å supportere opprettelse av en full-tekst indeks for å søke innen Arkivering (P) Tjenesten.
3.3 *Kryptering.* Beskjedinnhold data og indeks data (med unntak for felter som dato og annen data som ikke er personlig

identifiserbar informasjon) er kryptert ved å bruke industri standard krypteringsteknologier basert på en KUNDE-spesifikk krypteringsnøkkel som kun innehas av Kunden. Kunden innehar alene alle passord, krypteringsnøkler og konfigurerings innstillinger og følgelig bør Kunden påse at disse oppbevares trygt, og holdes i escrow eller på annen passende lokasjon. Symantec kan ikke akseptere ansvar for tap av passord, krypteringsnøkler eller konfigurering innstillinger. Kunden forstår at tap av passords og krypteringsnøkler vil resultere i at arkivet blir utilgjengelig.

3.4 *Retensjon Policies*. Kunden kan definere og oppdatere lagrings policies via bruker interface. Hver lagrings policy kan vurdere kriterier inklusiv partene involvert, nøkkelord/fraser i innholdet og file type vedlagt. Når hver beskjed er arkivert, vil den bli vurdert opp mot gjeldende sett av lagrings policies. Hvis en beskjed passer flere enn en lagrings policy, vil policy med lengst lagringsperiode bli anvendt. Hvis ingen bestemt lagrings policy passer beskjeden, vil default lagrings policy bli anvendt.

3.5 *InfoTags (metadata)*. Kunden kan definere og oppdatere InfoTags via bruker interface. Hver InfoTag kan vurdere kriterier inklusiv hvilke parter som er involvert, nøkkelord/fraser i innholdet, og hvilken filtype som er vedlagt. Ved arkivering av hver melding, vil den bli vurdert mot aktivt sett InfoTags og flagges med hver som kommer til anvendelse.

3.6 *Policy Tracking*. Endringer som gjøres i lagrings og overvåknings policies vedlikeholdes av systemet i format som ikke kan endres for referanse formål. Kunden kan lage en PDF-format file av gjeldende eller tidligere versjoner av policies via bruker interface.

3.7 *Historisk Bruker Tracking*. En liste over alle Brukere som har en mailboks innen Exchange avgis til systemet hver natt for å opprettholde en løpende liste over alle mailbokser som har eksistert siden Arkivering (P) Tjenesten ble implementert. Slik informasjon kan anvendes til å lage policies og lovlig oversikt over Brukere som har blitt slettet fra Active Directory, så vel som å besørge andre Brukere tilgang til tidligere ansattes email.

3.8 *Vedlegg Stubbing*. Kunden kan muliggjøre funksjonalitet som erstatter vedlegg innhold innen Kundens mail system ("Mailboks Data") med en peker til angjeldende kopi innen arkivet. Kunden kan definere og oppdatere stubbing policies med forskjellige regler for hver gruppe av mailbokser, basert på alder og størrelse på beskjeden så vel som folderen som den befinner seg i. For å fasilitere automatisk gjenoppretting av originalt vedlegg fra arkivet når Brukere videresender mail, kan Kunden installere Vedlegg Stubbing tilpassing form til dets Organization Forms Library (en spesiell offentlig folder på Exchange server). Outlook vil da automatisk installere tilpasset form fra serveren. For å fasilitere tilgang til å gjenfinne vedlegg utenfor Kundens nettverk, kan Kunden installere arkivet Proxy på deres front-end (OWA) Exchange servere. Default innstilling er at kun Mailboks Data som tidligere har vært arkivert vil bli stubbed. Kunden kan muliggjøre en valgmulighet som lagrer en kopi av vedlegg som ikke tidligere er arkivert for å fasilitere stubbing av vedlegg som finnes i mailboksen. Kunden kan konfigurere lagrings policies på en pr.-mailboks basis for å definere hvor lenge vedlegg som lagres på denne måten skal beholdes. Hvis ikke dette er spesifisert, vil default lagrings policy gjelde for disse. Vedlegg som lagres av denne prosessen er ikke søkbare innen arkivet.

3.9 *End-User Tilgang*. Kunden kan velge å besørge tilgang til individuelle Brukere for søk i arkivet, enten innen web user interfacet eller direkte innen Outlook.

3.10 *Legal Discovery Tilgang*. Kunden kan utføre søk mot hele arkivet innen bruker interfacet. Kunden kan lage en "legal hold" som er et oppbevaringssted for beskjeder relevant til et bestemt tema. Kunden kan utføre søke aktiviteter innen "legal hold" på samme måte som de kan søke igjennom det aktive arkivet.

3.11 *Ad-Hoc Legal Holds*. Kunden kan bruke policy bruker interface for å definere og oppdatere ad-hoc legal holds. Legal hold kan vurdere kriterier inklusiv partene som er involvert, nøkkelord/fraser i innholdet, og file type vedlagt. Når hver beskjed er arkivert, vil den bli vurdert mot gjeldende sett legal holds. Beskjeden blir assosiert med hvert legal hold som den matcher. For å fange opp eksisterende arkivert data til en ad-hoc legal hold, kan Kunden utføre et søk med lignende kriterier, kopiere resultatene til en folder, deretter kopiere innholdet av folderen til legal hold. Hver ad-hoc legal hold har en ubegrenset lagringsperiode – alle beskjeder i en gitt ad-hoc legal hold beholdes inntil slikt hold blir frigjort.

3.12 *People-basert Legal Holds*. Kunden kan bruke policy bruker interface for å definere og oppdatere people-basert legal holds. Hvert people-basert legal hold definerer et sett av Brukere. Når hver beskjed er arkivert, som gjelder en av de personer som er listet på et gitt hold, vil den bli assosiert med slikt hold. Systemet vil også automatisk fange opp eksisterende mail som tilhører Brukerne som til enhver til tilhører holdet og lage en ny kopi av beskjeden til holdet. Når Brukere fjernes fra en people-basert legal hold definisjon, vil beskjeder som kun tilhører disse Brukerne som ikke lenger er listet, automatisk bli slettet fra holdet. Beskjeder for Brukere som for tiden er listet og dekkes av et hold, vil beholdes inntil slikt hold blir frigjort.

3.13 *Data Export*. Beskjeder fra aktivt arkiv eller legal hold kan eksporteres til PST filer. Systemet vil lage flere PST filer hvis påkrevd på grunn av file størrelse begrensninger.

3.14 *Rapportering*. Rapporter om størrelse og vekst på arkivet er tilgjengelig til Kunden i bruker interfacet for visning i HTML eller for eksport til PDF eller CSV (data kun).

3.15 Audit Trail. Søk, beskjeder, se på, eksport, gjenfinning og tilsyn aktiviteter blir registrert. Audit Trail kan undersøkes som en egenskap ved enhver gitt beskjed. En Audit Trail visning på kryss av alle beskjeder tillates for filtrerte visninger basert på type aktivitet, person som har utført aktivitet og/eller dato for aktivitet.

3.16 *Integrasjon med Aktive Directory.* Tilgang til arkivet er administrert ved å legge til Brukere (eller eksisterende grupper av Brukere) til et sett av forhånds definerte sikkehetsgrupper innen Active Directory. Hver av disse grupper har et sett privilegier assosiert med dem. En Bruker kan utføre flere roller i kraft av deres medlemskap i flere av disse sikkehetsgrupper. Autentitetskontroll utføres direkte mot Active Directory. Brukere signerer inn ved å anvende deres standard Active Directory brukernavn og passord og deaktivert konti vil miste tilgang til rettigheter til arkivet. Active Directory grupper kan også bli tillagt forskjellige andre aspekter av systemet for enklere å fasilitere administrasjonen av deler av slike policies. En nattlig synkroniserings prosess anvendes til å fange opp endringer i gruppe medlemskap.

3.17 *Retensjon og Disposisjon Management*. Basert på lagrings policy definert av Kunden innen bruker interfacet, vil Arkivering (P) Tjenesten kategorisere beskjeder og enten tildele en mål disposisjonsdato eller registrere måned som beskjeden ble arkivert for ubegrenset lagring. Mål disposisjonsdatoer settes til begynnelsen av hver måned. Så snart beskjeder har nådd deres mål disposisjonsdato, kan Kundens autoriserte Bruker(e) formelt godkjenne disposisjon av alle beskjeder assosiert med slik mål disposisjonsdato. For beskjeder arkivert iht en ubegrenset lagringsperiode, kan Kundens autoriserte Bruker(e) formelt tillate disposisjon for alle beskjeder som ble arkivert i løpet av en gitt måned. Kunden forstår og godtar at når data er angitt for sletting, kan den ikke re-lagres i lesbar format fra noe lagringsmedium (inklusiv uten begrensning back-ups).

4. Premium Funksjoner

Følgende funksjoner er kun inkludert i *Symantec MessageLabs Email Archiving.cloud Premium (P*) Tjenesten:

4.1 *Tilsyn.*

4.1.1 *Automatisk Utvelgelse for Tilsynsgjennomgang.* Kunden kan definere og oppdatere policies via bruker interface som legger til beskjeder til en kø for gjennomgang. Hver policy kan vurdere partene involvert, nøkkelord/fraser i innholdet, og file type. I tillegg, kan tilfeldig prøvetakings policies konfigureres for bestemte Brukere.

4.1.2 Tilsyns gjennomgang. Kunden kan gi rett til tilgang for lesing av beskjeder som har blitt lagt til kø for gjennomgang og for flagging av beskjeder som akseptable eller ikke.

4.2 *Bloomberg Arkivering*

4.2.1 Symantec MessageLabs Email Archiving.cloud Premium (P) Tjenesten bruker loggings funksjoner av Bloomberg Professional Tjenesten som registrerer email og instant beskjed konversasjoner i XML filer som er deklarert på nattlig basis til Bloomberg FTP site.

4.2.2 Hvis Kunden abonnerer på Bloomberg Professional Tjenesten, kan Email Arkivering Appliance anvendes til å gjenfinne en kopi av disse XML filer fra FTP site for konvertering inn i HTML format beskjeder og inngivelse til arkivet.

4.2.3 FIRM formatet blir supportert, men ikke KONTO formatet eller historisk ekstrakt format av Bloomberg logger.
4.2.4 Bloomberg arkivering integrasjon renser ikke innhold fra Bloomberg FTP site, men sporer at filer har blitt prosessert. Fordi Bloomberg renser innhold fra dets FTP site på regelmessig basis, og Bloomberg arkivering integrasjon prosess renser kopier som den har laget på Emailen Arkivering Appliances, må Kunden kontrollere at slik arkivering integrasjon fungerer på en fortløpende basis slik at filer ikke blir slettet før Bloomberg arkivering integrasjon har vært i stand til å gjenfinne og fullt ut prosessere dem.
4.2.5 En liste med Bloomberg FIRM identifiers anvendes til å identifisere at brukere referert til i XML er interne ansatte. Bloomberg arkivering integrasjon besørger en web-basert mapping bruker interface som tillater en administrator å assosiere hver Bloomberg bruker konti til korresponderende Active Directory bruker konti. Når XML filer er prosessert, og en beskjed refererer til en intern bruker som ikke ennå er kartlagt, vil adressen bli tillagt til ikke-kartlagt adresse liste og beskjeden vil ikke bli prosessert. Så snart administratoren har kartlagt disse adresser vil den kunne utløse re-prosessering av de assosierte beskjedene. Oppklarte selskaps email adresser anvendes som avsender/mottaker av beskjeden.
4.2.6 En informerende del av beskjeden besørger tilleggsinformasjon om de aktuelle adresser/visningsnavn for partene av beskjeden/konversasjonen inklusiv brukerens Bloomberg konto informasjon.

5. Legacy Data Importere
5.1 Kunden kan importere legacy data inn i Arkivering (P) Tjenesten som er underlagt gebyrbetaling basert på mengden av data som blir importert. I tilfelle faktisk mengde legacy data overskrider kjøpt mengde importert data, forbeholder Symantec seg retten til å vederlagsbelaste slik tilleggs data til gjeldende standard rater.
5.2 I tilfelle Kunden velger å anvende uavhengig tredjeparts software for å fasilitere import av data til arkivet, forstår og godtar Kunden at Symantec ikke er ansvarlig for slik tredjeparts software og at Kunden gjør dette for egen risiko og regning.

6. Opphør av tjeneste
6.1 Ved opphør av tjenesten Archiving.cloud (P) skal Symantec slette kundens data fra arkivet. Før opphøret kan kunden trekke ut sine data fra arkivet, eller kunden kan be om at Symantecs oppnevnte tredjeparter overfører de arkiverte dataene tilbake til kunden i et PST-filformat, i samsvar med klausul 6.2 nedenfor.
6.2 Hvis kunden ber Symantecs oppnevnte tredjepart om å overføre arkiverte data ved opphør:
6.2.1 Kunden må inngå en direkte avtale med den oppnevnte tredjeparten. Symantec skal ikke være part i en slik avtale.
6.2.2 Ettersom dataene er lagret i kryptert format, må kunden gi tredjeparten en krypteringsnøkkel for å dekode e-posten til et fritt format.
6.2.3 Kunden har ansvaret for overføringskostnadene. Kostnadene skal avtales i avtalen med tredjeparten. Kostnader avhenger av: (i) Datamengde. (ii) overføringens format/medium, (iii) kostnad ved oppsett av overføringsprosessen, (iv) tid og materialer brukt til å gjennomføre overføringen.
6.2.4 Symantec forbeholder seg retten til å belaste sine nåværende priser for lagring dersom dataene ikke eksporteres og slettes fra arkivet på opphørsdatoen.

7. Tjeneste Vilkår og Betingelser
7.1 Symantec kan, etter eget valg, terminere Arkivering (P) Tjenesten med umiddelbar effekt uten varsel og utføre følgende forsvarsmessige handlinger, som måtte synes påkrevd:
7.1.1 Hvis krevd av en domstol eller kompetent myndighet;
7.1.2 I tilfelle angrep på Arkivering (P) Tjenesten eller nettverket;
7.1.3 I tilfelle Kunden eller en av dets Brukere er skyldig i brudd på Akseptabel User Policy i klausul 7.3 nedenfor.
7.2 Kunden er ansvarlig for å besørge at den og alle Kundens Brukere er kjent med og overholder Akseptabel User Policy i klausul 7.3 nedenfor.
7.3 *Akseptabel User Policy*. Brukere må ikke under noen omstendighet gjøre, eller forsøke å gjøre, ei heller medvirke eller oppmuntre noen handling som kan true Arkivering (P) Tjenesten, uavhengig av om dette skjer med overlegg, uaktsomt eller uten skyld. Dette skal inkludere, men er ikke begrenset til:
7.3.1 Et hvert forsøk på å krasje en tjeneste host eller nettverk;
7.3.2 "Denial av tjeneste" angrep eller "flooding" angrep mot en tjeneste host eller nettverk;
7.3.3 Et hvert forsøk på å komme rundt bruker stadfesting eller sikkerhet ved en tjeneste host eller nettverk;
7.3.4 En lastefull bruker av Arkivering (P) Tjenesten;
7.3.5 Opprettelse, overføring, lagring, eller publisering av noen form for Virus eller korrupt program eller korrupte data;
7.3.6 En hver annen handling som negativt kan påvirke Arkivering (P) Tjenesten eller dens drift.
7.4 INGEN EMAIL ARKIVERINGSTJENESTE KAN GARANTERE 100% NØYAKTIGHET OG PÅ DENNE BAKGRUNN KAN SYMANTEC IKKE AKSEPTERE ANSVAR FOR NOEN SKADE ELLER TAP SOM RESULTERER DIREKTE ELLER INDIREKTE FRA MANGLER VED TJENESTE, UTOVER UTTRYKKELIG AVTALT AVHJELP AV MANGLER TIL DET NIVÅ SOM ER AVTALT.
7.5 Kunden erkjenner at email kan inneholde personlig identifiserbar informasjon og at arkivering av email derfor kan innebære prosessering av personlig data. Videre, Kunden erkjenner at Arkivering (P) Tjenesten er en konfigurerbar tjeneste og at Kunden alene er ansvarlig for konfigurering av Arkivering (P) Tjenesten i henhold til Kundens akseptable computer bruker policy (eller tilsvarende) og gjeldende lovgivning eller regler. En hver template som gjøres tilgjengelig av Symantec er ment kun som en guide for å gjøre Kunden i stand til å lage dens egne tilpassede policies og andre templates. Følgelig råder Symantec Kunden til alltid å undersøke lokal lovgivning før implementering av Arkivering (P) Tjenesten, og å forsikre seg om at den, og dets ansatte, er klar over og overholder forpliktelser de måtte ha i forhold til data beskyttelse og privatliv lovgivning og/eller regler i tilknytning til Kundens bruk av Arkivering (P) Tjenesten. I visse land vil det være nødvendig å innhente samtykke fra individuell personell forut for bruk av Arkivering (P) Tjenesten. Symantec kan ikke akseptere ansvar for sivile krav eller straffeansvar som kan pådras av Kunden som følge av Kundens drift av Arkivering (P) Tjenesten. Kunden må ta dette inn i vurderingen ved konfigurering av Arkivering (P) Tjenesten.
7.6 Kunden er pålagt å velge lokasjon for arkivering data sentre på bestillingstidspunktet og vederlaget beregnes basert på slikt valg. HVIS ET ARKIVERINGS DATA SENTER I USA ER VALGT, AKSEPTERER KUNDEN Å GJØRE ALLE NØDVENDIGE HANDLINGER FOR Å (I) INFORMERE ALLE DETS ANATTE, AGENTER OG KONTRAKTØRER SÅVEL SOM TREDJEPARTER SOM BRUKER KOMMUNIKASJONSSYSTEMET SOM DEKKES AV ARKIVERING (P) TJENESTE OM AT ENHVER INFORMASJON, INKLUDERT MEN IKKE BEGRENSET TIL, PERSONLIG IDENTIFISERBAR INFORMATION OM INDIVIDER, KAN BE PROSESSERT I USA; OG (II) INNHENTE SLIKT SAMTYKKE FRA ANSATTE, AGENTER OG KONTRAKTØRER SOM MÅTTE VÆRE NØDVENDIG FOR SLIK PROSSESERING FORUT FOR ARKIVERING (P) TJENESTEN TAS I BRUK AV KUNDEN.
7.7 Kunden forstår og godtar at (i) Symantec skanning tjenester (Email AV, Email AS, Email IC og Email CC) ikke skanner alle email som originalt kommer inn i arkivet og (ii) Symantec skanning tjeneste (Email AV, Email AS, Email IC og Email CC) ikke skanner email som er frigjort fra arkivet for gjeninnsetting til brukerens mailboks. Følgelig kan Symantec ikke holdes ansvarlig for virus, spam, bilder eller upassende innhold som slike gjeninnsatte email kan inneholde, og videre, Service Level Agreement skal ikke gjelde slike gjeninnsatte email.

8. Software Lisens
8.1 De følgende vilkår og betingelser gjelder for software installert på Emailen Arkivering Appliance ("Software"):
8.1.1 Kunden forstår og godtar som gjeldende til enhver tid mellom Kunden og Symantec, at Symantec og/eller dets leverandører er eier av Software. Denne Avtalen gir Kunden en ikke-eksklusiv begrenset lisens til bruk av Software i tilknytning til Arkivering (P) Tjenesten beskrevet i dette Bilag og gir ingen rett til å overdra Software eller annen immateriell rettighet. Alle rettigheter som ikke er uttrykkelig gitt under denne Avtalen, reserveres for Symantec og dets leverandører.
8.1.2 Kunden kan bruke en kopi av Software med en Email Arkivering Appliance. Slik "bruk" som omhandlet i denne Avtale,

innebærer rett til å utføre, kjøre, vise og lagre Software så lenge Arkivering (P) Tjenesten skal besørges.
8.1.3 Software er beskyttet av canadisk og USAs copy rett lovgivning og internasjonale konvensjoner. Kunden kan ikke leie bort eller lease Software eller kopiere dokumentasjon som medfølger Software. Kunden kan ikke kopiere, reverse engineer, ta fra hverandre eller avkode eller forsøke å lage kildekode fra Software.
8.1.4 Kunden aksepterer at et brudd på disse bestemmelser vil resultere i uopprettelig skade for Symantec og dets leverandører, og aksepterer herved at Symantec og/eller dets leverandører direkte kan tvinge igjennom etterlevelse av disse bestemmelser inklusiv (uten begrensning) gjennom midlertidig forføyning og tilsvarende rettslige avgjørelser tilgjengelig iht. lovgivningen.
8.1.5 All teknologi, software, dokumentasjon og prosesser som anvendes av Symantec for å besørge Arkivering (P) Tjenesten er Symantecs eksklusive eiendom eller eiendom av dets leverandører.

Bilag 9 – Symantec MessageLabs EIM.cloud Tjeneste

1. Tjeneste Beskrivelse

1.1 Symantec MessageLabs EIM.cloud Tjenesten ("EIM") er en administrert tjeneste som gir mulighet for administrativ kontroll, sentralisert lagring og domene administrasjon av umiddelbare beskjeder.

1.2 Med unntak for MSI og Java versjoner, vil EIM client ("POD") være installert på hver Brukers arbeidsstasjon. Alle varianter gir Brukeren en sikker tilkobling til EIM plattform og bruker EIM. POD har følgende funksjonalitet:

(a) Fil deling;
(b) Sikker instant messaging konferanse;
(c) Kompatibilitet med offentlig instant messaging nettverk (kun med CONNECT pakke).

1.3 EIM administrasjon verktøy, en web-basert konsoll, som tillater at definerte administratorer styrer deres domene struktur og brukerbase.

2. EIM Tjeneste Funksjoner

Tjeneste Funksjoner – Symantec MessageLabs EIM Communicate.cloud ("COMMUNICATE")

(i) Integrert fil deling (100mb kapasitet pr. Bruker);
(ii) Desktop tilbake-up løsning;
(iii) Mulighet til å dele informasjon med EIM Brukere som er online eller offline;
(iv) Tilgang kontroll lister;
(v) Sikker, 168-bit 3DES SSL kryptert POD-til-POD kommunikasjon;
(vi) Web-basert administrasjon konsoll;
(vii) Omfattende bruker muligheter interface;
(viii) Avansert tilstedeværelse påvisning og tracking;
(ix) Support for en stor mengde av proxy servere ;
(x) HTTP tunnelling capabilities;
(xi) Advarsel varslinger for nye filer;
(xii) Objekt orientert file system med omfattende søke muligheter.

Tjeneste Funksjonalitet – Symantec MessageLabs EIM Connect.cloud ("CONNECT")

Alle funksjoner i COMMUNICATE pakken gjelder med tillegg av følgende:

(i) Interoperable Instant Messenger (AOL, MSN, Yahoo!);
(ii) SMS messaging (2 beskjeder pr. Bruker, eller "Bruker Kvote");
(iii) Instant Messaging Logg muligheter.

Tjeneste funksjonalitet – COLLABORATE

Alle funksjoner i CONNECT pakken gjelder med tillegg av følgende:

(i) Integrasjon med WebEx;
(ii) Integrasjon med Salesforce.com.

3. Ansvar for Konto Antall/Passord.

3.1 Kunden er ansvarlig for alle brukere av administrasjon web site, uavhengig av om bruken er autorisert av Kunden og Kunden er ansvarlig for å opprettholde konfidensialitet rundt Kundens konto login og passord. Kunden plikter å varsle Symantec umiddelbart dersom det skjer uautorisert bruk av Kundens konto.

4. Ansvar for Innhold av Kommunikasjon på Kundens Konto.

4.1 Symantec gir ingen garanti for besørgelsen av EIM Tjenesten utover det som er sagt uttrykkelig i denne Avtale. Symantec garanterer ikke 100% Virus eller Spam påvisnings rate og Symantec vil derfor ikke akseptere ansvar for noen skade eller tap som resulterer direkte eller indirekte fra mangler ved EIM i forhold til å oppdage Virus eller Spam eller for feilaktig identifisering av en beskjed som mistenkelig Virus eller Spam, som deretter viser seg å ikke være det.

4.2 Symantec gir ingen uttrykkelig eller underforstått garanti vedrørende tilgjengelighet av EIM, eller muligheten for EIM til holde på alle data.

4.3 Symantec fremhever at konfigurering av EIM er fullstendig kontrollert av Kunden. I visse land vil det være nødvendig å innhente samtykke fra individuell personell. Symantec råder Kunden til alltid å undersøke lokal lovgivning før implementering av EIM. Symantec vil ikke akseptere ansvar for sivile krav eller straffeansvar som kan pådras av Kunden som følge av drift av EIM.

5. Forpliktelser

5.1 Kunden aksepterer at den ikke vil:

5.1.1 overføre eller lagre via POD eller EIM noen data, tekst, video, audio, software, eller annet innhold som er ulovlig;

5.1.2 overføre eller lagre via POD eller EIM noe innhold som krenker noe patent, varemerke, copy right, offentlige rettigheter, eller annen immateriell rettighet;

5.1.3 overføre eller lagre noe innhold som krenker gjeldende lokal, statlig, nasjonal, eller internasjonal lovgivning som kan gi grunnlag for sivilt eller straffeansvar;

5.1.4 overføre eller lagre noen uanmodet reklame innhold, annonse materiell, Spam, "spim," chain-letters, eller annet slik inntrengende anmodning;

5.1.5 bruke POD eller EIM til offentlig broadcast, overføre, eller vise innhold for annet formål enn selskaps kommunikasjon;

5.1.6 bruke POD eller EIM til forsettlig å overføre innhold som inkluderer et Virus, worm, cancelbot, tidsbombe, Trojan-horse, sniffer, eller annen kode som er designet for å skaffe informasjon om andre brukere eller ødelegge funksjonalitet eller tilgjengelighet av noe computer program, database, EIM eller annen Internett host; eller

5.1.7 kamuflere POD Brukerens identitet for spoofing, forging headers, bruke tredjepart relayers, eller på annen måte gjøre opprinnelsen uklar for overført innhold, inklusiv men uten begrensning, å utgi seg for annen person eller selskap.

6. Kompatibilitet

6.1 Kunden vil motta kompatibilitet funksjonalitet iht Klausul 2 ovenfor (se CONNECT pakke ovenfor). Symantec gir ingen garanti knyttet til muligheten for EIM til å fungere med noen IM provider inklusiv, men ikke begrenset til, AOL, MSN og Yahoo!.

7. Kun USA Datalagring

7.1 KUNDEN BES VÆRE OPPMERKSOM PÅ AT ALLE BESKJEDER VIL BLI LAGRET I USA OG SYMANTEC KAN IKKE AKSEPTERE NOE ANSVAR FOR NOE BRUDD PÅ GJELDENDE LOVGIVNING ELLER REGLER. KUNDEN AKSEPTERER AT KONFIGURERING OG BRUK AV EIM ER FULLSTENDIG UNDERLAGT KUNDENS KONTROLL OG VALG. Symantec kan ikke akseptere ansvar for sivile krav eller straffeansvar som Kunden kan pådra seg som følge av anvendelsen av EIM. Kunden må ta dette inn i vurdering ved konfigurering EIM.

8. Loggføring og samsvar

8.1 Kunden kan velge å loggføre direktemeldinger som passerer gjennom EIM-tjenesten, forutsatt at kunden betaler prisen for loggføringsfunksjonen.

8.2 Symantec sender loggfiler til kunden hver dag slik at kunden om ønskelig kan oppbevare slike logger i et kompatibelt arkiv.

8.3 Symantec oppbevarer logger i tre (3) år, deretter blir loggene permanent slettet. Kundens autoriserte representant kan via skriftlig anmodning be om (i) en kopi av slike logger eller (ii) sletting av slike logger når som helst før utgangen av ovennevnte treårsperiode.

8.4 Kunden gjøres oppmerksom på at administrasjonskonsollen gjør kunden i stand til å deaktivere loggføring etter gruppe eller delgruppe når som helst, og at loggene derfor kan utgjøre en ufullstendig historikk for bruken av EIM-tjenesten.

8.5 Symantec vil gi seks (6) måneders skriftlig varsel dersom selskapet har til hensikt å innstille leveranse av og støtte for EIM-tjenesten. Når denne varslingsperioden utløper, vil EIM-tjenesten opphøre.

8.6 Ved opphør av EIM-tjenesten kan kunden kreve retur eller sletting av sine logger. Hvis kunden ikke fremlegger sine ønsker innen nitti (90) dager etter opphøret, vil Symantec slette loggene permanent.

8.7 Kunden forstår og samtykker i at Symantec ikke under noen omstendighet kan opptre som en tredjeparts nedlaster i forbindelse med overholdelse av krav fra amerikanske SEC.

9. Software Lisens

9.1Tilståelse av Lisens

Iht Avtalens vilkår og betingelser, gir Symantec Kunden en ikke-eksklusiv, ikke-overførbar rett til å installere og bruke Software

for EIM Tjenesten kun for Kundens egen interne business drift ("Software" betyr ethvert Symantec software program for EIM Tjenesten i objekt kode format lisensiert av Symantec og underlagt vilkårene i Avtalen, inklusiv uten begrensning nye utgivelser eller oppdateringer som besørges iht avtalen). Alle immaterielle rettigheter til Software er og skal fortsatt være Symantecs eiendom (og/eller dets leverandører). Software er lisensiert av Symantec, ikke solgt. Kunden erkjenner at Software og all relatert informasjon, inklusiv uten begrensning oppdateringer, er beskyttet eiendom for Symantec og dets leverandører. Kunden er fullt ut ansvarlig for enhver End Users oppfyllelse av eller brudd av vilkår i denne Avtalen. Kunden skal umiddelbart varsle Symantec om evt uautorisert bruker eller brudd på andre vilkår i denne lisens.

9.2. Kopiering og Bruker Restriksjoner

Kunden kan nedlaste og installere Software underlagt følgende betingelser:

9.2.1. Kunden kan ikke nedlaste eller installere Software til flere enn antallet End User lisenser som er lisensiert av Kunden ("End User" skal bety fysiske computere hvor software er installert).

9.2.2. Kunden kan kopiere Software i rimelig utstrekning for nødvendig back-up, arkivering eller disaster recovery formål. Skriftlig Dokumentasjon kan reproduseres av Kunden kun for intern bruk ("Dokumentasjon" betyr Symantecs bruker guides og/eller manualer for drift av Software som er inkludert med nedlastet Software.).

9.2.3 Kunden kan ikke, heller ikke tillate noen tredjepart å: (i) dekompilere, ta fra hverandre, eller reverse engineer Software, bortsett fra når det er uttrykkelig lov iht gjeldende lovgivning, med mindre Symantecs har skriftlig gitt forhåndssamtykke; (ii) fjerne noen produkt identifikasjon eller varsel om beskyttede rettigheter; (iii) lease, låne bort eller bruke Software for tidsdeling eller tjeneste bureau formål; (iv) modifisere, oversette, tilpasse eller lage avledede works fra Software, eller (v) på annen måte bruke eller kopiere Software, utover det som er uttrykkelig avtalt i denne Avtale.

9.3. Overføring av Rettigheter

Kunden kan ikke overføre, overdra eller delegere software lisens under denne Avtale uten skriftlig forhåndssamtykke fra Symantec. Slik overførsel, overdragelse eller delegasjon i strid med foregående vil være ugyldig.

9.4. Begrenset Garanti og Ansvarsfraskrivelse

9.4.1 Symantec garanterer at nedlastet Software i all hovedsak vil være i samsvar med Symantecs gjeldende Dokumentasjon.

9.4.2 Foregående garanti vil ikke gjelde hvis: (i) Software ikke anvendes i henhold til Avtalen eller Dokumentasjon; (ii) Software eller noen del av den har blitt modifisert av noen andre enn Symantec; eller (iii) en feil i Software har blitt forårsaket av noe av Kundens utstyr eller tredjepart software.

9.4.3 SYMANTEC GARANTER IKKE AT DRIFTEN AV SOFTWARE VIL BE UAVBRUTT ELLER FEILFRI. SYMANTEC FRASKRIVER SEG UTTRYKKELIG ALLE GARANTIER (WARRANTIES) AV NOE SLAG, UAVHENGIG AV UTTRYKKELIG, UNDERFORSTÅTT ELLER PÅ ANNEN MÅTE, INKLUSIV MEN IKKE BEGRENSET TIL, GARANTI FOR SALGSMULIGHET, TILFREDSSTILLENDE KVALITET, ELLER ANVENDELIGHET FOR ET BESTEMT FORMÅL.

9.5. Avslutning

Ved avslutning av EIM Tjenesten eller Avtalen, opphører Kundens rett til bruk Software med umiddelbar effekt og Kunden skal umiddelbart returnere til Symantec eller ødelegge alle kopier av Software og Dokumentasjon.

Bilag 10 – Symantec MessageLabs Policy Based Encryption.cloud

1. Tjeneste Beskrivelse

1.1 Symantec MessageLabs Policy Based Encryption.cloud Tjenesten ("PBE") gir mulighet for å sende og motta kryptert Email basert på Kundens email sikkerhet policy.

1.2 For å motta PBE, må Kunden også abonnere på følgende Tjenester:

- **Symantec MessageLabs Email Boundary Encryption.cloud ("BE**") som beskrevet i Vedlegg 2 Bilag 5; og
- **Symantec MessageLabs Email Content Control.cloud ("Email CC")** som beskrevet i Vedlegg 2 Bilag 4.

1.3 PBE besørger følgende funksjonalitet:

- Mulighet for bruk av Email CC til å definere utgående krypteringspolicy for Email;
- Kryptert Email levering til eksterne mottakers innboks;
- Mottaker oppnår tilgang til kryptert Email via en sikker web portal;
- Mottaker kan ha tilgang til sikker web portal for å svare på Emailen i kryptert format.

2. PBE Funksjoner

2.1 PBE tillater Kunden å sende en kryptert Email direkte inn i en mottakers innboks uten behov for mottaker til nedlaste software.

2.2 Kunden kan konfigurere krypteringsmetode til enten Push eller Pull. For Symantec MessageLabs Policy Based Encryption.cloud (Z) ("PBE Z"), Email CC regel bestemmes mellom Push eller Pull. For Symantec MessageLabs Policy Based Encryption.cloud (E) ("PBE E"), default krypteringsmetode er Pull, men kan endres til Push av mottaker ved nedlasting av Sikker Reader funksjonalitet innen mottakers sikker web portal.

2.2.1 "PBE Push" varianten av PBE Tjenesten sender mottaker en email varsling med original Email lagret som et kryptert vedlegg. Etter første registrering online, vil mottaker ha mulighet til å se dekryptert Email offline ved å bruke en Java applikasjon på deres desktop.

2.2.2 "PBE Pull" variant av Tjenesten sender mottaker en email varsling. Mottaker har mulighet for å se på dekryptert Email online via en sikker SSL sesjon i deres browser når de logger på til en sikker web portal og inngir deres passord.

2.3 PBE gir også mulighet for mottaker til å gå inn på en sikker web portal og besvare en kryptert Email i kryptert format.

2.4 Kunden kan merke portalen som mottakere bruker til å lese deres krypterte Email (for eksempel ved å inkludere Kundens logo og support telefon nummer).

2.5 Mottaker av en kryptert Email kan også send en helt ny Email til noen av Kundens PBE Brukere.

2.6 Hvis Kunden abonnerer på PBE E, vil en tredjepart Outlook Plug-In være tilgjengelig, som legger til et "kryperingsikon" til mottakers Outlook verktøylinje. Kunden forstår og godtar at Symantec ikke er ansvarlig for slik tredjepart software.

2.7 Hvis Kunden abonnerer på PBE E er følgende tilleggsfunksjoner tilgjengelig:

a) en mottaker kan velge språk for mottakers sikker web portal og varslings email fra en liste med mulige språkvalg;

b) mottakere kan logge inn på deres konti uten å åpne en bestemt beskjed, og selv om de ikke har noen aktive beskjeder;

c) mottakere kan se på alle deres tidligere beskjeder (som ikke har blitt varig slettet) i deres innboks, inklusiv beskjeder som de har sendt;

d) hvis man bruker Pull metode, så vil en beskjed laget i web portalen kunne ha flere mottakere forutsatt at slike mottakere deler et domene som Brukeren tidligere har mottatt en sikker email fra;

e) hvis man bruker Push metode, så kan mottakere svare til en hver email adresse under samme domene;

f) første varsling til nye Brukere er tilgjengelig i flere språk;

g) Det er mulig å bruk tredjeparts sertifikat/ krypteringsnøkkel for utgående Email ved å anvende mottakers offentlig nøkkel og dekryptere en innkommende Email ved å bruke mottakers privat nøkkel, isteden for default sertifikat/nøkler som produseres av PBE Tjenesten.

3. Anskaffelse, Fakturering og Endringsordre

3.1. Symantec vil belaste for PBE fra datoen Symantec bekrefter at kundens nettverk er teknisk i stand til å støtte PBE ("dato for teknisk godkjenning").

3.2 Paragraf 5.2 i Vedlegg 1 gjelder ikke for PBE. Symantec vil søke å levere PBE-bestillinger og PBE-endringsanmodninger innen 4 uker etter dato for teknisk godkjenning, forutsatt at kunden har utført alle nødvendige forberedelser.

3.3 Kunden aksepterer å besørge alle nødvendig ressurser, informasjon, og tillatelser som er påkrevd, og å aktivere eller korrigere dets DNS mail tjeneste for tilkoblingsmulighet til PBE.

3.4 Kunden kan endre merking (branding) av portal maksimum to ganger pr. år.

4. Konfigurering

4.1 Kunden er ansvarlig for å implementere konfigurering av PBE iht Kundens behov. Kunden konfigurerer PBE via ClientNet ved å velge tilgjengelig muligheter i Email CC Tjenesten.

4.2 Symantec fremhever at konfigurering av PBE er fullstendig underlagt Kundens kontroll og at nøyaktighet ved slik konfigurering vil avgjøre nøyaktigheten av PBE. Symantec kan således ikke akseptere ansvar for noen skade eller tap som resulterer direkte eller indirekte fra mangler ved PBE i forhold til å oppfylle Kundens krypteringsforpliktelser.

5. Tjeneste Parametre

5.1 De følgende begrensninger gjelder PBE:

5.1.1 Antall sikre Emailer Kunden kan sende pr. måned ved å anvende PBE Z kan ikke overskride tre hundre (300) ganger Registeret Usage for PBE. Antall sikre Email Kunden kan sende pr. måned ved å anvende PBE E kan ikke overskride fire hundre og åtti (480) ganger Registeret Usage for PBE. Når det sendes til flere mottakere, vil hver unike adresse bli talt som en sikker Email. I tilfelle Kunden overskrider antall tillatte sikre Email pr. måned, vil Symantec følgelig øke Registeret Usage. Hvis Symantec øker Registeret Usage, kan Symantec etter eget valg utstede tilleggsfaktura og/eller gjøre justeringer i senere faktura for å dekke vederlaget for økt Registeret Usage på pro-rata basis for gjenstående del av gjeldende fakturaperiode

5.1.2 Email dirigert gjennom PBE Z er begrenset til en maksimum størrelse på femti megabytes (50 MB) pr. Email når komprimert. Email dirigert gjennom PBE E er begrenset til en maksimum størrelse på femti megabytes (50 MB) pr. Email etter kryptering.

5.1.3 Email Ventetid Service Level i Service Level Agreement skal ikke gjelde PBE.

5.1.4 Minimums antall for Brukere av PBE Z er 50 Brukere. Første og senere ordre for PBE Z kan plasseres for minimum blokker av 50 Brukere eller forøkelser av 10 Brukere for ordre som overskrider 50 Brukere.

5.1.5 PBE KAN BARE ANVENDES I FORBINDELSE MED BE OG EMAIL CC TJENESTE OG KAN IKKE ANVENDES SOM EN STANDALONE TJENESTE. HVER INDIVIDUELLE PBE BRUKER MÅ VÆRE EN EMAIL CC BRUKER.

6. Vilkår og Betingelser

6.1 Bruk av kryptert tjeneste er i visse land underlagt lovgivning. Kunden rådes til å alltid undersøke relevant lovgivning forut for anvendelse av PBE. Symantec kan ikke akseptere ansvar for sivile krav eller straffeansvar som Kunden kan pådra seg som følge av anvendelsen av PBE.

Bilag 11- Symantec Email Continuity.cloud ("EC")

1. EC Oversikt

1.1 EC er et standby messaging system for Microsoft Exchange og Lotus Notes miljøer. EC vil synkronisere nøkkel system og Bruker informasjon inklusiv, men ikke begrenset til, Email kataloger og individuell Brukeres personlige kontakter. Kunden kan også konfigurere EC til supportere BlackBerry® enheter gjennom trådløs videresending ved å anvende BlackBerry® Web Client eller BlackBerry® Internett Tjeneste, og en integrert Outlook opplevelse for Brukere på Outlook 2003 Cached Mode eller Outlook 2007 Cached Mode gjennom en installert Outlook Extension.

1.2. *Supporterte Versjoner*: Microsoft Exchange 5.5, Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007, Lotus Notes Versjon 6, Lotus Notes Versjon 7.

1.3 *Supporterte Versjoner for Outlook Extension*: Microsoft Outlook 2003 i Cached Mode; Microsoft Outlook 2007 i Cached Mode.

1.4 Kunden har ansvaret for å forsyne og vedlikeholde nødvendig maskinvare og programvare (slik det beskrives på leveranseskjemaet).

2. EC Tjeneste Beskrivelse

2.1. A*ktivering.* Kunden kan anmode om aktivering av EC via telefon til Symantec support team eller via Email Management Tjenesten ("EMS") portal. Ved aktivering av EC, skal Kunden motta varsel via SMS til utpekte mobiltelefonnumre og personlige email adresser. På det tidspunkt vil EC begynne å motta og sortere innkommende Email, og filtrere dem (iht Klausul 4.4 nedenfor) i samsvar med andre Symantec Email Tjenester som Kunden abonnerer på (f.eks. Emailen AV Tjeneste), og dirigere dem til de bestemte Bruker mailbokser. EC vil besørge lagring av Email trafikk sendt og mottatt i løpet av aktivering for inntil tretti (30) dager etter deaktivering for å gjøre Kunden i stand til å integrere slik Email inn i dets primær mail system dersom det er ønskelig.

2.2 *Retensjon.* Kunden har ansvaret for å angi for hvilke Brukere Email skal beholdes og spesifisere lagringsperiode for hver slik Bruker. Oppbevart Email vil bli slettet ved tidligste alternativ av følgende (a) utløp av angitt lagringsperiode for slik Bruker eller (b) avslutning av EC. Kunden er pålagt å kjøpe tilstrekkelig lagring for å oppfylle dets lagringsbehov i henhold til klausul 5.1 nedenfor.

2.3 *Autentisering Manager.* Kunden kan utvide Kundens sikkehetspolicy for Microsoft Active Directory Autentisering til EC ved å bemyndige Brukere til å logge inn i deres EC mailbokser ved å anvende deres Windows passord, og derved fjerne behovet for et separat EC passord. Windows autentisering krever tilgjengelighet av en Windows domene kontroll med tilgang for Autentisering Manager som på tidspunktet for EC aktivering kan autentisere Brukere som prøver å logge seg på EC mailbokser. Supporterte Versjoner: Microsoft Exchange 2000, Microsoft Exchange 2003, Microsoft Exchange 2007

2.4 Minimum antall av Brukere av EC som kan kjøpes av Kunden er største alternativ av følgende (a) antall Brukere som er lik antall mailbokser i Kundens Microsoft Exchange organisasjon eller (b) ti (10) Brukere.

3. Reservert.

4. Konfigurering

4.1 *Delvis aktivering*: For visse email systemer/versjoner (Microsoft Exchange 2000, 2003 og 2007 miljøer), er det mulig å aktivere EC for deler av Kundens miljø (en eller flere individer, servere og/eller lokasjoner), "Delvis aktivering", for å håndtere flere lokale email avbrudd.

4.2 *Aktivering*: EC abonnement gir Kunden rett til tjuefire (24) aktiveringer pr. år, hver varer for en periode på inntil tolv (12) sammenhengende timer ("Inkludert Aktiveringer"). (For illustrasjonsformål, vil en enkel aktivering som varer seks (6) timer telle som en (1) aktivering, og en enkel aktivering som varer nitten (19) timer vil telle som to (2) aktiveringer.) I tilfelle Kunden har anvendt dets kvote av inkludert Aktiveringer, kan Kunden kjøpe tilleggsaktiveringer (hver med varighet for en periode på inntil tolv (12) sammenhengende timer) fra Symantecs til enhver tid gjeldende rater.

4.3 System Testing: System Testing skal inkludere (a) en (1) kvartalsvis test av EC for alle Brukere, som varer inntil fire (4) timer, og (b) for Microsoft Exchange 2000, Microsoft Exchange 2003 eller Microsoft Exchange 2007 miljøer, ubegrenset delvis testing av inntil ti prosent (10%) av Brukere. Kunden må avtale disse tidspunkt for tester med Symantec ikke senere enn sju (7) virkedager forut for Kundens ønskede test dato.

4.4 **KUNDEN ERKJENNER OG AKSEPTERER AT NÅR KUNDEN ER I EN AKTIVERT TILSTAND, OG KUNDEN DA SENDER EMAIL TIL, ELLER MOTTAR EMAIL FRA EN ANNEN ORGANISATION SOM OGSÅ ER I EN AKTIVERT TILSTAND, VIL EMAIL PASSERE SYMANTEC INNKOMMENDE OG UTGÅENDE SKANNING TJENESTER SOM KUNDEN ABONNERER PÅ**.

4.5 Hvis Kunden bruker Emailen AV, Email AS, Email CC og/eller Email IC Tjeneste, kan Symantec konfigurere failover routing for Kundens email til EC miljø innen ClientNet. Slik failover routing vil bli anvendt når EC tjenesten er aktivert.

4.6 **HVIS KUNDEN IKKE BRUKER EMAIL AV, EMAIL AS, EMAIL CC ELLER EMAIL IC, ER DET KUNDENS ANSVAR Å KONFIGURERE OG TESTE FAILOVER ROUTING FOR KUNDENS EMAIL TIL EC MILJØ. DISSE FAILOVERS MÅ LAGES IHT SYMANTECS INSTRUKSJONER I LØPET AV ANSKAFFELSESPROSESSEN OG MÅ DERETTER VEDLIKEHOLDES. I TILFELLE KUNDEN UNNLATER Å LAGE ELLER VEDLIKEHOLDE SLIK FAILOVERS, ERKJENNER KUNDEN OG AKSEPTERER AT EMAIL IKKE KAN BLI DIRIGERT TIL EC.**

5. Muligheter

5.1 *Symantec Email Continuity.cloud Storage Option*.

5.1.1 Kunden er pålagt å kjøpe tilstrekkelig lagring for lagringsformål.

5.1.2. Hvis Kunden abonnerer på følgende Symantecs tjenesteknipper ("bundles"); Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email & Web Safeguard.cloud eller Symantec MessageLabs Ultimate Safeguard.cloud bundles, skal Tjenesten omfatte maksimum 0.7GB ny email-lagring pr. Bruker pr. år for kombinasjonen av Tjenestene EC og Symantec Email Continuity Archive.cloud. Hvis Kundens nye email lagring overskrider slik tillatt lagringsmengde, skal Kunden være pålagt å kjøpe tilstrekkelig lagring for Tjenestene til Symantecs til enhver tid gjeldende priser.

5.1.3. Hvis Kunden ikke abonnerer på et av "tjenesteknippene" som er opplistet i Klausul 5.1.2, skal ingen lagring være inkludert i pr. Bruker prisen og Kunden plikter å kjøpe tilstrekkelig lagring for Tjenestene til Symantecs til enhver tid gjeldende priser.

5.1.4. Når Kunden er pålagt å kjøpe tilleggslagring, skal Symantec sende tilleggsfaktura og/eller gjøre justering I etterfølgende faktura for å inndekke tilleggsvederlaget for økt lagring på en pro-rata basis for gjenstående del av gjeldende faktura periode.

5.2 *Symantec Email Continuity.cloud Wireless Option (Trådløst).*

5.2.1 Hvis Kunden abonnerer på Symantec Email Continuity.cloud Wireless Option, kan system administratorer anskaffe bestemte BlackBerry® enheter administrert av deres selskap RIM BlackBerry® Enterprise Servere (BES). Når EC er aktivert, vi anskaffede BlackBerry® enheter fortsette å sende og motta Email ved kommunikasjon med EMS, via en sikker kanal etablert av BES server.

5.2.2. Supporterte Versjoner: Microsoft Exchange 2000, Microsoft Exchange 2003 eller Microsoft Exchange 2007; BlackBerry® Enterprise Server versjon 4.0 (eller over); BlackBerry® Handheld Devices firmware versjon 4.1 (eller over).

6. EC Vilkår og Betingelser

6.1 INGEN EMAIL KONTINUITET TJENESTE KAN GARANTERE EN 100% SYNKRONISERING OG SÅLEDES KAN SYMANTEC IKKE AKSEPTERE ANSVAR FOR NOEN SKADE ELLER TAP SOM RESULTERER DIREKTE ELLER INDIREKTE FRA MANGLER VED EC I FORHOLD TIL Å SYNKRONISERE EMAIL SYSTEMER.

6.2 Symantec fremhever at konfigurering av EC er fullstendig underlagt Kundens kontroll. Symantec anbefaler at Kunden har en akseptabel computer bruker policy (eller tilsvarende) på plass. I visse land vil det være nødvendig å innhente samtykke fra individuelt personell. Symantec råder Kunden til alltid å sjekke lokal lovgivning forut for at EC tas i bruk. Symantec kan ikke akseptere ansvar for sivile krav eller straffeansvar som Kunden kan pådra seg som følge av anvendelsen av EC.

7. Software Lisens for EC

7.1 Tilståelse av Lisens

Iht vilkår og betingelser i denne Avtalen, gir Symantec Kunden en ikke-eksklusiv, ikke-overførbar rett til installere og bruke gjeldende Software for EC kun for Kundens egen interne forretningsdrift. ("Software" betyr ethvert Symantec software program for EC i objekt kode format lisensiert av Symantec og underlagt vilkårene i Avtalen, inklusiv uten begrensning nye utgivelser eller oppdateringer som siden besørges iht avtalen).

Alle immaterielle rettigheter til Software er og skal være eiendommen til Symantec (og/eller dets leverandører). Software er lisensiert av Symantec, ikke solgt. Kunden erkjenner at Software og all relatert informasjon, inklusiv uten begrensning oppdateringer, er eiendommen til Symantec og dets leverandører. Kunden er fullt ut erstatningsansvarlig for hver Brukers overholdelse av eller brudd på vilkår i denne Avtale. Kunden skal med umiddelbar effekt varsle Symantec i tilfelle uautorisert bruk eller overtredelse av vilkår i denne lisens.

7.2. Kopiering og Bruker restriksjoner

Kunden kan nedlaste og installere Software underlagt de følgende betingelser:

7.2.1. Kunden kan ikke nedlaste eller installere Software til flere enn det antall End User lisenser lisensiert av Kunden. ("End User" skal bety fysiske computere hvor software er installert).

7.2.2. Kunden kan kopiere Software i rimelig utstrekning for nødvendig back-up, arkivering eller disaster recovery formål. Skriftlig Dokumentasjon kan reproduseres av Kunden kun for intern bruk. ("Dokumentasjon" betyr Symantecs bruker guides og/eller manuals for drift av Software som er inkludert med nedlastet Software).

7.2.3 Kunden kan ikke, heller ikke tillate noen tredjepart å: (i) dekompilere, ta fra hverandre, eller reverse engineer Software, med unntak for når dette er uttrykkelig tillatt av gjeldende lovgivning,, uten å innhente Symantecs skriftlige forhånds samtykke; (ii) fjerne noen produkt identifikasjon eller varsel om beskyttede rettigheter; (iii) lease ut, leie ut, eller bruke Software for tidsdeling eller tjeneste byrå formål; (iv) modifisere oversette, tilpasse eller lage avledede produkter av Software, eller (v) på annen måte bruker eller kopiere Software med unntak for det som uttrykkelig er lovlig iht denne Avtale.

7.3. Overføring av Rettigheter

Kunden kan ikke overføre, overdra eller delegere software lisens under denne Avtale uten skriftlig forhånds samtykke fra Symantec. Dersom slik overføring, overdragelse eller delegasjon skjer i strid med foregående, vil den være ugyldig.

7.4. Begrenset Garanti og Ansvarsfraskrivelse

7.4.1 Symantec forsikrer at Software ved nedlasting i all vesentlighet vil være i samsvar med Symantecs gjeldende Dokumentasjon.

7.4.2 Foregående garanti vil ikke gjelde hvis: (i) Software ikke anvendes i henhold til denne Avtalen eller Dokumentasjon; (ii) Software eller noen del av denne har blitt modifisert av noen annen enn Symantec; eller (iii) en feil ved Software har blitt forårsaket på grunn av Kundens utstyr eller tredjepart software.

7.4.3 SYMANTEC GARANTERER IKKE AT DRIFTEN AV SOFTWARE VIL VÆRE UAVBRUTT ELLER FEILFRI. SYMANTEC UTTRYKKELIG FRASKRIVER SEG ET HVERT ANSVAR, UTTRYKT ELLER UNDERFORSTÅTT ELLER PÅ ANNEN MÅTE, INKLUSIV MEN IKKE BEGRENSET TIL, ANSVAR FOR FORRETNINGSMULIGHET, TILFREDSSTILLENDE KVALITET, ELLER FORMÅLSEGNETHET

7.5. Avslutning

Ved avslutning av EC, VIL alle Kundens rettigheter til bruk AV Software gitt iht Avtalen bortfalle med umiddelbar effekt og Kunden skal umiddelbart returnere til Symantec eller ødelegge alle kopier av Software og Dokumentasjon.

Bilag 12 - Schemus Verktøy

1.1 Schemus Verktøy er software som synkroniserer data mellom Kundens katalog server og Symantec tjeneste som Kunden abonnerer på.

1.2 Schemus Verktøy er lisensiert til Kunden av Schemus og Begrenset ved en separat End User lisensavtale ("Third Party EULA").

1.3 Kunden forstår og godtar at tilgang til og bruk av Schemus Verktøy er forutsetter at Kunden aksepterer og oppfyller vilkår og betingelser i Third Party EULA (kopi av denne er tilgjengelig fra Symantec etter anmodning).

1.4 Schemus Verktøy er kontrollert teknologi som er underlagt gjeldende import og eksport lovgivning og regler som ytterligere er detaljert i eksport kontroll bestemmelser i den "Generelle" del av Avtalen. **KUNDEN FORSTÅR OG GODTAR AT DEN VIL MÅTTE SIGNERE EN ERKLÆRING OM OPPFYLLELSE (KOPI ER TILGJENGELIG FRA SYMANTEC ETTER ANMODNING) (I) FORUT FOR SOFTWARE NEDLASTING, (II) FORUT FOR LISENS NØKKEL UTSTEDELSE OG (III) ÅRLIG DERETTER HVIS ANMODET AV SYMANTEC**.

1.5 Symantec besørger ingen tilleggsgaranti (uansett utrykkelig, underforstått, lovmessig eller på annen måte) med hensyn til Schemus Verktøy. I tilfelle mangel ved Schemus Verktøy, vil Symantec gjøre kommersielt rimelige anstrengelser for å hempe til å finne kilden til problemet, og hvor relevant, eskalere problemet til Schemus Limited.

1.6 Symantecs maksimums ansvar overfor Kunden i relasjon til Schemus Verktøy er begrenset til en sum som er lik det faktiske beløp betalt av Kunden til Symantec for Schemus Verktøy eller £250 (eller €350 hvis Kunden betaler i Euros), herav det høyeste av de to beløp.

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

1 Oversikt

1.1. Kunden plikter å synkronisere dets bruker katalog med Symantec for å lage en liste av Active Directory brukernavn og korresponderende instant beskjed (IM) brukernavn innen ClientNet. En "Intern Bruker" er en bruker som er kjent i Kundens katalog og opplastet inn i IMSS administrative interface. En "Ekstern Bruker" er en bruker som er ukjent i Kundens katalog og/ikke er opplastet inn i IMSS administrative interface.

1.2. Kunden er også pålagt å gjøre brannmur endringer for å styre dets IM konversasjoner via Symantec.

1.3. Så snart IMSS har blitt konfigurert i henhold til klausuler 1.1 og 1.2 ovenfor, vil IMs som går fra Interne Brukere til Eksterne Brukere og vice versa dirigeres gjennom IMSS for skanning ved bruk av ledende produkts inklusiv Symantecs egen heuristiske skanner, Skeptic™.

1.4. IMSS er kun i stand til å skanne visse versjoner av offentlig IM klienter. Symantec skal publisere en liste av supporterte versjoner av offentlig IM klienter på ClientNet. Kunden erkjenner og aksepterer at Symantec kan oppdatere og endre denne listen på en jevnlig basis uten varsel.

1.5. Hvis en **innkommende** IM:

1.5.1 Antas å inneholde et virus eller annen ødeleggende kode, vil den bli blokkert;

1.5.2 inneholder en URL for en web side hvor et virus eller annen ødeleggende kode har blitt oppdaget, skal tilgang til slik web side bli nektet.

1.6. IMSS også besørger grunnleggende anti-Phishing funksjonalitet som vil blokkere **innkommende** IMs som antas å være Phishing angrep.

1.7. IMSS er i stand til skanne visse versjoner av Word, Excel og PowerPoint dokumenter, men ikke annet vedlegg.

1.8. IMSS er ikke i stand til skanne kryptert IMs.

2. Reservert.

3. IMSS Innhold Kontroll

3.1. IMSS tillater Kunden å konfigurere dets egne regler basert på innhold filter strategi for innkommende og utgående IMs.

3.2. Kunden er ansvarlig for å implementere konfigureringsmuligheter i samsvar med Kundens akseptable computer bruker policy (eller tilsvarende) via ClientNet. Regler kan bli konfigurert på gruppe eller individuell basis. Endringer som gjøres av Kunden i regler vil bli effektive innen fire (4) timer.

3.3. Muligheter er tilgjengelig for å definere handlinger som skal tas ved påvisning av kontrollert innhold innen en IM. Disse muligheter er detaljert på ClientNet og i gjeldende versjon av administrator veiledningen.

3.4. Kunden kan gjennomgå resultatene av dets regler via ClientNet i form av daglig, ukentlig, månedlig og årlig sammendrag organisert både etter regel og etter Bruker.

4 Logger og Lagring

Hvis Kunden har muliggjort logging funksjonalitet, vil Symantec daglig sammenstille logger av IMs skanning. Hver logg skal inkludere dato og tids angivelse, innhold, og navn på filer som er overført. Noen logger som ikke er i stand til å bli sendt Kunden skal lagres for en periode på tretti-en (31) dager og deretter ødelegges.

4.2. Kunden kan også konfigurere IMSS til å sende en kopi av hver IM til Kundens kompatibel arkiv eller lagringsløsning.

5 Varslinger

5.1 Kunden kan konfigurere IMSS til å sende en automatisk varsling:

5.1.1 til avsender og påtenkt mottaker i tilfelle en IM er blokkert fordi den antas å inneholde et virus, Phishing attakk eller kontrollert innhold; eller

5.1.2 til mottaker hvis tilgang til en webside nektes fordi den antas å inneholde et virus eller ødeleggende innhold.

5.2. Kunden kan aktivere, tilpasse og deaktivere varsling ved å anvende ClientNet.

6 Support

6.1 Support inkluderer:

6.1.1 Gjennomgang av IMSS interface inklusiv en tjeneste beskrivelse og Q&A sesjon. (Dette inkluderer ikke assistanse til å lage regler eller analyse av effektivitet av regler);

6.1.2 Administrator Veiledning;

6.1.3 Bruker Guide.

7 IMSS Vilkår og Betingelser

7.1 Veiledende innhold, kontroll ordlister og template regler som leveres av Symantec kan inneholde ord som kan ansees å være støtende. Kunden aksepterer at Symantec kan sammenstille og publisere default ordlister ved å anvende ord som tas fra Kundens' tilpassede ordlister.

7.2 Kunden erkjenner at IMs kan inneholde personlig identifiserbar informasjon og at logging og avskjæring av IMs således kan innebære prosessering av personlig data. Videre, erkjenner Kunden at IMSS er en konfigurerbar tjeneste og at Kunden alene er ansvarlig for å konfigurere IMSS i henhold til Kundens akseptable computer bruker policy (eller tilsvarende) og all gjeldende lovgivning eller regler. Følgelig råder Symantec Kunden til alltid å undersøke lokal lovgivning før implementering av IMSS, og til å sikre at den, og alle dets ansatte, er kjent med og overholder forpliktelsene de har med hensyn til databeskyttelse og privatliv lovgivning og/eller regler i tilknytning til Kundens bruk av IMSS. I visse land vil det være nødvendig å innhente samtykke fra individuell personell forut for avskjæring og logging av IMs. Som et minimum, skal Kunden implementere, med rimelig og minimal tilpassing, Symantecs default varsling for IMSS til de som bruker noe kommunikasjonssystem dekket av IMSS som (i) indikerer at kommunikasjon overført gjennom slikt system vil bli logget og kan bli avskåret, (ii) indikerer formålet med slik logging og avskjæring, og (iii) innhenter bruker samtykke til slik logging og avskjæring. Kunden kan oversette men skal ikke på annen måte modifisere språk vedrørende punktene (i), (ii) og (iii) i foregående setning som del av tilpassingen av default varsling for IMSS. Symantec aksepterer ikke ansvar for sivile krav eller straffeansvar som kan pådras av Kunden som følge av Kundens drift av IMSS. Kunden skal holde Symantec skadesløs fra ethvert krav fra dets ansatte, noen tredjepart og/eller offentlig instans vedrørende avskjæring eller logging av IMs av Symantec eller Kundens manglende oppfyllelse av lovgivning og/eller regler.

7.3 KUNDENS BES VÆRE OPPMERKSOM PÅ DET FORHOLD AT IMS SOM GÅR IGJENNOM IMSS KAN BLI SKANNET OG LAGRES PÅ HARDWARE LOKALISERT I USA. FØLGELIG AKSEPTERER KUNDEN AT DEN MÅ TA ALLE FORHOLDSREGLER FOR Å (I) INFORMERE DETS ANSATTE, AGENTER OG KONTRAKTØRER SÅVEL SOM TREDJEPARTER SOM BRUKER KOMMUNIKASJONSSYSTEMET DEKKET AV IMSS OM DET FORHOLD AT INFORMATION, INKLUDERT MULIG PERSONLIG IDENTIFISERBAR INFORMATION OM INDIVIDER, SOM SENDES IGJENNOM IMSS KAN BE PROSESSERT I USA; OG (II) INNHENTE SAMTYKKE FRA SLIKE ANSATTE, AGENTER, KONTRAKTØRER OG TREDJEPARTER' TIL SLIK PROSESSERING FORUT FOR ELLER SAMTIDIG MED DRIFT OF IMSS AV KUNDEN. VIDERE, AT NOE PERSONLIG DATA SOM KUNDEN BESØRGER TIL SYMANTEC KAN BLI OVERFØRT TIL SYMANTECS TILKNYTTEDE SELSKAP OG/ELLER SUBKONTRAKTØRER SOM HANDLER PÅ VEGNE AV SYMANTEC. SLIKE TILKNYTTEDE SELSKAP ELLER SUBKONTRAKTØRER KAN VÆRE LOKALISERT I USA ELLER ANNET LAND SOM KAN HA MINDRE STRENG DATA BESKYTTELSES LOVLIVNING ENN LOVGIVNING I REGIONEN HVOR KUNDEN ER LOKALISERT, I HVILKET TILFELLE SYMANTEC VIL FORETA HANDLINGER SLIK AT INNSAMLET DATA, HVIS OVERFØRT, OPPNÅR ET ADEKVAT NIVÅ AV BESKYTTELSE. KUNDEN AKSEPTERER AT DEN VIL TA ALLE NØDVENDIGE FORHÅNDSREGLER FOR Å (I) INFORMERE ALLE DETS ANSATTE, AGENTER OG KONTRAKTØRER SÅVEL SOM TREDJEPARTER SOM HAR GITT PERSONLIG DATA SOM KUNDEN BESØRGER TIL

SYMANTEC OM DET FORHOLD AT DERES DATA KAN BLI PROSESSERT I SLIKE LAND; OG (II) INNHENTE SAMTYKKE FRA SLIKE ANSATTE, AGENTER, KONTRAKTØRER OG TREDJEPARTER' TIL SLIK PROSESSERING. SYMANTEC AKSEPTERER IKKE NOE ANSVAR FOR NOE KORRESPONDERENDE BRUDD PÅ GJELDENDE LOVGIVNING ELLER REGLER.

7.4 INTET SOFTWARE ELLER TJENESTE KAN GARANTERE EN 100% IM PÅVISNINGS RATE OG SYMANTEC KAN SÅLEDES IKKE AKSEPTERE ANSVAR FOR NOE TAP ELLER SKADE SOM RESULTERER DIREKTE ELLER INDIREKTE FRA MANGLER VED IMSS I FORHOLD TIL Å OPPDAGE SPAM, VIRUS, PHISHING ANGREP, ØDELEGGENDE KODE, BLOKKERT URLs ELLER KONTROLLLERT INNHOLD, ELLER FOR IMSS FEILAKTIGE IDENTIFISERING OM AT IM INNEHOLDER SPAM, VIRUS, PHISHING ANGREP, ØDELEGGENDE KODE, BLOKKERT URLs ELLER KONTROLLLERT INNHOLD. Videre, konfigurering av IMSS innhold kontroll regler er fullstendig underlagt Kundens kontroll og nøyaktighet ved slik konfigurering vil påvirke nøyaktigheten av IMSS.

Bilag 14 – Symantec Email Continuity Archive.cloud og Symantec Email Continuity Archive Lite.cloud

1. Oversikt

1.1 Symantec Email Continuity Archive.cloud og Symantec Email Continuity Archive Lite.cloud Tjeneste er hosted email lagring systemer som tillater Kundens system administratorer til å sette bestemte email lagrings policies for lagring av historisk email for et sett av utpekte email mailbokser.

2. Kunden Forpliktelser

2.1 Kunden er ansvarlig for følgende handlinger i forbindelse med Tjenesten:

2.1.1 Besørge og vedlikeholde nødvendig hardware og software (som identifisert i Anskaffelse skjema);

2.1.2 Forsikre at dedikerte tekniske resurser med administrative rettigheter er tilgjengelig for Anskaffelse av Tjenesten;

2.1.3 Utpeke Brukere som er berettiget til motta Tjenesten og spesifisere lagringsperiode for hver slik Bruker;

2.1.4 Utpeke og beskytte tilgang privilegier til arkivet via KUNDENs interface;

2.1.5 Innstilling og håndtering av arkiverings lagrings policies;

2.1.6 Utføre søk for gjenfinning av arkivert data.

2.2 I tilfelle Kunden har unnlatt å utføre påkrevde handlinger som er nødvendige for Tjenesten innen tretti (30) dager fra datoen for Kundens bestilling, kan Symantec påbegynne fakturering for Tjenesten.

3. Funksjoner

3.1 *Symantec Email Continuity Archive.cloud Tjenesten* inkludere følgende tjeneste funksjoner:

3.1.1 *Email Capture og Storage* – email fanges opp fra den er levert til Kundens primære email miljø og overført til et email arkiv for indeksering og lagring. Email er kryptert og lagres på Tjenesten. Email lagrings policies kan innstilles slik at Brukere kan avgjøre når email vil bli renset fra Tjenesten.

3.1.2 *Recovery* – besørger mulighet for re-lagring av email fra email arkivet tilbake til Kundens lagring for Exchange beskjeder.

3.1.3 *E-Discovery* – besørger mulighet for Kundens system administratorer til å spesifisere visse Brukere som "Gjennomgåere", og gi dem mulighet til gjennomgå email i andre mailbokser enn deres egne for elektronisk oppdagelse og annet formål. Gjennomgåere kan lage et oppdagelsesarkiv som inneholder resultatene fra et søk på kryss av Brukernes mailbokser. Oppdagelsesarkivet kan eksporteres til en enkelt mailboks.

3.1.4 *Windows Autentisering* – å tillate en Kunden som bruker Microsoft Exchange 2000, Microsoft Exchange 2003 og/eller Microsoft Exchange 2007 til å utvide Kundens sikkerhet policies for Microsoft Active Directory autentisering ved bruk av Tjenesten ved å bemyndige Brukere til å logge inn på Tjenesten ved å anvende deres Active Directory passord.

3.1.5 *End User Arkivet* – muliggjøre at Brukere som er part av en lagrings policy, får tilgang til deres personlige arkiv som inneholder email fra deres mailboks gjennom en web-basert interface. Kundens email administratorer kan også spesifisere hvorvidt en Bruker kan videresende email fra deres personlige arkiv.

3.1.6 *Storage Management* – Kundens system administrator kan definere en lagrings management policy som vil flytte vedlegg fra Kundens Exchange beskjeder til å lagres i Tjenesten med det formål at lagringsbehovet reduseres.

3.2 *Symantec Email Continuity Archive Lite.cloud Tjenesten* inkluderer følgende tjeneste funksjoner (hver er ytterligere beskrevet ovenfor):

3.2.1 *Email Capture og Storage*

3.2.2 *Recovery*

3.2.3 *E-Discovery*

3.2.4 *Windows Autentisering*

Symantec Email Continuity Archive Lite.cloud Tjenesten inkluderer ikke End User Arkivet eller Storage Management funksjoner. Kunden kan oppgradere for å inkludere End User Arkiv tjeneste funksjon ved å abonnere på *Symantec Email Continuity Archive Lite.cloud Lite End User Pack*.

3.3 *Import* - Kunden kan importere tidligere data inn i Tjenesten fra pst filer ved nedlasting og ved å anvende et verktøy for import, og tjenesten er underlagt forpliktelsen til å betale et import vederlag basert på mengden av data som skal bli importert. I tilfelle at virkelig mengde av tidligere data overskrider mengden av kjøpt import data, reserverer Symantec sin rett til å kreve vederlag for slik tilleggsdata til dets gjeldende standard rater.

4. Bruker Policies

4.1 Kundens lagring skal måles ved måling av råmengden av email som overføres til Tjenesten og til enhver tid er lagret.

4.2 Hvis Kunden abonnerer på et av de følgende Symantec tjenesteknipper; Symantec MessageLabs Complete Email Safeguard.cloud, Symantec MessageLabs Complete Email & Web Safeguard.cloud eller Symantec MessageLabs Ultimate Safeguard.cloud:

4.2.1 Tjenesteknippet skal inkludere maksimum 0.7GB ny email ny email-lagring pr. Bruker pr. år for kombinasjonen av Tjenestene EC og Symantec Email Continuity Archive.cloud. Hvis Kundens nye email lagring overskrider slik tillatt lagringsmengde, skal Kunden være pålagt å kjøpe tilstrekkelig lagring for Tjenestene til Symantecs til enhver tid gjeldende priser.

4.2.2 Tjenesteknippene inkluderer ikke lagring for overtatt data importert iht Klausul 3.3 ovenfor og Kunden er pålagt å kjøpe tilstrekkelig tilleggslagring for å oppfylle slike lagringsbehov til Symantecs til enhver tid gjeldende rater.

4.3 Hvis Kunden ikke abonnerer på ett av tjenesteknippene opplisted i Klausul 4.2, skal ingen lagring være inkludert i pr. Bruker prisen og Kunden plikter å kjøpe tilstrekkelig lagring for Tjenestene til Symantecs til enhver tid gjeldende priser.

4.4 Når Kunden er pålagt å kjøpe tilleggslagring, skal Symantec sende tilleggsfaktura og/eller gjøre justering I etterfølgende faktura for å inndekke tilleggsvederlaget for økt lagring på en pro-rata basis for gjenstående del av gjeldende faktura periode.

5. Vilkår og Betingelser

5.1 INGEN EMAIL ARKIV TJENESTE KAN GARANTERE 100% NØYAKTIGHET OG SÅLEDES KAN SYMANTEC IKKE AKSEPTERE ANSVAR FOR NOEN SKADE ELLER TAP SOM RESULTERER DIREKTE ELLER INDIREKTE FRA MANGLER VED TJENESTE UTOVER AVHJELP SOM UTTRYKKELIG BESØRGES I SERVICE LEVEL AGREEMENT.

5.2 Symantec skal ikke bli ansvarlig for noen umulighet i forhold til å besørge Tjenesten som er spesifisert her og som medfører (a) at Symantecs ikke er i stand til å besørge at dets standard praksis i tas i bruk og besørge Tjenesten til Kunden, (b) feil fra Kunden i forhold til å følge Symantec veiledning som vist i brukermanual eller Anskaffelse skjema, eller (c) unnlatelse fra Kunden til å aktivere eller bruke Tjenesten.

5.3 Symantec fremhever at konfigurering og bruk av Tjenesten er fullstendig underlagt Kundens kontroll. Symantec anbefaler at Kunden har en akseptabel computer bruker policy (eller tilsvarende) på plass. I visse land vil det være nødvendig å innhente samtykke fra individuelt personell. Symantec råder Kunden til alltid å sjekke dets lokale lovgivning forut for at Tjenesten tas i bruk. Symantec kan ikke akseptere ansvar for sivile krav eller straffeansvar som Kunden kan pådra seg som følge av anvendelsen av Tjenesten.

5.4 KUNDEN FORSTÅR OG AKSEPTERER AT DELER ELLER HELE TJENESTEN KAN BLI UTFØRT I USA OG AT KUNDEN ER ANSVARLIG FOR Å INNHENTE ALLE SAMTYKKER OG TILLATELSER PÅKREVD FOR Å GJENNOMFØRE OVERFØRINGEN AV DATA. VIDERE FORSTÅR KUNDEN OG AKSEPTERER AT SYMANTEC IKKE KAN AKSEPTERE NOE ANSVAR FOR NOE KORRESPONDERENDE BRUDD PÅ GJELDENDE LOVGIVNING ELLER REGLER.

5.5 Kunden forstår og godtar at (i) Symantecs skanning tjenester (Email AV, Email AS, Email IC og Email CC) ikke skanner alle email som kommer inn i arkivet og (ii) Symantec skanning tjenester (Email AV, Email AS, Email IC og Email CC) ikke skanner email som er frigjort fra arkivet for å gjeninnsettes inn i en Brukers mailboks. Følgelig kan Symantec ikke bli ansvarlig for noe virus, spam, bilder eller upassende innhold som slik gjeninnsatte email kan inneholde, og videre, Service Level Agreement skal ikke gjelde for slike gjeninnsatte email.

5.6 Kunden anerkjenner og samtykker i at Symantec ikke under noen omstendighet kan opptre som en tredjeparts nedlaster i forbindelse med overholdelse av krav fra amerikanske SEC.

6. Software Lisens

6.1 Tilståelse av Lisens

Underlagt vilkår og betingelser i denne Avtalen, gir Symantec Kunden en ikke-eksklusiv, ikke-overførbar rett til installere og bruke Software for Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud Tjenesten kun for Kundens egen interne forretningsdrift. ("Software" betyr ethvert Symantec software program for Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud Tjenesten i objekt kode format lisensiert av Symantec og underlagt vilkårene i Avtalen, inklusiv uten begrensning nye utgivelser eller oppdateringer som besørges iht avtalen). Alle immaterielle rettigheter til Software er og skal fortsette å være eiendommen til Symantec (og/eller dets leverandører). Software er lisensiert av Symantec, ikke solgt. Kunden erkjenner at Software og all tilknyttet informasjon, inklusiv uten begrensning oppdateringer, er eiendommen til Symantec og dets leverandører. Kunden er fullt ut ansvarlig for egen og hver Brukers overholdelse av eller brudd på vilkår i denne Avtale. Kunden skal med umiddelbar effekt varsle Symantec om uautorisert bruk eller brudd på vilkår i denne lisens.

6.2. Kopiering og Bruker restriksjoner

Kunden kan nedlaste og installere Software underlagt følgende betingelser:

6.2.1. Kunden kan ikke nedlaste eller installere Software til flere enn det antall End User lisenser som er lisensiert av Kunden. ("End User" skal bety fysiske computere hvor software er installert).

6.2.2. Kunden kan kopiere Software i rimelig utstrekning for nødvendig for back-up, arkivering eller disaster recovery formål. Skriftlig Dokumentasjon kan reproduseres av Kunden for intern bruk kun. ("Dokumentasjon" betyr Symantecs bruker guides og/eller manualer for drift av Software, som er inkludert med nedlastet Software).

6.2.3 Kunden kan ikke, heller ikke tillate noen tredjepart å: (i) dekompilere, ta fra hverandre, eller reverse engineer Software, med unntak for uttrykkelig tillatt av gjeldende lovgivning, uten å innhente Symantecs skriftlige forhåndssamtykke; (ii) fjerne noen produkt identifikasjon eller varsel om beskyttede rettigheter; (iii) lease, låne ut eller bruke Software for tidsdeling eller tjeneste byrå formål; (iv) modifisere, oversette, tilpasse eller lage avledede produkter av Software, eller (v) på annen måte bruker eller kopiere Software med unntak for det som uttrykkelig er tillatt i denne Avtale.

6.3. Overføring av Rettigheter

Kunden kan ikke overføre, tildele eller delegere software lisens under denne Avtale uten å innhente skriftlig forhåndssamtykke fra Symantec. Slik ulovlig overføring tildeling eller delegasjon i strid med det foregående vil være ugyldig.

6.4. Begrenset Garanti og Ansvarsfraskrivelse

6.4.1 Symantec forsikrer at, ved nedlasting, vil Software være i all hovedsak være i overensstemmelse med Symantecs gjeldende Dokumentasjon.

6.4.2 Foregående garanti vil ikke gjelde hvis: (i) Software ikke anvendes i henhold til Avtalen eller Dokumentasjon; (ii) Software eller noen del av denne er blitt modified av noen annen part enn Symantec; eller (iii) en feil i Software har blitt forårsaket av noe av Kundens utstyr eller tredjepart software.

6.4.3 SYMANTEC GARANTERER IKKE AT DRIFT AV SOFTWARE VIL FOREGÅ UAVBRUTT ELLER FEIL-FRITT. SYMANTEC UTTRYKKELIG FRASKRIVER SEG ALLE GARANTIER AV NOE SLAG, UTRYKKELIG ELLER UNDERFORSTÅTT ELLER PÅ ANNEN MÅTE, INKLUSIV MEN IKKE BEGRENSET TIL GARANTIER FOR AV SALGBARHET, TILFREDSSTILLENDE KVALITET, ELLER PASSENDE FOR ET BESTEMT FORMÅL.

6.5. Avslutning

Ved avslutning av Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud Tjenesten, vil alle Kundens rettigheter til bruk av Software iht Avalen bortfalle med umiddelbar effekt og Kunden skal umiddelbart returnere til Symantec eller ødelegge alle kopier av Software og Dokumentasjon.

7. Opphør av tjeneste og datauttrekk

7.1 Ved opphør av tjenesten Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud skal Symantec slette alle kundens data fra arkivet.

7.2 Kunden kan trekke ut sine data fra arkivet når som helst før opphøret.

Bilag 15 – Symantec MessageLabs Volume Mail Tjenesten (Volum Mail)

1. Hvis Kunden abonnerer på Volum Mail Tjenesten, kan Kunden sende og motta Volum Mail underlagt følgende betingelser:

1.1 Volum Mail kan kun bestå av bekreftende og oppfordrede mottakere. Kunden skal iht Symantecs anmodning og underlagt gjeldende lovgivning, besørge bevis for slike bekreftelser.

1.2 størrelse på hver Volum Mail inklusiv vedlegg må ikke overskride 500 kilobytes.

1.3 'Mottakere' boks for hver enkelt Volum Mail må ikke inneholde mer enn fem hundre (500) Email adresser.

1.4 Kunden må ha et effektivt liste-management-system, inklusiv rask fjerning av ugyldige og abonnement kansellerte email adresser.

1.5 Kunden må motta Symantec MessageLabs Email Anti-Virus.cloud Tjeneste for dets standard Email.

1.6 Kundens Volum Mail må stamme fra eller bli dirigert mot et separat domene til deres standard Email bemyndigede Volum Mail for å bli dirigert mot et spesifikt besørget Kontroll Tårn.

1.7 default utgående banner skal varsle mottaker at Volum Mail har blitt virus skannet, men den vil ikke inneholde Symantecs logo.

1.8 Hvis Kunden abonnerer på Bånd F eller G av Volum Mail Tjenesten i Del B "Tjenester og Pris", må Kunden sende eller motta Volum Mail i batches på maksimum 250.000 mottakere pr. dag.

1.9 Kunden forstår og aksepterer at sending av Volum Mail sannsynligvis vil ha en vekslende effekt på flyten av Email trafikk. Slik effekt er utenfor Symantecs kontroll og på grunn av dette skal Service Level som angitt i Service Level Agreement ikke gjelde for Volum Mail.

1.10 Hvis på noe tid (i) Kundens Email systemer blir svartelistet, eller (ii) Kunden forårsaker at Symantecs systemer blir svartelistet på grunn av utsendelse av Spam, eller (iii) Kunden ikke oppfyller noen av sine forpliktelser som angitt i dette Bilag, skal Symantec informere Kunden og forbeholder seg retten til, etter eget valg, å holde tilbake besørgelsen av, suspendere eller terminere alle eller deler av Tjenestene med umiddelbar effekt.

1.11 Hver Volum Mail Tjeneste Bånd har en maksimum kvote av tillatte Mottakere pr. Måned. Slike kvoter er ikke overførbare eller kumulative og således vil uanvendt del av Mottaker kvote ikke overføres til påfølgende måneder.

1.12 Kunden skal varsle Symantec hvis på noe tidspunkt dets virkelige Volum Mail bruk overskrider antall av Mottakere tillatt pr. Måned for Kundens gjeldende Bånd, og Symantec skal øke vederlaget for de bestemte Bånd i henhold til Symantecs til enhver tid gjeldende prisliste. I tillegg vil Symantec kontrollere Kundens virkelige Volum Mail bruk og hvis antall Mottakere pr. Måned overskrider antall tillatte for Kundens gjeldende Bånd, vil Symantec øke vederlaget i henhold til Symantecs til enhver tid gjeldende prisliste. Symantec vil kunne velge å sende tilleggsfaktura og/eller gjøre justering i senere fakturabeløp for å dekke slike økninger.

Bilag 16 – Symantec Enterprise Vault.cloud

1. Oversikt

Symantec EV.cloud er fellesnavnet for en rekke arkiveringstjenester (hver av dem beskrevet i paragraf 1.1 t.o.m. 1.10 nedenfor) som kunden kan abonnere på. Alle tjenestene innenfor Symantec EV.cloud er kompatible med godkjente versjoner av lokale Exchange-servere og vertsbaserte Exchange-servere.

1.2 Følgende gjelder begge tjenestene, Symantec Enterprise Vault Personal.cloud og Symantec Enterprise Vault Discovery.cloud:

1.2.1 Maksimal e-poststørrelse som kan innføres av Symantec Enterprise Vault Personal.cloud og Symantec Enterprise Vault Discovery.cloud, er 50 MB.

1.2.2 Følgende gjelder begge tjenestene, Symantec Enterprise Vault Personal.cloud og Symantec Enterprise Vault Discovery.cloud:

1.2.3 Kunden kan svare direkte eller videresende meldinger i arkivet som er opprettet av en av tjenestene, som gjør kunden i stand til jevnlig å opprette sikkerhetskopieringsfiler i tilfelle kundens e-post skulle svikte.

1.2.4 Ingen av tjenestene erstatter behovet for at kunden sikkerhetskopierer sin e-postserver lokalt. Dersom kunden må bygge om sin e-postserver, bør den bygges om fra lokalt håndterte data og ikke fra arkivet.

1.1. Symantec Enterprise Vault Personal.cloud

Tjenesten Symantec Enterprise Vault Personal.cloud er Symantecs tjeneste for Internett-basert e-postarkivering, konstruert for å gi kundens individuelle brukere tilgang til sitt personlige e-postarkiv direkte fra Microsoft Outlook eller Outlook Web Access (der dette støttes) for å kunne finne og gjenopprette tapte eller slettede e-postmeldinger.

1.1.1 Kundens innkommende og utgående e-post, med vedlegg, samles opp i et søkbart arkiv på Internett ("personlig arkiv"), som brukeren kan søke i for å finne tapte eller slettede e-postmeldinger.

1.1.2 Brukere får også tilgang til sitt personlige arkiv fra Microsoft Outlook, Outlook Web Access (der dette støttes), IBM Lotus Notes, BlackBerry®-enheter og via nettleserbaserte, sikre webområder.

1.1.3 Brukere kan søke i det personlige arkivet etter spesifikke e-postmeldinger og vedlegg på to måter: hurtigsøk og avansert søk. Avansert søk gir brukeren muligheten til å tilpasse søket etter en rekke kriterier som nøkkelord i meldingen, til, fra, emne, dato(er) og vedleggstype.

1.1.4 Hvis dette aktiveres, kan brukere opprette, svare på og videresende meldinger direkte fra Symantec Enterprise Vault Personal.cloud, på samme måte som de gjør i Outlook eller Notes.

1.1.5 Brukere kan opprette tilpassede søk, basert på ulike kriterier (f.eks. datointervall, e-postavsender, vedleggstype osv.) og deretter lagre dem slik at brukerne kan bruke søket på nytt etter ønske.

1.1.6 Ved å flytte kundens arkiverte e-post over i det personlige arkivet og fjerne dem fra lokale arkiver, frigjøres plass på kundens delte stasjoner og e-postservere.

1.1.7 Kundens personlige arkiv kan brukes til å gjenopprette historisk e-post hvis en datamaskin eller bærbar PC tapes eller stjeles.

1.1.8 Kunder kan overføre PST-filer til Symantec Enterprise Vault Personal.cloud, der mappestrukturen vedlikeholdes optimalt fra første arkivering.

1.2. Symantec Enterprise Vault Discovery.cloud

Symantec Enterprise Vault Discovery.cloud er Symantecs Internett-baserte tjeneste for e-postarkivering, konstruert for å dekke anmodninger om juridisk dokumentasjon (e-dokumentasjon), håndheve bruksregler for e-post og hjelpe til å redusere tap av data. Det juridiske arkivet hjelper kunden til å bevare e-post forbundet med rettssaker/juridisk dokumentasjon og hjelper til å beskytte kommunikasjon mellom advokat og klient.

1.2.1 Symantec Enterprise Vault Discovery.cloud lagrer og katalogiserer e-post, vedlegg og BlackBerry®-meldinger (SMS-tekst, PIN-til-PIN, samtalelogg) i et sentralisert arkiv på Internett..

1.2.2 Kunder kan aktivere juridisk arkivering av spesifikk kommunikasjon (basert på søkekriterier) for å verne kundens ansatte eller for å forhindre at automatisert sletting fra å slette saksrelevante e-postmeldinger. Administratorer og kontrollører kan flagge kommunikasjon underlagt gjensidig taushetsplikt, som kan ekskluderes fra anmodninger om juridisk dokumentasjon.

1.2.3 Søkeloggen i Symantec Enterprise Vault Discovery.cloud registrerer aktivitetene til kontrollørene slik at administratorene kan gjennomføre passende gjennomganger.

1.2.4 Administratorer kan gruppere brukerne på grunnlag av tilpassede kriterier. Kontrollører kan søke på tvers av disse gruppene.

1.2.5 Kundene kan søke i innholdet av arkiverte e-postmeldinger og vedlegg med bruk av en rekke søkekriterier, inkludert til, fra, dato, emne, meldingstekst, vedlegg og andre meldingsdetaljer.

1.2.6 Kundens kontrollører kan navigere effektivt i søkeresultatene, opprette nye søkebegreper og merke potensielt skadelig e-post slik at disse med letthet kan hentes ut for videre gjennomgang.

1.2.7 Kundene kan merke e-post relatert til en spesifikk sak eller et juridisk forhold og deretter eksportere e-postmeldingene til en ekstern saksstyringsløsning eller annet program for viderebehandling.

1.2.8 Kundens kontrollører kan opprette og lagre tilpassede e-postsøk basert på kundens regler for e-post, og kan kjøre disse søkene om igjen etter behov.

1.2.9 Kundens kontrollører kan sette opp regelbaserte varsler for å melde fra når en e-post oppfyller kriteriene for et "lagret søk" (f.eks. inneholder spesifikke ord eller fraser).

1.3. Symantec Enterprise Vault.cloud BlackBerry® Option

Symantec Enterprise Vault.cloud BlackBerry® Option er Symantecs Internett-baserte tjeneste som gir kundens individuelle brukere tilgang til og muligheten til å søke i arkiverte e-postmeldinger, vedlegg, SMS, PIN-til-PIN og samtalelogger via deres BlackBerry®-enheter. Brukere kan finne og gjenopprette tapt eller slettet e-post og fortsette å bruke sin BlackBerry®-enhet til å opprette, besvare og sende meldinger i sanntid selv når kundens primære e-postserver er nede. Symantec Enterprise Vault.cloud BlackBerry® Option er en separat tilleggstjeneste til Symantecs tjeneste Symantec Enterprise Vault Personal.cloud.

1.3.1 Symantec Enterprise Vault.cloud BlackBerry® Option kan aktiveres av administrator for brukere fra en BlackBerry® Enterprise Server (BES) eller av brukere via BlackBerry® Desktop Manager.

1.3.2 Brukere kan logge seg på Symantec Enterprise Vault.cloud BlackBerry® Option ved å klikke på ikonet på enhetens startskjermbilde.

1.3.3 Når brukere klikker på applikasjonen, vises et startskjermbilde i tre sekunder, og deretter blir brukeren bedt om å angi brukernavn/passord.

1.3.4 Etter en vellykket pålogging bli brukeren dirigert til startskjermbildet (dvs. listevisning) til Personal Archive.

1.3.5 Fra skjermbildet for lister (postkasse) kan brukeren bruke en rekke funksjoner, inkludert: opprette nye meldinger, svare på eller videresende e-post og utføre enkle eller avanserte søk.

1.3.6 Brukere kan finne gamle, tapte eller slettede e-postmeldinger med bruk av enkle eller avanserte søk i alle meldinger og samtaleloggfiler lagret i deres personlige arkiv, og kan deretter gjenopprette disse meldingene til deres innboks.

1.3.7 Brukeren kan angi tekst i søkefeltet og trykke på søkeikonet for å starte søket. Søkeresultater kan filtreres etter "dato", "fra" og "til".

1.3.8 Brukeren kan benytte sitt personlige arkiv til å opprette, svare på og sende meldinger selv når kundens primære e-postplattform (f.eks. Microsoft Exchange) er utilgjengelig.

1.4 AdvisorMail on Symantec.cloud™

AdvisorMail on Symantec.cloud™ (AdvisorMail) er Symantecs Internett-baserte tjeneste for e-postarkivering som tilrettelegger gjennomgang av e-post som kreves av lov. Tjenesten AdvisorMail arkiverer e-post i et enkelt arkiv. Meldingene gjennomsøkes automatisk og merkes på grunnlag av kundens spesifikke regler. Meldinger og vedlegg som inneholder spesifikke nøkkelord eller fraser kan deretter gjennomgås av personer med ansvar for overholdelse av lover og regler.

1.4.1 AdvisorMail fanger automatisk opp avsendte og mottatte meldinger uten at kunden gjør noe mer, og sender dem til flere datasentre for arkivering med bruk av TLS- eller VPN-kryptering.
1.4.2 AdvisorMail har styrings- og rapporteringsverktøy, inkludert gjennomgang før og etter arkivering, vilkårlig prøvetaking, tilpasning av regler for spesifikke domener eller e-postadresser og samlede rapporter.
1.4.3 AdvisorMail gir to separate nivåer av e-postgjennomgang: administratorer (full tilgang) og revisorer (overvåkingsrettigheter for utvalgte postkasser).
1.4.4 AdvisorMail har en rekke verktøy for å effektivisere overvåkingsprosessen, inkludert automatisk flagging av mistenkelig e-post for gjennomgang av revisor.
1.4.5 Kundene kan forhåndsvelge sine startmapper (f.eks. etter gjennomgang), dataområde og meldingsvisning (f.eks. visning av liste eller korte utdrag).
1.4.6 Kundene kan bruke funksjonen Neste Klikk til å hoppe til neste regelbrudd i e-postmeldinger og vedlegg med et enkelt museklikk, for deretter å velge kommandoer ved å høyreklikke (f.eks. for å legge til nye nøkkelord).
1.4.7 AdvisorMail har en lagdelt overvåkingsfunksjon som lar kunden distribuere en liste med krenkende nøkkelord og fraser til eksterne kontorer med en enkelt kommando.
1.4.8 AdvisorMail har en "hviteliste" som lar kundene godkjenne nøkkelord og fraser som ofte finnes i ansvarsfraskrivelser (dvs. juridiske fraskrivelser som vises i e-postens fotnote) for å redusere antallet falske positive regelbrudd.
1.4.9 AdvisorMail lar kundene legge til e-postadresser, flytte brukere til andre kontorer, endre regler og gjennomgå flere e-postmeldinger.
1.4.10 Søkeloggen i AdvisorMail registrerer revisjonsaktivitetene til selskapets kontrollører og hjelper administratorene med å oppfylle samsvarskravene.
1.4.11 Kontrollørene kan om nødvendig legge notater til meldingene.

1.5 AdvisorMail IM Option on Symantec.cloud™
AdvisorMail IM Option on Symantec.cloud™ er Symantecs Internett-baserte arkiveringstjeneste for støttede direktemeldingsplattformer. Direktemeldinger fanges opp, lagres og katalogiseres i AdvisorMail, og overvåkes deretter på grunnlag av kundens spesifikke samsvarsregler. Direktemeldinger som inneholder spesifikke nøkkelord eller fraser kan deretter gjennomgås av personer med ansvar for overholdelse av lover og regler. AdvisorMail IM Option on Symantec.cloud™ er en separat tjeneste i tillegg til AdvisorMail.
1.5.1 AdvisorMail IM Option on Symantec.cloud™ virker med støttede direktemeldingsnettverk og -klienter, som for tiden omfatter AOL, MSN, Yahoo og Google Talk, private nettverk (Reuters), og direktemeldingsklienter for bedrifter (Microsoft Office Communicator, Lotus Sametime og Jabber).
1.5.2 Direktemeldinger katalogiseres og kopieres i sin opprinnelige form til medier der kundene lett kan søke på dem.
1.5.3 Kunden kan søke på og hente ut spesifikke direktemeldingssamtaler på grunnlag av en rekke søkekriterier, inkludert datointervall, nøkkelord eller frase og avsender/mottaker.
1.5.3 Det finnes en historisk logg av revisjonshensyn.

1.6 AdvisorMail Bloomberg Option on Symantec.cloud™
AdvisorMail Bloomberg Option on Symantec.cloud™ er Symantecs Internett-baserte arkiveringstjeneste for Instant Bloomberg (direktemeldinger) og Bloomberg e-post. Bloomberg-meldinger fanges opp, lagres og katalogiseres i AdvisorMail, og overvåkes deretter på grunnlag av kundens spesifikke samsvarsregler. Bloomberg-meldinger som inneholder spesifikke nøkkelord eller fraser kan deretter gjennomgås av personer med ansvar for samsvar. AdvisorMail Bloomberg Option on Symantec.cloud™ er en separat tilleggstjeneste til AdvisorMail.
1.6.1 AdvisorMail Bloomberg Option on Symantec.cloud™ er en tjeneste som fanger opp Bloomberg-direktemeldinger og Bloomberg-e-post i AdvisorMail i deres opprinnelige formater.
1.6.2 Bloomberg-direktemeldinger katalogiseres og kopieres i sin opprinnelige form til medier der kundene lett kan søke på dem.
1.6.3 Kunden kan søke på og hente ut spesifikke Bloomberg-direktemeldingssamtaler på grunnlag av en rekke søkekriterier, inkludert datointervall, nøkkelord eller frase og avsender/mottaker.
1.6.4 Det finnes en historisk logg av revisjonshensyn.

1.7 Reserverte.

1.8 Symantec Enterprise Vault.cloud Data Import Option
Symantec Enterprise Vault.cloud Data Import Option er Symantecs Internett-baserte tjeneste for migrering og innføring av eksisterende e-postdata i kundens arkiv. Importtjenesten lar kunden deretter søke i e-postarkivet (f.eks. Symantec Enterprise Vault Personal.cloud, Symantec Enterprise Vault Discovery.cloud og AdvisorMail), både etter arkivert e-post og ny e-post.
1.8.1 Symantec Enterprise Vault.cloud Data Import Option krever at kunden sender e-postdata via S-FTP eller sikker e-post i PST- eller EML-format.
1.8.2 Kunden kan manuelt trekke ut data og benytte et PST- eller EML-format eller bruke Symantec profesjonelle tjenester til automatisk uttrekking av data fra støttede arkiver.
1.8.3 På grunnlag av kundens retningslinjer vil Symantec Enterprise Vault.cloud Data Import Option definere eierskapet til hver melding som finnes. Meldinger som ikke kan tilordnes en bestemt person, arkiveres i en oppsamlingspostkasse i e-postarkivet.
1.8.4 All migrering kan loggføres og revideres for å sikre integriteten til kundens e-postdata og opprettholde "arkiveringskjeden".
1.8.5 Symantec Enterprise Vault.cloud Data Import Option involverer kundens aktive deltakelse i planlegging, analyse og utførelse av en innføringsplan med minimale avbrudd i normal drift.
1.8.6 Maksimal e-poststørrelse som kan innføres er 40 MB.

1.9 Symantec Enterprise Vault Mailbox Continuity.cloud
HVIS SYMANTEC ER UTE AV STAND TIL Å ETABLERE EN SMTP-FORBINDELSE MED KUNDEN, VIL KUNDENS E-POST BLI RUTET TIL TJENESTEN SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD PÅ VEGNE AV KUNDEN ("KONTINUITETSHENDELSE"). FOR Å UNNGÅ TVIL: (I) HVIS KUNDENS BRANNMUR FUNGERER SOM PROXY OG SVARER PÅ VEGNE AV E-POSTSERVEREN, ELLER (II) HVIS KUNDENS E-POSTSERVER GIR ET SVAR (INKLUDERT, UTEN BEGRENSNING, FEILKODER), VIL DETTE UTGJØRE EN SMTP-FORBINDELSE OG VIL IKKE VÆRE EN KONTINUITETSHENDELSE.
1.9.1 Under en kontinuitetshendelse får kundenes individuelle brukere tilgang til sin e-post via en dedikert mappe i Microsoft Outlook® eller et nettbasert brukergrensesnitt. Brukeren kan: (i) vise opptil nitti (90) dager med historisk e-post, inkludert ny e-post som sendes/mottas under kontinuitetshendelsen, (ii) opprette, svare på og videresende e-post og (iii) bruk vanlige e-postverktøy som stavekontroll, vedlegg og rik formatering.
1.9.2 Hvis kunden kun abonnerer på Symantec Enterprise Vault Mailbox Continuity.cloud, vil kontinuitets-e-post bli lagret i denne tjenesten i nitti (90) dager. Hvis kunden har kjøpt en ytterligere arkiveringstjeneste under dette vedlegg 17, vil kontinuitets-e-post beholdes på grunnlag av oppbevaringsperioden kunden har valgt i denne tjenesten.
1.9.3 Kontinuitets-e-post vil bli levert til kundens primære e-postserver på det tidspunktet denne serveren igjen kan akseptere e-post, bortsett fra at e-post som har ligget i kø i over sju (7) dager, ikke vil bli levert, men må gjenvinnes av kunden fra kontinuitetsarkivet, slik det beskrives i klausul 1.9.2 ovenfor.
1.9.4 Tjenesten Symantec Enterprise Vault Mailbox Continuity.cloud bruker en opportunistisk, heller enn en tvungen, forbindelse med transportlagssikkerhet ("TLS") når den forsøker å levere e-post. TLS er en forbedret sikkerhetsprotokoll som er designet for å beskytte/kryptere e-post under transport over Internett. **ALLE KUNDER MED GRENSEKRYPTERING OG REGELBASERT KRYPTERING SOM OGSÅ VELGER TJENESTEN SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD, ANERKJENNER OG SAMTYKKER I AT EN TLS-FORBINDELSE VIL BLI FORSØKT, MEN VIL KANSKJE IKKE OPPNÅS, OG AT SLIK E-POST DERMED IKKE VIL BLI KRYPTERT KUNDEN ER INNEFORSTÅTT MED AT KUNDEN IKKE BØR SENDE ELLER MOTTA SENSITIVE DATA VIA TJENESTEN SYMANTEC ENTERPRISE VAULT MAILBOX CONTINUITY.CLOUD, ELLER AT KUNDEN GJØR DETTE HELT PÅ EGEN RISIKO.**

1.9.5 Symantec Enterprise Vault Mailbox Continuity.cloud Forpliktelser
Tjenesten Symantec Enterprise Vault Mailbox Continuity.cloud leverer kun e-post til én enkelt angitt server per spesifisert domene og "per brukerruting". Kunden aksepterer herved denne siden av tjenesten. Kunden samtykker i å skulle konfigurere tjenesten Symantec Enterprise Vault Mailbox Continuity.cloud som en reserveleveringsrute med ClientNet-grensesnittet, og videre i å informere Symantec om leveringsstedet (e-postvertens navn eller IP-adresse) per domene for deres e-postservere ved starten på denne tjenesten. Kunden anerkjenner og samtykker i at kunden har en kontinuerlig forpliktelse til å oppdatere Symantec under varigheten av tjenesten Symantec Enterprise Vault Mailbox Continuity.cloud om alle endringer av slike leveringssteder. Kunden anerkjenner at kundens mangel på slike konfigurasjoner eller ikke å gi Symantec slik leveringsinformasjon, vil ha negativ innvirkning på funksjonaliteten til tjenesten 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 er en tilleggstjeneste til tjenesten Symantec Enterprise Vault Personal.cloud, beskrevet i avsnitt 1.1 av dette vedlegget. Tjenesten Symantec Enterprise Vault.cloud Folder Sync Option gjør en kunde i stand til å se e-post i tjenesten Symantec Enterprise Vault Personal.cloud på en måte som ligner på hvordan e-post organiseres i kundens Outlook-mapper. Symantec Enterprise Vault.cloud Folder Sync Option lar administratorer synkronisere kundens Outlook-mappestruktur i Symantec Enterprise Vault Personal.cloud. Når kunden flytter e-post mellom Outlook-mapper og oppretter og flytter på Outlook-mapper, vil synkroniseringstjenesten deretter kopiere mappenes struktur i Symantec Enterprise Vault Personal.cloud.
1.10.2 Symantec Enterprise Vault.cloud Folder Sync Option implementeres av administratorer for kunden via en lokal tjeneste som sporer mappenes og innholdets bevegelser.
1.10.3 Etter den første synkroniseringen gir Symantec Enterprise Vault.cloud Folder Sync Option inkrementell synkronisering mellom Outlook-mappene og Symantec Enterprise Vault Personal.cloud.
1.10.4 Inkrementell synkronisering kan planlegges på time-, dags- eller ukebasis, etter kundens eget ønske.
1.10.5 En kunde kan filtrere resultatene av et arkivsøk ved å aktivere "filter"-funksjonen og velge en mappe fra listen som returneres i Søkefiltre.
Tjenesten støttes kun på plattformene Microsoft Exchange Server 2003, 2007 eller 2010.

2. Ytterligere vilkår.

2.1 Symantec understreker at konfigurasjon og bruk av tjenesten fullstendig kontrolleres av kunden. Symantec anbefaler kunden å ha etablert regler for akseptabel bruk av datamaskiner (eller tilsvarende). I visse land kan det være behov for å innhente samtykke fra individuelle ansatte. Symantec råder kunden til alltid å kontrollere lokal lovgivning før tjenesten tas i bruk. Symantec aksepterer ikke ansvar for brudd på sivil- eller strafferettslig lovgivning som kunden kan gjøre seg skyldig i som følge av bruken av tjenesten.
2.2 **KUNDEN ANERKJENNER OG SAMTYKKER I AT HELE ELLER DELER AV TJENESTEN KAN UTFØRES I USA OG AT KUNDEN HAR ANSVAR FOR Å INNHENTE NØDVENDIG SAMTYKKE OG GODKJENNING FOR OVERFØRING AV DATA. KUNDEN ANERKJENNER OG SAMTYKKER OGSÅ I AT SYMANTEC IKKE HAR ANSVAR FOR NOEN BRUDD PÅ GJELDENDE LOVER ELLER FORSKRIFTER.**
2.3 Kunden anerkjenner og samtykker i at (i) Symantecs gjennomsøkingstjenester (Email AV, Email AS, Email IC og Email CC) ikke gjennomsøker all e-post som opprinnelig overføres til arkivet og (ii) at Symantecs gjennomsøkingstjenester (Email AV, Email AS, Email IC og Email CC) ikke gjennomsøker e-post som frigjøres fra arkivet for å gjenopprettes i brukerens postkasse. Symantec kan derfor ikke holdes ansvarlig for virus, spam, bilder eller upassende innhold som slik gjenopprettet e-post kan inneholde, og tjenesteavtalen gjelder ikke for slike gjenopprettede e-postmeldinger.
2.4 Under vilkårene og betingelsene i denne avtalen gir Symantec kunden en ikke-eksklusiv, ikke-overførbar rett til å installere og bruke all programvare som tilhører ovennevnte tjenester, til bruk kun i kundens egen, interne virksomhet. Alle immaterielle rettigheter til denne programvaren tilhører og vil fortsette å tilhøre Symantec (og/eller deres leverandører). Programvaren lisensieres av Symantec, men selges ikke. Kunden anerkjenner at programvaren og all relatert informasjon, inkludert uten begrensning oppdateringer, tilhører Symantec og deres leverandører. Kunden har det fulle ansvar for hver brukers overholdelse av eller brudd på vilkårene i avtalen. Kunden skal øyeblikkelig melde fra til Symantec ved uautorisert bruk av eller brudd på vilkårene til denne lisensen.
2.5 Kunden anerkjenner og samtykker i at Symantec ikke under noen omstendighet kan opptre som en tredjeparts nedlaster i forbindelse med overholdelse av krav fra amerikanske SEC.
2.6 Alle kundedata som lagres eller arkiveres under denne avtalen av Symantec eller selskapets tredjepartsleverandører, forblir kundens eksklusive eiendom ("kundedata"), og ikke noe i dette dokumentet gir Symantec eller dets leverandører juridisk eller reel rettighet, eiendomsrett eller interesse til kundedata.
2.7 Kundedata skal lagres eller arkiveres under tjenesteperioden og i en periode på ett hundre og tjue (120) dager etter tjenesteperioden, eller i ett hundre og tjue (120) dager etter opphørsdatoen dersom tjenesten opphører før perioden løper ut (samlet, "oppbevaringsperiode etter opphør"). Under eller før oppbevaringsperioden etter opphør skal kunden skriftlig meddele sitt valg om at Symantec skal: (i) slette kundedataene vederlagsfritt (med mindre dette forbys av lov eller rettsbeslutning) eller (ii) gi en offline kopi i PST-format via et harddiskmedium til Symantecs gjeldende priser og med en hastighet på maks to (2) terabyte levert per måned til alle kundedata er returnert til kunden. Hvis kunden ikke gir Symantec skriftlige instruksjoner slik det beskrives i foregående setning, skal Symantec slette kundedataene (med mindre dette forbys av lov eller rettsbeslutning) ved utløpet av oppbevaringsperioden etter opphør

Bilag 17 – Symantec Endpoint Protection.cloud

1. Oversikt

1.1 For å kunne motta Symantec Endpoint Protection.cloud Service må kunden installere en agent på relevante sluttbrukerdatamaskiner og opprette passende regler for bruk av tjenesten. Styringsportalen for Symantec Endpoint Protection.cloud er en administratorportal for styring av datamaskiner, regler, varsler og rapporter ("styringsportalen").

1.2 Kunden må kanskje gjøre noen mindre endringer i brannmuren for å tillate agenten å kommunisere med og bruke Symantec Hosted Services-infrastrukturen.

1.3 Når tjenesten har blitt konfigurert i samsvar med klausulene 1.1 og 1.2, brukes styringsportalen til å administrere agenten(e).

1.4 Symantec vil publisere en liste med operativsystemer som agenten støtter, og med nettlesere som støttes av styringsportalen. Kunden er innforstått med og samtykker i at Symantec kan oppdatere og endre denne listen jevnlig uten forvarsel.

1.5 Agenten på datamaskinen:

1.5.1 Skal beskytte datamaskinen mot oppdagede skadeprogrammer, basert på kjente metoder i henhold til tjenesten.

1.5.2. Skal blokkere kjente ondsinnede angrep fra tilgang til nettverket og datamaskinen.

1.5.3 Skal søke å gi beskyttelse mot nettfisking for støttede nettlesere og blokkere nettfiskingsangrep.

2. Styringsportal

2.1 Styringsportalen lar kundene konfigurere sine egne sikkerhetsbaserte regler for agentene.

2.2 Kunden har ansvaret for å implementere konfigurasjonsvalgene på linje med kundens regler for akseptabel bruk av datamaskiner (eller tilsvarende) via styringsportalen. Regler konfigureres for datamaskingruppen.

2.3 Endringer av reglene synliggjøres umiddelbart via styringsportalen og sendes i batch ut til agentene. Gjeldende regelinnstillinger på individuelle agenter kan vises på styringsportalen eller på agenten som kjører på sluttbrukerens datamaskin.

3. Logger og rapporter

3.1 Alle logger og rapporter fra agenten lagres på styringsportalen og kan vises og lastes ned i tolv (12) måneder, deretter blir de slettet.

4. Meldinger

4.1 Kunden kan konfigurere Symantec Endpoint Protection.cloud Service til å sende automatiske meldinger til konfigurerte e-postmottakere, basert på varselreglene som kan konfigureres via styringsportalen.

4.2 Kunden kan opprette, slette og tilpasse meldinger via styringsportalen.

5. Brukerstøtte

5.1 Støtten omfatter:

5.1.1 Trinnvis innføring i styringsportalen, inkludert en beskrivelse av tjenestene og en økt med vanlige spørsmål. (Dette inkluderer ikke hjelp til oppsett av regler eller analyse av reglenes effektivitet).

5.1.2 Administratorveiledning.

5.1.3. Brukerhåndbok.

6. Datavern for Symantec Endpoint Protection.cloud

6.1 Kunden er innforstått med at loggene kan inneholde personlig identifiserbar informasjon og at loggføring og avskjæring av logger kan omfatte behandling av personopplysninger. Kunden er videre innforstått med at Symantec Endpoint Protection.cloud er en konfigurerbar tjeneste og at kunden har eneansvar for å konfigurere Symantec Endpoint Protection.cloud i samsvar med kundens regler for akseptabel bruk av datamaskiner (eller tilsvarende) og for alle gjeldende lover og forskrifter. Symantec råder derfor kunden til alltid å sjekke lokal lovgivning før Symantec Endpoint Protection.cloud tas i bruk, og til å påse at kunden og alle ansatte er klar over og etterfølger alt ansvar de har i følge dataverns- og personvernlover og/eller forskrifter i forbindelse med kundens bruk av Symantec Endpoint Protection.cloud. I visse land kan det være behov for å innhente samtykke fra individuelle ansatte før avskjæring og loggføring. Kunden må installere alle agenter for Symantec Endpoint Protection.cloud med rimelig og minimal tilpasning. Kunden er innforstått med og godtar at enheter som dekkes av Symantec Endpoint Protection.cloud Service, (i) logger informasjon som er relatert til bruken av Symantec Endpoint Protection.cloud Service, (ii) at denne informasjonen overføres til Symantec med den hensikt å gi informasjon og rapportering om administrasjon til kunden og (iii) kunden godkjenner slik logging og overføring. Symantec aksepterer ikke ansvar for brudd på sivil- eller strafferettslig lovgivning som kunden kan gjøre seg skyldig i som følge av kundens bruk av Symantec Endpoint Protection.cloud.

7. Konfigurasjon

7.1 Hvis kunden har kjøpt tjenesten via en Symantec-forhandler, gir kunden uttrykkelig denne Symantec-forhandleren tillatelse til å (i) endre tjenestens konfigurasjon for å oppnå optimal funksjonalitet med tjenesten og (ii) sende inn forespørsler om støtte på kundens vegne.

Bilag 18 – Symantec MessageLabs Web v2 Smart Connect.cloud ("Smart Connect.cloud")

1. **Oversikt**

1.1. Når roamingbrukeragenten er installert og nødvendige endringer av konfigurasjonen er utført, blir søk på webområder og vedlegg automatisk rutet via brukeragenten til Symantec MessageLabs Web v2 URL.cloud Service ("Web v2 URL") og Symantec MessageLabs Web v2 Protect.cloud Service ("Web v2 Protect"), der de blir digitalt undersøkt.

2. **Tjenestebeskrivelse**

2.1. Når brukere kobler seg til Internett i de definerte "tjenestelandene", blir kundens eksterne HTTP- og FTP-over-HTTP-søk, inkludert alle vedlegg, makroer eller kjørbare programmer dirigert gjennom tjenestene Web v2 URL og Web v2 Protect.

3. **Konfigurasjon**

3.1. Konfigurasjonen som kreves for å dirigere denne eksterne webtrafikken til agentprogramvaren for roaming-brukere, og for å sende all utgående trafikk til tjenestene Web v2 URL og Web v2 Protect, utføres og oppdateres av kunden og er avhengig av kundens tekniske infrastruktur. Kunden må installere en PAC-fil på brukerens PC slik at nettleseren peker til Symantecs roamingagent når nettleseren startes opp. En mal for en PAC-fil kan lastes ned fra ClientNet og kan modifiseres av kunden. Kunden må påse at intern HTTP/FTP-over-HTTP-trafikk (f.eks. til selskapets Intranet) ikke dirigeres til roamingagenten.

3.2. Tilgang til Web v2 URL og Web v2 Protect er begrenset til autoriserte systemer som inneholder en gyldig versjon av kundens roamingagentprogram, i tillegg til autoriserte brukere som er aktivert for disse tjenestene i ClientNet. Roamingagentprogrammet og opplysninger om autoriserte brukere benyttes til å identifisere kunden og dynamisk velge kundespesifikke innstillinger.

3.3. Reglene for tjenesten Web v2 URL og for innholdssøk for tjenesten Web v2 Protect vil være de samme når en bruker bruker roamingagenten som når han er tilkoblet vi et konfigurert nettverk, f.eks. selskapets LAN.

3.4. Kunden er innforstått med at roamingagenten vil bli levert med MessagLabs' standardinnstillinger, som inkluderer et rimelig forsøk på å rute brukeren webtrafikk til et "optimalt" tilgangspunkt for infrastrukturen. Denne rutingen er basert på en forståelse av roamingbrukerens lokalisering, basert på IP-adresse og bruk av en tredjeparts database for geo-lokalisering for å identifisere det landet der brukeren i øyeblikket sannsynligvis kobler seg til fra. Symantec vil rute brukerne med passende landtilhørighet til det man anser som det optimale tilgangspunktet for det spesifikke landet. Dette gjøres uavhengig av noen vurdering av mulig kvalitet på den individuelle brukerens forbindelse, og kun for land som Symantec anser å være i stand til å yte et akseptabelt tjenestenivå.

For alle land utenom de akseptable tjenestelandene, er kunden innforstått med at Symantec ikke vil kunne levere tjenestene Web v2 URL eller Web v2 Protect. I disse situasjonene, når det fastslås at sluttbrukeren befinner seg i et "land uten tjeneste", vil roamingagenten "automatisk åpnes" slik at sluttbrukeren kan koble seg til Internett uten fordelene med Symantecs tjenester som er tilgjengelig i akseptable tjenesteland.

KUNDEN ER INNEFORSTÅTT MED OG SAMTYKKER I AT BRUKERENS WEBTRAFIKK, FOR BEHANDLING, KAN BLI DIRIGERT TIL INFRASTRUKTUR SOM BEFINNER SEG PÅ ET GEOGRAFISK STED UTENFOR EU, I SAMSVAR MED DENNE KLAUSUL 3.4. KUNDEN HAR ANSVARET FOR Å INNHENTE ALLE OVERENSKOMSTER OG GODKJENNINGER FOR OVERFØRING AV SLIK WEBTRAFIKK. KUNDEN ANERKJENNER OG SAMTYKKER OGSÅ I AT SYMANTEC IKKE HAR ANSVAR FOR NOEN BRUDD PÅ GJELDENDE LOVER ELLER FORSKRIFTER.

4. **Ytterligere eksportvilkår for Smart Connect.cloud**

4.1 Kunde eller partner må ikke, og må ikke gi noen tredjepart tillatelse til å, selge, videreselge, reeksportere, overføre, avlede, distribuere, kaste, fremlegge eller på annen måte handle med kontrollert teknologi, direkte eller indirekte, til noen av følgende land: Afghanistan, Angola, Armenia, Aserbajdsjan, Bosnia og Herzegovina, Burma, Burundi, Kina, Cuba, Kongo, Eritrea, Etiopia, Iran, Irak, Nord-Korea, Liberia, Libya, Nigeria, Rwanda, Sierra Leone, Somalia, Sudan, Syria, Tanzania, Uganda og Zimbabwe.

4.2 Kunde og partner må ikke overføre webroamingagenten til et annet selskap eller til en annen person som ikke er ansatt hos kunden eller partneren, bortsett fra at: (i) kunde eller partner kan overføre til eller tillate nedlasting av webroamingagenten for sine eksterne underentreprenører for bruk på kundens eller partnerens vegne, og/eller (ii) kunde eller partner kan overføre til eller tillate nedlastning av webroamingagenten for sine eksterne sluttbrukerkunder som de videreselger Symantec-tjenesten til, forutsatt at kunden og partneren gjør slike eksterne kunder klar over forpliktelsene i denne klausulen.

Vedlegg 3
Service Level Agreement

1. Definisjoner

1.1.de følgende ord skal ha følgende betydning i denne Service Level Agreement:

"**Credit Request**" betyr varsel som Kunden må inngi til Symantec pr Email til support@messagelabs.com med tittel-feltet "Credit Request" (med mindre Symantec varsler om annet);

"**Designated Tårn Cluster**" betyr to (2) eller flere Tårn, distribuert over minimum to (2) lokasjoner, bestemt for å besørge Tjenesten til Kunden;

"Email Virus False Positive" betyr en lovlig Email feilaktig markert/ angitt å inneholde et virus;

"**Email Tjenester**" betyr Emailen AV, Email AS, Email IC, Email CC, Policy Basert Krypterings og Boundary Krypterings Tjenester;

"Known Virus" betyr et virus som på tidspunktet for mottak av innholdet av Symantec: (i) en signatur har allerede blitt gjort offentlig tilgjengelig for et minimum av en (1) time for konfigurering av tredjeparts kommersielle skannere anvendt av Symantec; eller (ii) er inkludert i "Wild List" som finnes på http://www.wildlist.org og identifisert til å være "In wild" av minimum to Wild List deltagere.

"Symantec Tracker" betyr et Symantec verktøy som måler Tjenestens Tilgjengelighet og Ventetid;

"**Månedlig Vederlag**" betyr månedlig vederlag for angjeldende Tjenester som detaljert i Avtalen;

"**Service level**" betyr hver av Tjenestens parametere definert i denne Service Level Agreement;

"Spam False Negative" betyr en Spam Email som ikke er identifisert som Spam;

"Spam False Positive" betyr en lovlig Email feilaktig merket/fanget som Spam;

"Spam Recommended Innstillinger" betyr Symantecs best practice konfigurerings veiledning for Emailen AS Tjenesten; og

"Tårn" betyr et antall av belastnings balanserte servere;

"**Web Tjenester**" betyr Web v2 Protect og Web v2 URL Tjenester sammen.

2. Generelt

2.1. I tilfelle Kunden antar han har rett til avhjelp i henhold til denne Service Level Agreement, må Kunden inngi en Credit Request innen ti (10) virkedager etter utløpet av gjeldende kalender måned. Kunden anerkjenner at logger kun beholdes for et begrenset antall dager og således vil en Credit Request inngitt utenfor den angitte tidsfrist bli ansett ugyldig.

2.2.Alle Credit Requests vil bli underlagt verifikasjon av Symantec i henhold til gjeldende bestemmelser i denne Service Level Agreement.

2.3.Denne Service Level Agreement vil ikke gjelde: (i) i løpet av perioder av Planlagt Vedlikehold eller Nød-vedlikehold, perioder av ikke-tilgjengelighet på grunn av force majeure eller handlinger eller unnlatelser fra enten Kunden eller en tredjepart; (ii) i løpet av en periode hvor tjenesten er suspendert av Symantec i henhold til vilkårene i Avtalen; (iii) hvor Kunden er i brudd med bestemmelser i Avtalen (inkludert uten begrensning hvis kunden har forfalte regninger); (iv) i forhold til all e-post som ikke har passert tjenesten (inkludert uten begrensning hvis kunden ikke har stilt sin ruter til å sende all e-posttrafikk til Symantec); eller (v) med hensyn til enhver inngående eller utgående e-postmelding som opprinnelig ble sendt til Symantec som inneholdt mer enn 500 mottakere per SMTP-økt.

2.4.avhjelp fastsatt i denne Service Level Agreement skal være Kundens eneste avhjelp iht kontrakt og erstatning utenfor kontrakt (inklusiv men uten begrensning uaktsomhet) eller på annen måte i forhold til nivåer for Tjenesten.

2.5.akkumulert maksimums ansvar for Symantec under denne Service Level Agreement i en hvilken som helst kalender måned skal ikke være større enn hundre prosent (100%) av Månedlig Vederlag for Kunden betaler for de(n) berørte Tjeneste(r).

2.6.Hvis berørt Tjeneste er del av en Non-Severable Tjeneste Bundle:

a) for å kalkulere tjeneste kreditter, skal Månedlig Vederlag for slik berørt Tjeneste bli beregnet som totalt Månedlig Vederlag for Non-Severable Tjeneste Bundle delt på antall Tjenester som omfattes av slik bundle; og

b) hvis Kunden terminere den berørte Tjenesten i henhold til denne Service Level Agreement, skal revidert vederlag for Non-Severable Tjeneste Bundle bli beregnet som originalt totalt Månedlig Vederlag for Non-Severable Tjeneste Bundle, delt på originalt antall Tjenester omfattet av slik bundle, og multiplisert med antall gjenstående Tjenester omfattet av slik bundle.

2.7 Service Level er for Email Tjenester gjelder ikke Kundens EC Tjeneste og således Service Level for Email Tjenester i klausuler 3 til 5 inklusiv nedenfor skal bli suspendert i løpet av noen periode hvor EC Tjenesten er i en aktivert tilstand.

3. 100% Tjeneste Tilgjengelighet

3.1 Service Availability Service Level vil kun gjelde dersom Kunden utnytter en eller flere av Email Tjenester eller Web Tjenester.

3.2 In relasjon til Email Tjenester, skal Service Availability Service Level bety mulighet for å etablere en SMTP sesjon på port 25 av Designated Tårn Cluster, som målt av Symantec Tracker. Denne Service Level skal kun gjelde hvis Designated Tårn Cluster er i stand til:

3.2.1 motta Kundens innkommende Email på vegne av Kundens domene på en 24x7 basis; og

3.2.2 akseptere Kundens utgående Email fra en korrekt konfigurert Kunde SMTP host på vegne av Kundens domene(r) på en 24x7 basis.

3.3 I relasjon til Web Tjenester, skal dette Service Availability Service Level bety tilgjengelighet av Web Tjenester til å akseptere Kundens utgående web anmodninger og skal kun gjelde hvis Kundens host, gateway enheter eller proxy(s) er korrekt konfigurert på en 24x7 basis.

3.4 Hvis i noen kalender måned Service Availability er under hundre prosent (100%), kan Kunden være berettiget til følgende prosentvise kreditt (godskrivelse):

Prosent Tjeneste Tilgjengelighet Pr. Kalender Måned	Prosent kreditt av Månedlig Vederlag
< 100% men >= 99%	25
< 99% men >= 98.0%	50
< 98.0%	100 og avslutning av berørt Tjeneste etter Kundens valg

3.5 I tilfelle Tjeneste Tilgjengelighet faller under nittiåtte prosent (98%) i noen kalender måned, skal Kunden være berettiget til å terminere berørt Tjeneste og motta en pro rata refusjon av vederlaget betalt på forhånd for berørt Tjeneste for perioden etter avslutning.

4. 100% Email Levering

4.1 Email Levering Tjeneste nivå vil kun gjelde hvis Kunden anvender en eller flere av Email Tjenester.

4.2 Symantec vil levere 100% av alle Emailer sendt til eller fra Kunden underlagt følgende:

4.2.1 Emailen må ha blitt mottatt av Kundens Designated Tårn Cluster; og

4.2.2 Emailen må ikke inneholde et virus, Spam eller annet innhold som har forårsaket at den blir blokkert av Email Tjenester.

4.3 Underlagt Klausuler 4.1 og 4.2 ovenfor, i tilfelle Symantec mislykkes i å levere en Email til eller fra Kunden og Kunden ikke er i brudd på vilkår i Avtalen, skal Kunden har rett til terminere Email Tjenester med tretti (30) dager forhånds skriftlig varsel.

5. Email Ventetid – 60 Sekunder

5.1. Underlagt Klausul 5.2, skal Email Ventetid Sevice level kun gjelde hvis Kunden anvender en eller flere Email Tjenester.

5.2. Email Ventetid Service level skal **ikke** gjelde Policy Basert Krypterings Tjeneste.

5.3. Hvis i noen kalender måned gjennomsnittlig rundtur tid (som målt av Symantec Tracker) for Email sendt hvert 5 minutt til og fra hvert Email Tjenester Tårn innen Kundens Designated Tårn Cluster overskrider forsinkelser som angitt nedenfor i tabellen, kan Kunden inngi en Credit Request i henhold til tabellen nedenfor:

Gjennomsnittlig rundtur tid for 100% av målingene (i minutter og sekunder)	Prosent kreditt av Månedlig Vederlag
> 1 min men <= 1min 30 sek	25

> 1min 30sek men <= 2 min	50
> 2 min men <= 2mins 30 sek	75
> 2 min 30 sek	100

5.4. Email Ventetid Service level vil ikke gjelde:
5.4.1. Hvis Kunden ikke har gitt Symantec en liste med bestemte Email adresser for å motta Tjenesten ("Validation List") og Kunden lider av "Denial of Service attakk";
5.4.2. I løpet av perioder med forsinkelse forårsaket av en mail loop fra/til Kundens systemer.

6. Web Ventetid – 0.1 Sekunder

6.1 Web Ventetid Service level vil kun gjelde hvis Kunden anvender en eller flere Web Tjenester.
6.2. Hvis gjennomsnittlig skanning tid av Web innhold, målt fra når Symantec mottar innholdet til punktet for Symantecs forsøk på å overføre innholdet, beregnet i løpet av en kalender måned er mindre enn 100% i henhold til tabellen nedenfor, kan Kunden inngi en Credit Request:

Gjennomsnittlig prosent av web innhold skanning innen 100 millisekunder	Prosent kreditt av Månedlig Vederlag
< 100% men >= 99%	25
< 99% men >= 98%	50
< 98% men >= 97%	75
< 97%	100 og avslutning av berørt Tjeneste at Kundens valg

6.3 Web Ventetid Service level skal kun gjelde objekter på 1MB eller mindre.

7. Spam – False Positives 0.0003%

7.1. Spam False Positive Service level vil kun gjelde hvis Kunden anvender Email Anti Spam Tjenesten og implementerer Symantec Spam Recommended Innstillinger.
7.2. Hvor gjennomsnittlig Spam False Positive fanging rate øker til mer enn 0.0003% av alle Kundens Email trafikk i noen kalender måned, kan Kunden ha krav på kreditt (godskrivelse) i henhold til tabellen nedenfor:

Prosent Spam False Positive capture rate i løpet av kalender måned	Prosent kreditt av Månedlig Vederlag
>0.0003 men <= 0.003	25
> 0.003 men <= 0.03	50
>0.03 men <= 0.3	75
>0.3	100

7.3.de følgende Email vil ikke utgjøre Spam False Positive Email for formål av denne Service level:
7.3.1. Email som ikke er en legitim business Email;
7.3.2. Email som inneholder flere enn 20 mottakere;
7.3.3. Hvor avsender av Emailen er på Kundens blokkert avsender liste, inklusiv uten begrensning slike definert av individuell Bruker hvis Kunden har muliggjort Bruker-nivå innstillinger;
7.3.4. Email som er sendt fra en kompromittert maskin;
7.3.5. Email som er sendt fra en maskin som er på en tredjepart blokkere-liste;
7.3.6. Email som har blitt sendt til flere enn 20 mottakere (i en enkel operasjon eller i en serie operasjoner) og minst har 80% av samme innhold.

8. 99% Spam Capture Rate

8.1. Spam Capture Service level vil kun gjelde hvis Kunden anvender Emailen Anti Spam Tjenesten og implementerer Spam Recommended Innstillinger. Bestemmelsene i denne Klausul 8 korresponderer til antallet av Spam False Negatives målt i en måned.
8.2. Kunden kan bli berettiget til en kreditt (godskrivelse) i henhold til tabellen nedenfor:

Prosent Spam Capture rate i løpet av kalender måned	Prosent Credit av Månedlig Vederlag
>98% - <= 99%	25
> 97% - <= 98%	50
> 96% - <= 97%	75
< 96%	100

8.3. Spam Capture Service level vil ikke gjelde hvor Email ikke ble sendt til en legitim adresse.
8.4 En lavere Spam Capture rate enn 95% skal gjelder Email som inneholder Asian character tegn. I tilfelle at slik Spam Capture rate faller under 95% skal Kunden være berettiget til en 25% prosent kreditt (godskrivelse) av Månedlig Vederlag. I tilfelle at Spam Capture rate faller under 90% skal Kunden være berettiget til en 100% prosent kreditt (godskrivelse) av Månedlig Vederlag.

9. Spam Tjenesten Credit Requests

9.1. For å bli mottakelig for kreditt (godskrivelse) under Klausuler 7 og 8 må Kunde sende mistenkelig False Positive eller False Negative Email til support@Symantec.com innen 5 dager av mottak av Emailen. Symantec vil undersøke og bekrefte hvorvidt eller ikke Emailen er en Spam False Positive eller Spam False Negative og vil registrere funnene. På slutten av kalender måneden, hvis Kunden antar at antallet bekreftede Spam False Positives eller Spam False Negatives gir rett til en kreditt (godskrivelse) i henhold til tabellen ovenfor, må Kunden sende en Credit Request til Symantec i henhold til klausul 2.1 av dette Vedlegg.

10. Email Virus Beskyttelse – 100%

10.1. Email Virus Beskyttelse Service level vil kun gjelde hvis Kunden anvender Emailen Anti Virus Tjenesten.
10.2. hvis kundens systemer blir infisert av en eller flere Virus i noen kalender måned som varslet til Symantec i en logget og bekreftet support anrop som et virus har blitt sendt Kunden gjennom Email AV Tjenesten, kan Kunden fakturere Symantec for forhåndsavtalt skadekrav tilsvarende det laveste av enten 100% av Månedlig Vederlag som gjelder til slikt tidspunkt eller £5,000/€10,000 (avhengig av valutaen i som Kunden faktureres i). Avhjelp fastsatt i denne Klausul 10.2 skal være eneste avhjelp etter kontrakten og iht. erstatningsrett utenfor kontrakt (inklusiv men uten begrensning uaktsomhet) eller på annen måte i forhold til noen infeksjon av et virus sendt til Kunden eller en tredjepart gjennom Tjenesten. For å avklare all tvil, så skal avhjelp som angitt i denne Klausul 10.2 ikke gjelde saker med forsettlig selv-påføring.
10.3. Kundens systemer anses å være infisert hvis et virus inneholdende i en Email mottatt gjennom Emailen AV Tjenesten har blitt aktivert innen Kundens systemer enten automatisk eller med manuell intervensjon.
10.4. I tilfelle at Symantec oppdager men ikke stopper en virus-infisert Email, vil Symantec øyeblikkelig varsle Kunden, forutsatt tilstrekkelig informasjon muliggjøre Kundens identifisering og sletting av Virus-infisert Email. Hvis slik varsling resulterer i forhindring av infeksjon skal avhjelp som angitt i klausul 10.2 ovenfor ikke gjelder. Dersom Kunden ikke handler umiddelbart iht slik informasjon, vil den ikke ha rettigheter iht Service level som beskrevet i klausul 10.2 ovenfor.
10.5. Email AV Tjenesten vil skanne så mye av Emailen og dets vedlegg som mulig. Den kan være at det ikke er mulig å skanne vedlegg med innhold som er under direkte kontroll av avsender (for eksempel, passord beskyttet og/eller kryptert vedlegg). Slik Email og/eller vedlegg er ekskludert fra Service level i klausul 10.2 ovenfor.
10.6. Email Virus Beskyttelse Service level skal ikke gjelde i relasjon til Virus som forsettelig har blitt frigjort av Kunden.

11. Email Virus False Positives 0.0001%

11.1 Email Virus False Positive Service level vil kun gjelde hvis Kunden anvender Emailen Anti Virus Tjenesten.
11.2. Hvor Emailet virus False Positive capture rate øker over 0.0001% av alle Kundens Email trafikk i noen kalender måned kan Kunden ha rett til en kreditt (godskrivelse) i henhold til tabellen nedenfor:

Prosent Email Virus False Positive capture rate i løpet av kalender måned	Prosent kreditt av Månedlig Vederlag
>0.0001 men <= 0.001	25
> 0.001 men <= 0.01	50
>0.01 men <= 0.1	75
>0.1	100

12. Web Virus Beskyttelse – 100% Known

12.1 Web Virus Beskyttelse Service level vil kun gjelde hvis Kunden anvender Web v2 Protect Tjenesten.
12.2. Skulle Kundens systemer bli infisert av en eller flere Known Virus i noen kalender måned som varslet til Symantec i en logget og bekreftet support anrop inklusiv detaljer for URL som denne ble nedlastet fra, og bekreftes som et Known Virus har blitt sendt til Kunden gjennom Web v2 Protect Tjenesten, kan Kunden fakturere Symantec for avtalt skadeserstatning som skal tilsvare laveste beløp av enten 100% av Månedlig Vederlag som gjelder til enhver tid eller £5,000/€10,000 (avhengig av valutaen i som Kunden er fakturert i. Avhjelp som beskrevet i denne Klausul 12.2 skal være eneste avhjelp iht kontrakten og også utenfor kontrakt iht erstatningsretten (inklusiv men uten begrensning uaktsomhet) eller på annen måte i

forhold til noen infeksjon av en Known Virus sendt til Kunden eller en tredjepart gjennom Web v2 Protect Tjenesten. For å unngå tvil, skal avhjelp som beskrevet i denne Klausul 12.2 ikke gjelde i tilfelle forsettlig selv-infeksjon eller forsettlig nedlasting av kjent ødeleggende kode fra Kundens side.

12.3 Kundens systemer skal ansees å være infisert hvis en Known Virus inneholdende i en web transaksjon mottatt gjennom Web v2 Protect Tjenesten har blitt aktivert innen Kundens systemer enten automatisk eller med manuell intervensjon.

12.4 I tilfelle at Symantec oppdager men ikke stopper et Known Virus som del av en web transaksjon gjennom Symantec Web v2 Protect Tjenesten, skal Symantec vil umiddelbart varsle Kunden, og besørge tilstrekkelig informasjon for å gjøre Kunden i stand til å identifisere og slette enheten Hvis slik varsling resulter i en forhindring av infeksjon skal avhjelp som foreskrevet i klausul 12.2 ovenfor ikke gjelde. Dersom Kunden unnlater å umiddelbart handle på basis av slik informasjon, vil dette forhold gjøre at Service level i klausul 12.2 ovenfor ikke skal gjelde.

12.5. Web v2 Protect Tjenesten vil skanne så mye som mulig av web item som er nedlastet. Den kan være at det ikke er mulig å skanne enheter som er innkapslet eller tunnelled for kommunikasjons formål via supportert Web Protocols (HTTP, og FTP over HTTP), overført over HTTPS, komprimert eller modifisert fra deres originale form for distribusjon, produkt lisens beskyttelse, nedlaste eller oppdatere, eller innhold som er under direkte kontroll av avsender (for eksempel, passord beskyttet og/eller kryptert enheter). Slik enheter og/eller vedlegg er ekskludert fra Service level i klausul 12.2.

13. 24x7 Tekniske Support og Feil Respons

13.1 Symantec vil på en tjue-fire (24) timer/dag av sju (7) dager/uke basis:

a) besørge tekniske support til Kunden for problemer ved Tjenesten; og

b) samarbeide med Kunden å løse slike problemer.

13.2 Når en Kunden tar opp et problem, feil eller anmoder om tjeneste informasjon via telefon eller email med Symantec, vil dets prioritets nivå og responstid være som fastsatt i tabellen nedenfor:

Prioritets Nivå	Definisjon	Respons Mål
Critical	Tap av Tjeneste	95% av henvendelser besvart innen 2 timer
Major	Delvis tap av Tjenesten eller dårlig Tjeneste	85% av henvendelser besvart innen 4 timer
Minor	Informasjons anmodning som kan eller ikke kan ha påvirkning på Tjenesten	75% av henvendelser besvart innen 8 timer

13.3 Feil som stammer fra Kundens handlinger eller som krever handling fra annen tjenestebesørger utover Symantecs kontroll og er uttrykkelig ekskludert fra "feil respons tid" i klausul 13.2 ovenfor.

13.4 Underlagt Klausul 13.3, hvis Kunden antar at den har opplevd en forsinkelse i Symantecs responstid i forhold til en anmodning (utenfor parametere definert i klausul 13.2 ovenfor) kan den gi grunnlag for en kreditt (godskrivelse). Credit Requests må angi tid, dato og logg for antall av hendelser. Hvis berettiget vil Kunden kunne bli kreditert i henhold til tabellen nedenfor:

Prioritet	Feil i forhold til å oppnå målet	Prosent Credit av Månedlig Vederlag
Critical	Mer enn en gang pr kalender måned	15
Major	Mer enn to ganger pr kalender måned	10
Minor	Mer enn tre ganger pr kalender måned	5

14. Arkivering (P) Tjenesten

14.1 Bestemmelsene i denne Klausul 14 skal kun gjelde Arkivering (P) Tjenesten.

14.1 Arkivering (P) Tjenesten Tilgjengelighet

14.1.1 Arkivering (P) Tjenesten vil være tilgjengelig 99.9% i hver kalender måned, eksklusiv Planlagt Vedlikehold og Nød-vedlikehold vindu. I dette tilfellet, skal "Tilgjengelig" være definert som at Symantec hosted infrastruktur er klart til å akseptere og arkivere Email. For det formål å kalkulere ikke-tilgjengelighet skal følgende kriterier gjelde: a) måling vil bli utført av Symantecs kontroll systemer (slik måling kan besørges til Kunden ved skriftlig anmodning), b) kontroll vil skje i 5 minutter intervaller med to påfølgende feil (unnlatelser) påkrevd til å bli en outage, c) kun Symantec hosted infrastruktur vil bli målt og slik måling ekskluderer ikke-tilgjengelighet som følge av en Email Arkivering Appliance outage, en Kunde nettverk outage, eller en Internett outage.

14.1.2 For hver en (1) prosent eller del av dette for ikke-tilgjengelighet utover tilgjengelighets målet på 99.9% under Klausul 14.1 i kalender måneden det gjelder, vil Kunden ha rett på en kreditt (godskrivelse) tilsvarende til ti prosent (10%) av månedlig vederlaget på grunn av Symantec i relasjon til Arkivering (P) Tjenesten, underlagt en maksimum av 100% av månedlig vederlaget pga relasjon til Arkivering (P) Tjenesten i noen kalender måneder. Kunden kan terminere Arkivering (P) Tjenesten etter eget valg hvis tilgjengeligheten til noen tid faller under nitti prosent (90%) i en kalender måned.

14.2 Arkivering (P) Tjenesten - Appliance Service level

14.2.1 Hvis en Email Arkivering Appliance feiler i løpet av garanti perioden pga en årsak som er dekket av Symantec Begrensede Garanti (som definert i dokumentasjon mottatt med Emailen Arkivering Appliance), vil Symantec, uten kostnad for Kunden, arbeide med Kunden for å trouble-shoot Email Arkivering Appliance (som kan kreve VPN Tilgang til Emailen Arkivering Appliance) innen fire (4) timer etter mottatt varsling av problemet fra Kunden i løpet av Normale Arbeidstimer og innen åtte (8) timer etter mottak av varsling for problem utenfor av Normal Arbeidstid. Innen tjue (20) Normale Arbeidstimer etter mottak av varsel om problem, vil Symantec enten:

14.2.1.1 varsle Kunden om at Email Arkivering Appliance fungerer ok og at problemet ikke stammer fra Emailen Arkivering Appliance eller Software; eller

14.2.1.2 reparere Emailen Arkivering Appliance som betyr avhjelp av hardware og/eller software; eller

14.2.1.3 varsle Kunden om at en erstatnings Email Arkivering Appliance er påkrevd; eller

14.2.1.4 hvis Symantec ikke er i stand til å reparere eller erstatte Emailen Arkivering Appliance, refundere månedlig vederlag for Arkivering (P) Tjenesten for gjeldende periode og terminere Arkivering (P) Tjenesten.

14.2.2 Skulle Symantec bli forpliktet under Klausul 14.2.1.3 ovenfor til å besørge en erstatnings Email Arkivering Appliance, skal Symantec levere slik erstatnings Email Arkivering Appliance til Kundens lokasjon innen førtiåtte (48) Normale Arbeidstimer fra den tid Symantec varsler Kunden om at ny Email Arkivering Appliance vil bli besørget.

14.2.3 Skulle Symantec være forpliktet under Klausuler 14.2.1.2 og 14.2.1.3 ovenfor til å reparere eller erstatte Emailen Arkivering Appliance eller Software og mislykkes i å gjøre dette innen tidsrammen angitt i klausuler 14.2.1 og 14.2.2, vil Symantec refundere Kunden fem prosent (5%) av månedlig vederlag for Arkivering (P) Tjenesten for hver dags forsinkelse.

14.2.4 Den beskrevne avhjelp i denne Klausul 14.2 skal være Kundens eneste avhjelp mht noen mangel eller brudd av garanti vedrørende Emailen Arkivering Appliance.

15. EC

15.1 Bestemmelsene i denne Klausul 15 skal kun gjelde EC Tjenesten.

15.1.1 EC vil være tilgjengelig 99.9% av hver kalender måned, eksklusiv Planlagt Vedlikehold og nød-vedlikehold vindu. "Tilgjengelig" er definert som at Symantec hosted infrastruktur er klar for å synkronisere nøkkel system og Bruker informasjon. For det formål å kalkulere ikke-tilgjengelighet skal følgende kriterier gjelde:

a) måling vil bli utført av Symantecs monitoring systemer (slik måling kan besørges til Kunden ved skriftlig anmodning), b) kun Symantec hosted infrastruktur vil bli målt og slik måling ekskluderer ikke-tilgjengelighet som følge av en Kundes nettverk outage, en tredjeparts outage, eller DNS issues utenfor Symantecs direkte kontroll.

15.1.2 For hver en (1) prosent eller del derav av ikke-tilgjengelighet utover tilgjengelighets mål på 99.9% under denne Klausul 15.1 i kalender måneden det gjelder, vil Kunden ha rett på en kreditt (godskrivelse) tilsvarende ti prosent (10%) av månedlig vederlaget på grunn av Symantec i relasjon til EC Tjenesten, underlagt en maksimum på 100% av betalbart månedlig vederlaget i relasjon til EC Tjenesten i en kalender måned. Kunden kan terminere EC Tjenesten etter eget valg dersom tilgjengelighet faller under nitti prosent (90%) i noen kalender måned.

16. Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud Tjenesten

16.1 Bestemmelsene i denne Klausul 16 skal kun gjelde Symantec Email Continuity Archive.cloud og Symantec Email Continuity Archive Lite.cloud Tjenesten.
16.1.1 Symantec Email Continuity Archive.cloud og Symantec Email Continuity Archive Lite.cloud Tjenester skal være tilgjengelig 99.95% av hver kalender måned. Tilgjengelighet skal beregnes ved å dele totalt antall timer som Symantec Email Continuity Archive.cloud og Symantec Email Continuity Archive Lite.cloud Tjenesten (fra gjeldende) har vært tilgjengelig (bortsett fra noen perioder av Kunden nettverk outages, maintenance, eller DNS issues utenfor Symantec direkte kontroll), på total antall planlagt tilgjengelige timer for Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud Tjenesten (fra gjeldende) i angjeldende kalender måneden.
16.1.2 For hver en (1) prosent av ikke-tilgjengelighet utover tilgjengelighetsmålet på 99.95% iht denne Klausul 16 i angjeldende kalender måned, skal Kunden ha rett til en kreditt tilsvarende vederlaget betalt til Symantec i relasjon til Symantec Email Continuity Archive.cloud og Symantec Email Continuity Archive Lite.cloud Tjenesten (siden gjeldende) for en dag av Symantec Email Continuity Archive.cloud eller Symantec Email Continuity Archive Lite.cloud Tjenesten.

17. Symantec EV.cloud

17.1 Symantec skal sikre 99,99 % servertilgjengelighet for Symantec EV.cloud. Hvis servertilgjengelighet for en full kalendermåned faller under 99,99 %, vil Symantec gi kunden en kreditt som beskrevet nedenfor:

Servertilgjengelighet	Prosentvis kreditt mot månedsprisen
99,9 % til 99,98 %	5 % av månedlig pris
98,0 % til 99,8 %	10 % av månedlig pris
95,0 % til 97,9 %	15 % av månedlig pris
90,0 % til 94,9 %	25 % av månedlig pris
89,9 % eller lavere	2,5 % av månedlig pris for hver 1 % av tapt tilgjengelighet opptil maksimalt 100 % av månedsprisen.

17.2 Krav om kreditt må inkludere datoer og tidspunkter da server var utilgjengelig. Symantec vil sammenligne kundens informasjon om utilgjengelig server med overvåkingsdata hos Symantec. Det skal gis kreditt hvis utilgjengelighet av server gir grunnlag for kreditt som beskrevet i paragraf 17.1 ovenfor. Kreditten som beskrives i paragraf 17.2 er kundens eneste botemiddel i forbindelse med mangel på servertilgjengelighet. Manglende servertilgjengelighet som skyldes vedlikehold er unntatt fra beregning av servertilgjengelighet.

18. Symantec Endpoint Protection.cloud

18.1 Bestemmelsene i klausul 18 gjelder kun for Symantec Endpoint Protection.cloud Service.
18.1.1 Symantec Endpoint Protection.cloud vil være 100 % tilgjengelig hver kalendermåned, bortsett fra under planlagt vedlikehold og nødvedlikehold. I dette tilfellet defineres "tilgjengelig" som at Symantec vertsbaserte infrastruktur er klar til å synkronisere regelinformasjon. Følgende regler gjelder for beregning av utilgjengelighet: a) målingen utføres av Symantecs overvåkingssystem (slike målinger kan sendes til kunden på skriftlig anmodning), b) Symantecs vertsbaserte infrastruktur vil bli målt og slike målinger ekskluderer all utilgjengelighet som skyldes at kundens nettverk er nede, at en tredjepart er nede eller DNS-problemer utenfor Symantecs direkte kontroll.
18.1.2 For hver en (1) prosent eller deler derav med utilgjengelighet utenfor tilgjengelighetsmålet per kalendermåned under klausul 18.1 på 99,9 %, vil kunden ha rett på en kreditt som tilsvarer ti prosent (10 %) av månedsprisen han betaler til Symantec i forbindelse med Symantec Endpoint Protection.cloud Service, opptil maksimalt 100 % av månedsbeløpet kunden betaler per kalendermåned for Symantec Endpoint Protection.cloud Service. Kunden kan si opp Symantec Endpoint Protection.cloud Service når kunden vil dersom tilgjengeligheten faller under nitti prosent (90 %) i enhver kalendermåned.
18.1.3 Kreditten som beskrives i paragraf 18.1.2 er kundens eneste botemiddel i forbindelse med mangel på servertilgjengelighet for tjenesten Symantec Endpoint Protection.cloud. Servicenivåene i avsnitt 3.1, 3.4 og 11.1 av denne servicenivåavtalen skal ikke gjelde for tjenesten Symantec Endpoint Protection.cloud.