Tjänstebeskrivning
IT-Arbetsplatshantering

IT-Arbetsplatshantering är en tjänst som består av olika komponenter. Genom att välja ut de komponenter som passar bäst för sina behov kan kundens säkerställa att arbetsstationsmiljön uppfyller behoven på ett säkert och optimalt sätt.

Innehåll

1 Översikt

Tjänsten IT-Arbetsplatshantering tillhandahålls av leverantören på kundägda eller leverantörens dedikerade arbetsstationer. Med den här tjänsten ser vi till att Kundens IT-arbetsplats (slutanvändarnas datorer och i vissa fall periferienheter) alltid är uppdaterad med aktuella applikationer, säkerhetssystem och funktioner enligt överenskomna policys som uppfyller kundens affärsbehov.

2 Tjänstens innehåll

Tjänsten består av separata Tjänstemoduler som stödjer utvecklingen av en arbetsstationsmiljö och som bidrar med mervärde till kundens verksamhet. Tjänsten omfattar följande Tjänstemoduler:

- Tjänstemodul för distribution av programvara och Microsofts säkerhetsuppdateringar.
- Tjänstemodul för filsynkronisering.
- Tjänstemodul för kryptering.
- Tjänstemodul för datorsäkerhet.

2.1 Tjänstemodul för distribution av programvara och Microsofts säkerhetsuppdateringar

Tjänsten för distribution av applikationer och Microsofts säkerhetsuppdateringar i kundens arbetsstationsmiljö tillhandahålls centralt. Tjänsten består av pilotdistributioner av applikationer och därefter sker distributionen "live" till samtliga användare som enligt Kundens policy ska ha aktuell distribution. Utöver detta omfattar tjänsten löpande distribution av säkerhetsuppdateringar för operativsystem och överenskomna applikationer.

Distribution av pilot- och live-distributioner beställs av kunden. Tjänsteavgiften (normalt per månad och arbetsplats) baseras på antalet beräknade distributioner för operativsystem och överenskomna applikationer (ofta benämnda BAS-applikationer). Syftet med Tjänstemodulen är att tillhandahålla en uppdaterad och säker plattform för Kundens användare.

Tjänsten kan också användas för distribution av Kundens övriga applikationer, utöver basapplikationerna. Dessa distributioner beställs separat per tillfälle.

2.1.1 Innehåll och uppgifter

Tjänsten beställs via leverantörens formulär för beställning av paketering, anpassning av maskiner och distribution enligt en standardrutin.

En distribution omfattar pilotdistributioner och live-distributioner i en sådan omfattning som avtalas med Kunden.

Tjänsten innehåller en funktion för att ominstallera datorer via Kundens nätverk på ett snabbt och effektivt sätt.

2.1.2 Tillval

2.1.2.1 Leverantörens deltagande i Kundens CAB-möten (Change Advisory Board)

Leverantören åtar sig att ta aktiv del i Kundens CAB-möten. CAB-möten syftar till att synkronisera förändringar i Kundens IT-miljö och besluta vilka förändringar som får ske och när de måste utföras. Leverantörens ansvar är att ta med information om aktuella uppdateringar och patchar som finns tillgängliga för operativsystem och överenskommen applikationslista.

Efter beslut om förändring så koordinerar Leverantörens representant resurser hos Leverantören för utförande.

2.1.2.2 Leverantören ansvarar för CAB-möten (Change Advisory Board) med Kundens beställare

Utöver vad som beskrivs som Leverantörens ansvar i punkt 2.3.1.1. så åtar sig Leverantören att driva CAB-möten i Kundens intresse. Åtagandet omfattar ordförandeskap i CAB-möten och rekommendationer om lämpliga åtgärder i Kundens IT-miljö utifrån IT-säkerhet, Kundens policys, Kundens budget. Kundens beställare måste delta på möten och ha beslutandemandat om vilka åtgärder som planeras och genomförs.

2.1.2.3 Funktionsleverans

Leverantören levererar Tjänstemodulen på kapacitetstjänst i egna datorhallar och står för hårdvara och licenser för den centrala plattformen. Leverantören väljer distributionssystem. Tjänsten utförs i koordination med Tjänsten Software Asset Management för bästa kostnadseffektivitet för Kunden under förutsättning att båda Tjänstemodulerna avropas från Kund.

2.1.2.4 Extra distributionspunkt

Leverantören tillhandahåller överenskommet antal extra distributionspunkter i Kunden nät. Extra distributionspunkt används exempelvis vid begränsad bandbredd till satelitkontor.

2.1.3 Uppgifter som debiteras separat

Specialuppgifter som utförs utanför tjänstens omfattning debiteras separat.

Manuella installationer på maskiner som inte ingår i det centrala distributionssystemet, eller till vilka distribution av någon anledning inte är möjligt.

2.1.4 Begränsningar och ansvar

Leverans av tjänsten kräver att kundens IT-infrastrukturmiljö är standardiserad och godkänd av leverantören.

Kundens miljö och distributionsverktyg ska beskrivas och kartläggas. Leverantören kräver också att kunden använder en produkt för distribution av applikationer och säkerhetsuppdateringar som stöds av leverantören. Om Tjänstemodulen köps som Funktionsleverans så är detta Leverantörens ansvar.

Om Tjänsten leveras på Kundens distributionssystem så måste systemet granskas och godkännas av Leverantören före initiering.

Tjänsteleveransen kräver att Leverantörens mjukvaruagent installeras på alla arbetsstationer som ingår i tjänsten.

Kundens ansvar:

- Kunden förbereder och levererar de installationsmedia, nycklar och uppgifter som behövs till leverantören, t.ex. en lista över applikationerna och ansvariga personer för dessa, samt över programtillverkare.
- Kunden utser ansvariga personer från sin organisation som ska testa de förberedda paketen på arbetsstationer i produktionsmiljön.
- Kunden köper in utrustningen för distributionsservrarna och testmiljön samt licenser om Tjänsten tillhandahålls på kundägt system.

2.1.5 Rapportering

Distributionsspecifika rapporter ingår i tjänsten, för vilka leverantören är ansvarig. På begäran kan leverantören leverera t.ex. månatliga rapporter. Ytterligare rapporter debiteras separat.

2.1.6 Aktiviteter vid initiering

Distributionssystem installeras som ett projekt, antingen i leverantörens lokaler eller i kundens, eller alternativt kan ett befintligt distributionssystem användas.

Efter initiering går leverantören igenom tjänsteprocessen och beställningsrutinen med Kunden.

2.1.7 Ändringar

Omfattande ändringar som påverkar tjänsteleveransen verkställs alltid som separata projekt. Byte av distributionssystem är ett exempel på en sådan ändring.

2.1.8 Aktiviteter efter uppsägning

När tjänsten sägs upp upphör de tjänster som inrättats under startfasen och produktion, kunddata tas bort från datalager på överenskommet sätt och användningen av tjänsterelaterade verktyg upphör.

En plan för att stänga ned tjänsten upprättas och leverantören utser en person som ansvarar för nedstängningen.

2.1.9 Teknik som stöds

- Microsoft System Center Configuration Manager (SCCM).
- Miradore.
- WSUS.

2.2 Tjänstemodul för filsynkronisering

Leverantörens tjänst för filsynkronisering gör det möjligt att synkronisera, versionshantera säkerhetskopiera data som lagrats på hårddisken i enskilda bordsdatorer på ett kontrollerat sätt. Funktionen innebär att användarna själva kan hantera dataåterställningar inklusive versionshantering.

2.2.1 Innehåll och uppgifter

Tjänsten innebär att Leverantören slår på synkroniseringsfunktion som finns tillgänglig i operativsystemet på klienterna samt på filservrarna. Angivna filer och kataloger synkroniseras automatiskt mellan klient och filserver. Allt data i filserverfunktionen säkerhetskopieras enligt överenskommen policy.

Användaren kan själv via filhanteraren återställa tidigare versioner av sina dokument.

Tjänsten innebär också att användarens filer finns tillgängliga för andra enheter som är anslutna till filtjänsten enligt överenskommen policy.

2.2.2 Uppgifter som debiteras separat

- Utbildning för slutanvändare.

2.2.3 Begränsningar och ansvar

Tjänsten kan enbart levereras till Kunder som också köper filserverfunktionen.
Det åligger användaren att själv hantera synkroniseringskonflikter.
Parterna tillsammans måste vara överens om synkroniserings- och säkerhetskopieringspolicy.

Leverantören är inte ansvarig för några direkta eller indirekta skador som kunden åsamkas på grund av en egenskap eller defekter i mjukvaran.

Kundens ansvar om tjänsten enligt separat avtal tillhandahålls med hjälp av kundens licenser och/eller utrustning:

- Enligt separat avtal kan tjänsten för filsynkronisering implementeras med hjälp av kundens egen serverutrustning, licenser och/eller utrustning i kundens lokaler som en s.k. hanterad tjänst. I den här modellen är kunden fullt ansvarig för de komponenter som används i tjänsten, om inte annat är överenskommet.

2.2.4 Rapportering

Ingen separat rapportering levereras för Tjänstemodulen.

2.2.5 Aktiviteter vid initiering

Vid initiering av tjänsten:

- Miljöns kompatibilitet specificeras och kontrolleras: servrar, utrustning och datakommunikation.
- Leverantören granskar systemkonfigureringen och funktionen.
- Profiler definieras tillsammans med kunden.

2.2.6 Ändringar

Ändringar som påverkar tjänsteleveransen verkställs alltid enligt gällande konsultprislista.

2.2.7 Aktiviteter efter uppsägning

När tjänsten sägs upp upphör de tjänster som inrättats under startfasen och produktion, kunddata tas bort från datalager på överenskommet sätt och användningen av tjänsterelaterade verktyg upphör.
En plan för att stänga ned tjänsten upprättas och leverantören utser en person som ansvarar för nedstängningen.

2.2.8 Operativsystem som stöds

Tjänsten stödjer följande operativsystem

- Microsoft Windows 7 (32 bitar och 64 bitar) eller högre version

2.3 Tjänstemodul för kryptering

Bordsdatorkrypteringstjänsten är en centralt administrerad informationssäkerhetstjänst, som omfattar hantering av krypteringsprogramvara och fjärrsupport till slutanvändare. Arbetsstationens hela hårddisk krypteras med stark kryptering, dvs. hela datainnhållet i hårddisken är i krypterat format. Den faktiska datakrypteringen äger rum i bakgrunden utan att användaren märker det.

2.3.1 Innehåll och uppgifter

Tjänsten omfattar följande:

- Bakgrundskryptering av hårddisk.
- Tvingad autentisering.
- Återställning av glömt lösenord.

2.3.1.1 Kryptering av enhetens hårddisk

Programvara som används i tjänsten kombinerar tvingad inloggning och stark hårddiskkryptering för fasta och bärbara arbetsstationer. På så sätt blir konfidentiella data som lagras på hårddisken inte tillgängliga för obehöriga personer. Funktionen möjliggör en hög informationssäkerhetsnivå vid fjärr- och mobilt arbete utan att informationssäkerheten äventyras. Hårddiskkrypteringsprogrammet genomför krypteringen i bakgrunden utan att användaren märker det.

En databas underhålls i leverantörens tjänstehanteringssystem på arbetsstationer som ingår i tjänsten.

En kundspecifik krypteringspolicy definieras före driftsättning av tjänsten.

2.3.1.2 Tvingad autentisering

Vid hantering av krypterade data måste användare logga in med sitt användarnamn och lösenord eller någon annans slags identifiering. Efter inloggning är data på hårddisken tillgängliga för användaren. Efter en fördefinierad inaktivitetsperiod blir data automatiskt låsta.

Enhetens låsningstid anges i krypteringspolicyn.

2.3.1.3 Återställning av lösenord

Om en användare glömmer sitt lösenord kan leverantörens Service Desk låsa upp den låsta arbetsstationen med användarens hjälp. Upplåsning av ett lösenord kräver att krypteringsprogrammet på datorn har installerats i enlighet med leverantörens krypteringsinställningar och specifikationer. Det kräver också att den kod som är kopplad till enheten lämnas till Service Desk eller att användaren kan identifieras på något annat tillförlitligt sätt innan frisläppningskoden skickas.

2.3.1.4 Krypteringsnycklar och inställningar

Leverantören behåller krypteringsinställningarna och de policyer som används vid installation i systemet.

Krypteringsspecifikationer och policyer implementeras i samarbete med kunden, i enlighet med den gemensamt överenskomna informationssäkerhetspolicyn. Specifikationerna för krypteringsinställningarna och policyerna genomförs som ett separat projekt utanför bastjänsten.

Det är kundens ansvar att på ett säkert sätt förvara de krypteringsnycklar som skapas vid installation av krypteringsprogrammet, om inte annat överenskommits med kunden (t.ex. om återställningsnycklar förvaras i Active Directory-tjänsten (AD) och kundens AD är leverantörens ansvar).

2.3.1.5 Programvaruuppdateringar

Bastjänsten omfattar installation av nödvändiga Service Pack, Service Releaser och Security Fix-programuppdateringar som programvaruleverantören rekommenderar för krypteringsprogrammet. Uppdateringen hanteras via överenskommet distributionssätt enligt punkt 2.5.1.6..

Krypteringsprogrammet kan kräva uppdatering av operativsystemversionen eller på Service Pack-nivå, varigenom dessa uppdateringar utförs som separat arbete utanför bastjänsten.

Andra uppgifter, t.ex. driftsättning eller uppdatering av en ny programversion, genomförs som ett separat projekt utanför bastjänsten.

2.3.1.6 Programdistribution

Förberedelse av ett installationspaket innefattar planering av installationen av krypteringsprogram med följande alternativa distributions- och installationsmetoder:

- Inställningar för Active Directory Group Policy.
- Microsofts distributionsprogram SCCM.
- Nätverksdrivrutin eller netlogon-skript.
- Manuell installation från en dedikerad installations-cd.
- Vissa andra metoder som används av leverantören.

Innan tjänsten startar måste krypteringsprogrammet installeras på alla datorer som ingår i tjänsten. Förinstallation i datorerna hanteras vid initieringen av Tjänsten som ett separat projekt.

2.3.2 Tillval

2.3.2.1 Implementering som helhetstjänst

Leverantören äger och är ansvarig för tjänsterelaterad maskinvara, programvara, licenser och supportavtal för dessa. Leverantören är ansvarig för kundens licenser till krypteringsprogram som omfattas av tjänsten och underhållsavtal för detta.

Slutanvändarsupport som ingår i tjänsten gäller endast uppgifter som rör nedmontering av krypteringstjänsten eller frisläppning av lösenord. Andra former av slutanvändarsupport ingår inte i tjänsten som beskrivs i denna tjänstebeskrivning.

Förutsättningar för tjänsten:

- Arbetsstationerna måste ha tillräcklig processkapacitet, minne och diskutrymme.
- Alla operativsystem som ingår i tjänsten måste möjliggöra installation av krypteringsprogrammet.
- Krypteringsnycklar som genereras vid installation av krypteringsprogram ska lagras på kundens nätverkshårddisk eller nätverks-AD-tjänst, vilkas data säkerhetskopieras regelbundet (om inte annat överenskommits för lagring av krypteringsnycklar).
- Initieringsprojektet, då säkerhetspolicyer och regler specificeras tillsammans med kunden, ska ha slutförts.
- Leverantören är inte ansvarig för några defekter i programvaran eller följder av detta. Leverantören ska om möjligt meddela kunden om sådana defekter utan onödigt dröjsmål. Leverantören ska försöka övertyga programvarutillverkaren eller licensleverantören om att åtgärda felet.

2.3.2.2 Implementering som en hanterad tjänst

Efter separat överenskommelse kan krypteringstjänsten för arbetsstationer implementeras med kundägda licenser och/eller med hjälp av en leverantörshanterad nyckel, som en s.k. hanterad tjänst.

Vid användning av kundägda licenser bär kunden ansvar för att rapportera till huvudman och säkerställa att licenserna är uppdaterade.

Utöver de punkter som räknas upp i föregående avsnitt kräver användning av dedikerade licenser att den licensierade produkten levereras med huvudproduktsupport, och att leverantören har behörighet att använda den och att produkten ingår i den tjänst som leverantören stödjer.

Nedanstående ska beaktas när leveransen tillhandahålls med leverantörshanterade krypteringsnycklar:

- En fungerande datauppkoppling krävs mellan kundens nätverk och leverantörens datacentral.
- Kunden är ansvarig för eventuella datauppkopplingar som behövs och för inköps- och driftskostnader.
- Datauppkopplingen ska vara lämplig för att tillhandahålla tjänsten, och en dirigering för anslutningen ska öppnas från leverantörens nätverk till nätverkssegmenten för alla arbetsstationer i tjänsten.
- Nödvändiga resurser för att lagra och säkerhetskopiera krypteringsnycklar.
- Krypteringspolicyn ska följa leverantörens rekommendationer.

Leverantören är inte ansvarig för några defekter i programvaran eller följder av detta. Leverantören ska om möjligt meddela kunden om sådana defekter utan onödigt dröjsmål. Leverantören ska försöka övertyga programvarutillverkaren eller licensleverantören om att åtgärda felet.

2.3.2.3 Kryptering av portabel utrustning

Tjänsten kan kompletteras med kryptering av enskilda filer och externa/portabla minnesenheter. Detta möjliggör överföring och lagring av filer utanför systemet, men fortfarande i krypterat format. Avkryptering av krypterade filer i ett externt system kräver inte alltid ett specifikt krypteringsprogram.

Driftsättning av tilläggstjänsten måste överenskommas separat med leverantören.

2.3.3 Uppgifter som debiteras separat

Nedanstående uppgifter debiteras separat:

- Datauppkopplingar mellan kunden och leverantören.
- Slutanvändarutbildning.
- Skapande av krypteringsinställningar och -regler.

2.3.4 Begränsningar och ansvar

Leverantören är inte ansvarig för några defekter i programvaran eller följder av detta. Leverantören ska om möjligt meddela kunden om sådana defekter utan onödigt dröjsmål. Leverantören ska försöka övertyga programvarutillverkaren eller licensleverantören att åtgärda felet.

2.3.5 Rapportering

Antalet arbetsstationer som ingår i tjänsten rapporteras.

2.3.6 Aktiviteter vid initiering av tjänst

Initiering av tjänst innefattar följande uppgifter:

- Specificering av krypteringsinställningar och regler tillsammans med kunden.
- Installation av krypteringsprogram i de maskiner som ingår i tjänsten och lagring av krypteringsnycklar på kundens nätverkshårddisk eller nätverks-AD-tjänst.
- Leverantören kontrollerar och accepterar systemkonfigurationer och funktioner tillsammans med kunden.
- Leverantören dokumenterar tjänstesystemet i leverantörens informationssystem.
- För kundunika system ska Kunden se till att programsupport och kontaktpersoner finns tillgängliga hos tillverkaren.

2.3.7 Ändringar

Standardsystemändringar som ingår i bastjänsten definieras i ändringshanteringsprocessen. Övriga förändringar genomförs enligt gällande konsultprislista.

2.3.8 Aktiviteter efter uppsägning

När tjänsten sägs upp upphör de tjänster som inrättats under startfasen och produktion, kunddata tas bort från datalager och användningen av tjänsterelaterade verktyg upphör. En plan för uppsägningen av tjänsten upprättas och leverantören utser en person som ansvarar för uppsägningen.

2.3.9 Teknik som stöds

Tjänsten stödjer följande operativsystem

- Microsoft Windows 7 (32 bitar och 64 bitar) eller högre version

2.4 Tjänstemodul för datorsäkerhet

Datorsäkerhet omfattar programvara för virusskydd, skydd mot skadlig kod, hantering av brandväggsprogram. Tjänsten kan leveraras enligt 2 alternativ, som molntjänst från Leverantören eller som Tjänst på Kundägd plattform.

2.4.1 Innehåll och uppgifter

Virusskyddsprogrammet som är installerat på kundens maskiner hanteras centralt av leverantören.

Tjänsten innehåller:

Virusskyddsprogram. Virusskyddsprogrammet upptäcker, förhindrar, avaktiverar eller avlägsnar virus och maskar.

Skydd mot skadlig kod. Skyddsprogram söker och avlägsnar olika typer av spionprogram och skadlig kod.

Brandvägg. Brandväggen i arbetsstationer skyddar mot obehörig access av förbjuden nätverkstrafik.

Tjänsten är beroende av en säkerhetspolicy. Säkerhetspolicyn definieras av Kunden i samråd med Leverantören vid initieringen av Tjänstemodulen.

Huvudanvändarsupport ingår i tjänsten, vilket innebär att leverantörens supporttekniker vägleder kundens huvudanvändare i användningen av programmet.

2.4.1.1 Realtidsunderhåll av virusdatabas

Databaser över virussignaturer och signaturer för skadlig kod uppdateras regelbundet av Leverantören. Leverantören övervakar vad som händer på marknaden och följer programleverantörernas rekommendationer. Bastjänsten omfattar löpande distribution för uppdateringar av program, anti-virussignaturer och signaturer mot skadlig kod för att hålla säkerheten uppdaterad.

2.4.2 Uppgifter som debiteras separat

Versionsuppgradering av mjukvara som kräver separat projekt som kräver mer än 16h arbetstid.

Utformning, implementering och uppdatering av brandväggsregler som begärts specifikt av kunden genomförs som separata projekt utanför bastjänsten.

Manuell installation eller konfiguration av mjukvara på datorer som av någon anledning inte kan hanteras via implementerad distributionsmotor.

2.4.3 Begränsningar och ansvar

Alternativ 1 – Leverans som helhetstjänst

Leverantören ansvarar för central plattform som krävs för att Tjänsten ska fungera. Leverantören levererar Tjänsten från en delad plattform. Dedikerad plattform kan levereras vid särskild överenskommelse.

Leverantören är ansvarig för licenserna för virusskyddsprogrammet och underhållsavtalen för detta. Leverantören väljer mjukvaruplattform.

Förutsättningar för Tjänsten:

- Leverantörens supporttjänst för slutanvändare.

- En fungerande datauppkoppling mellan kundens nätverk och leverantörens datacentral. Kunden är ansvarig för eventuella datauppkopplingar som behövs. Datauppkopling kan levereras av Leverantören enligt annan Tjänstemodul. Dataanslutningen ska vara lämplig för att tillhandahålla tjänsten och dirigering av http-protokoll ska öppnas från leverantörens nätverk till alla kundens nätverkssegment som är anslutna till tjänsten.
- Enheterna måste ha tillräcklig processkapacitet, minne och diskutrymme.
- Firmware och operativsystem som möjliggör installation av valt virusskyddsprogram.
- Ett startprojekt under vilket virusskyddspecifikationer och brandväggsregler dokumenteras tillsammans med kunden.

Alternativ 2 – Leverans som Tjänst på Kundägd plattform

Virusskyddstjänsten kan implementeras med hjälp av kundens egen serverutrustning, licenser och/eller hanteringsservrar i kundens lokaler som en s.k. hanterad tjänst.

Tjänsten inkluderar huvudanvändarsupport, som innebär att leverantörens medarbetare ger råd till kundens utsedda huvudanvändare om hur man använder den programvara som ingår i tjänsten.

Slutanvändarsupport ingår i den hanterade tjänsten som ett tillval.

Produceras tjänsten med kundägda licenser är kunden ansvarig för att säkerställa deras giltighet och för att rapportera till huvudmannen.

Förutsättningar för tjänsten – Kundens ansvar:

- Den licensierade produkten ska levereras med huvudproduktsupport, och leverantören ska ha rätt att använda den.
- Produkten som definierats för användning i tjänsten har stöd av leverantören.
- Produceras tjänsten i kundägd serverutrustning och/eller en hanteringsserver i kundens lokaler ska kunden säkerställa utrustningens kapacitet och tillgänglighet.
- Systemkonfigurationen ska följa rekommendationerna från tillverkaren av virusskyddsprogrammet/maskinvaran
- Att det finns en fungerande datauppkoppling mellan kundens nätverk och leverantörens datacentral.
- Att systemet ingår i leverantörens övervaknings- och hanteringstjänster.

Ansvarsbegränsning vid leverans av både alternativ 1 och 2 ovan.

Tjänsten inkluderar inte instruktioner om hur virus avlägsnas från maskinvara eller relaterad vägledning, slutanvändarsupport eller andra åtgärder, oavsett om tjänsten levereras med hjälp av leverantörsägd utrustning och licenser från kundlokaler, eller med hjälp av kundägd serverutrustning, licenser och/eller från hanteringsservrar i kundens lokaler.

Leverantören är inte ansvarig för några direkta eller indirekta skador som kunden åsamkas på grund av en egenskap i virusskyddsprogrammet eller defekter i själva programmet, som applikationstillverkaren inte kände till eller som inte upptäcktes under pilotfasen.

2.4.4 Rapportering

En sammanfattning av enheterna och de senaste uppdateringarna levereras regelbundet till kundens kontaktperson. Standardrapporteringsfrekvens är en månad.

2.4.5 Aktiviteter vid initiering

Vid initiering av tjänsten:

- Ska Kunden säkerställa att det finns en datauppkoppling mellan kundens nätverk och leverantörens datacentral om inte detta köps som en Tjänst från Leverantören.
- Ska Leverantören installera virusskyddprogram på de enheter som ingår i tjänsten.

- Parterna tillsammans skapa en säkerhetspolicy som specificerar virusskyddsregler och brandväggsregler.
- Ska Leverantören kontrollera att systemkonfigurationen fungerar.
- För kundunika system ska Kunden se till att programsupport och kontaktpersoner finns tillgängliga hos tillverkaren.

2.4.6 Ändringar

Omfattande ändringar som påverkar tjänsteleveransen verkställs alltid som separata projekt. Byte av virusskyddsprodukter räknas som en sådan ändring.

2.4.7 Aktiviteter efter uppsägning

När tjänsten sägs upp upphör de tjänster som inrättats under startfasen och produktion, kunddata tas bort från datalager och användningen av tjänsterelaterade verktyg upphör. En plan för uppsägningen av tjänsten upprättas och leverantören utser en person som ansvarar för uppsägningen.

2.4.8 Teknik som stöds

Leverantören stödjer följande produkter:

- F-Secure
- McAfee
- Symantec
- Microsoft UAG

Leverantören har en lista över de versioner av produkterna som stöds.

3 Uppgifter som debiteras separat

Nedanstående uppgifter debiteras alltid separat:

- Problemhanteringsuppgifter som utförs av leverantörens personal, förutsatt att problemet inte orsakades av något som är leverantörens ansvar.
- Arbete utanför åtgärdstiden.
- Separat avtalade utredningar och verifieringar av IT-arbetsplatsmiljö.
- Prestandamätning på Kundens uppdrag.

4 Begränsningar och ansvar

Leverantören levererar endast Tjänster i miljöer som stöds av dator- eller programtillverkaren.

Om tillverkaren upphör att stödja operativsystem, systemprogramvara eller serverapplikationer gäller inte längre den överenskomna tjänstenivån och kontraktsparterna måste förhandla om en ny miljö som ersätter den gamla. Leverantören har rätt att efter eget gottfinnande debitera kunden för kostnader för problemlösning efter det att stöd upphört.

5 Rapportering

Tjänsten rapporteras per specifik tjänstekomponentenhet.

6 Tjänstemodulernas livscykel

Leverantören livscykelhanterar samtliga standardtjänster. Detta innebär att Leverantören underhåller de plattformar som krävs för att upprätthålla Tjänsten samt utvecklar Tjänstemodulernas funktioner och avvecklar de tjänster som passerat bäst före datum. Kunden tar del av de nya funktioner som Leverantören tillhandahåller inom den versionen som blivit implementerad hos Kunden (normalt all utveckling av plattformar som inte kräver migrering till ny plattform). För att ta del av nya versioner (vilket oftast kräver migrering) så beställer Kunden uppgradering/migrering som separat projekt.

6.3 Aktiviteter vid initiering av tjänst

Initiering av Tjänstemodulerna sker i separat transitions/transformations-projekt tillsammans med Kunden. En detaljerad beskrivning och omfattning av initieringsfasen tillhandahålls per Tjänstemodul.

Initieringen accepteras som slutförd baserat på initieringsdokumentation efter ett gemensamt beslut av Kunden och Leverantören. Kunden är ansvarig för sina egna och systemleverantörens startkostnader.

6.4 Ändringar i tjänsten

Leverantören har rätt att ändra Tjänstens tekniska miljö utan överenskommelse med kunden i de fall då Tjänsten köps som funktion. Dock kommer förändringar som påverkar kundens tjänst alltid att överenskommas med kunden.

6.5 Aktiviteter efter uppsägning av tjänst

Efter uppsägning nedmonteras alla tjänster som beskrivs i tjänstebeskrivningen samt de tjänster som rör tjänsteinitiering och tjänsteleverans. Ett gemensamt avvecklingsprojekt upprättas, som innefattar följande uppgifter:

- Kommunikation.
- Borttagning av användarkonton från leverantörens system.
- Borttagning av dokumentation.
- Borttagning från tjänstehanteringssystem.
- Data som lagrats hos leverantören levereras till kunden (t.ex. innehåll i tillgångsregister) och kunddata från tjänsteobjekten förstörs.
- Upphörande av rapporteringsprocess.
- Nedmontering av datakommunikationsanslutningar.
- Överlämnande av uppgifter rörande finansiell hantering till kunden.

Avvecklingsprojektet debiteras enligt gällande konsultprislista.