Allmänna villkor

för infrastrukturen Mina meddelanden

Bilaga 1

Krav på säkerhet för brevlådeoperatörer

version 1.2

(Gäller fr.o.m. 2015-11-11)

Bakgrund och syfte

Skatteverket tillhandahåller en myndighetsgemensam infrastruktur för säkra elektroniska försändelser från myndigheter till enskilda enligt förordningen (2003:770) om statliga myndigheters elektroniska informationsutbyte.

Krav på säkerhet för Brevlådeoperatörer syftar till att etablera gemensamma krav för Brevlådeoperatörer, och att upprätthålla en hög grad av säkerhet och tillförlitlighet inom hela infrastrukturen för Mina Meddelanden.

1. Organisation och styrning

K1.1 Brevlådeoperatörer ska vara registrerade i aktiebolags- eller handelsregister eller liknande register, för mervärdesskatt, som arbetsgivare (där så är fallet)samt inneha F-skattebevis. Brevlådeoperatörer ska vara fri från skulder för svenska skatter och/eller socialförsäkringsavgifter hos Skatteverket och Kronofogden.

K1.2 Brevlådeoperatörer ska teckna och vidmakthålla för verksamheten erforderliga försäkringar.

K1.3 Brevlådeoperatörer ska ha en etablerad verksamhet, vara fullt operationell i alla delar som berörs i detta dokument, och vara väl insatt i de juridiska krav som ställs på denne som tillhandahållare av brevlådeoperatörstjänst.

K1.4 Brevlådeoperatörer ska förfoga över tillräckliga ekonomiska medel för att kunna bedriva verksamheten i minst 1 år samt kunna bära risken för skadeståndsskyldighet.

K1.5 Hela leveransen som omfattas av de allmänna villkoren (inkl tjänster och personal) ska ske inom EU/EES. Åtkomst till brevlåda via användargränssnitt kan dock ske utanför EU/EES av brevlådeinnehavare.

K1.6 En brevlådeoperatör som i enlighet med de Allmänna villkoren har anlitat underleverantör för utförandet av en eller flera säkerhetskritiska processer, ska genom skriftligt avtal definiera vilka kritiska processer som underleverantören är ansvarig för och vilka säkerhetskrav som är tillämpliga på dessa.

2. Informationssäkerhet

K2.1 Brevlådeoperatörer ska för de delar av verksamheten som berörs i detta dokument ha ett ledningssystem för informationssäkerhet (LIS) som i tillämpliga delar baseras på ISO/IEC 27001 eller motsvarande.

K2.2 Samtliga säkerhetskritiska administrativa, organisatoriska och tekniska processer ska dokumenteras och vila på en formell grund, där roller, ansvar och befogenheter finns tydligt definierade.

K2.3 Brevlådeoperatörer ska utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet, samt säkerställa att denne vid var tid har tillräckliga personella resurser till förfogande för att uppfylla sina åtaganden på ett betryggande sätt.

K2.4 Brevlådeoperatören ska ha definierad, dokumenterad och till berörda roller kommunicerat ansvar för skyddet av informationen i tjänsten.

K2.5 Brevlådeoperatörer ska inrätta en process för riskhantering som på ett ändamålsenligt sätt regelbundet analyserar hot och sårbarheter i verksamheten, och som genom införande av säkerhetsåtgärder balanserar riskerna till acceptabla nivåer.

K2.6 Brevlådeoperatörer ska inrätta en process för incidenthantering som systematiskt säkerställer kvaliteten i tjänsten, former för vidarerapportering och att lämpliga reaktiva och preventiva åtgärder vidtas för att lindra eller förhindra skada vid händelser som lett till eller kunnat leda till en incident.

K2.7 Brevlådeoperatörer ska upprätta och testa en kontinuitetsplan som tillgodoser verksamhetens tillgänglighetskrav genom en förmåga att återställa kritiska processer vid händelse av katastrof eller allvarliga incidenter.

K2.8 Brevlådeoperatören ska ha en dokumenterad och fungerande process för styrning och ändring av IT-system i enlighet med vedertagna principer.

K2.9 Ledningen inom Brevlådeoperatörer ska löpande informera sig om arbetet med informationssäkerheten samt minst en gång per år följa upp, utvärdera och förbättra detta arbete.

3. Spårbarhet och skydd mot informationsförlust

K3.1 Lagrade uppgifter, behandlingshistorik och andra uppgifter, ska säkerhetskopieras tillräckligt ofta för att säkerställa att uppgifterna skyddas mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring. Säkerhetskopiorna ska förvaras fysiskt åtskilda från och omfattas av samma skydd som de lagrade uppgifterna.

K3.2 Säkerhetskopiorna ska utplånas då de inte längre behövs.

K3.3 Säkerhetslogg och annan säkerhetsrelaterad information ska produceras och sparas i 2 år. Leverantören ska aldrig i någon situation lämna ut uppgifter om systemen, funktionen eller dess information. Uppstår en situation där någon hos/via leverantören vill begära ut allmän handling som upprättats av Skatteverket eller annan myndighet, ska denna hänvisas till Skatteverket.

K3.4 Dokumentation av tjänsterna, driftmiljön och där ingående komponenter ska skyddas från obehörig åtkomst.

4. Fysisk, administrativ och personorienterad säkerhet

K4.1 Verksamhetens centrala delar ska skyddas fysiskt mot skada som följd av miljörelaterade händelser, otillåten åtkomst eller andra yttre störningar. Tillträdeskontroll ska tillämpas så att åtkomst till känsliga utrymmen är begränsad till endast behörig personal, att informationsbärande lagringsmedia och pappersdokument förvaras på ett säkert sätt, och att tillträde till dessa skyddade utrymmen kontinuerligt övervakas och dokumenteras.

K4.2 Innan en person antar någon av de roller som är av särskild betydelse för säkerheten, ska brevlådeoperatören ha genomfört bakgrundskontroll i syfte att förvissa sig om att personen kan anses vara pålitlig samt att personen har de kvalifikationer och den utbildning som krävs för att utföra de arbetsuppgifter som följer av rollen på ett tillfredsställande, korrekt och säkert sätt.

K4.3 Personal hos leverantören ska innan de börjar arbeta med tjänsterna skriva under ett sekretessavtal av vilket det framgår ansvar för informationssäkerheten och att data/information som berör tjänsterna endast får användas för lämplig verksamhetsutövning.

K4.4 Innan personal ges åtkomst till utrustning för tjänsterna ska denne vara registrerad som behörig användare och har fått utbildning i de regler och säkerhetsinstruktioner som gäller för systemet.

K4.5 När åtkomst till utrustning för tjänsterna sker via en inloggningsprocess ska en lämplig rutin för in- och utloggning finnas.

K4.6 Allokering och användning av rättigheter ska begränsas och kontrolleras och personal ges en behörighetsprofil som endast medger åtkomst till de resurser i utrustning för tjänsterna som krävs för att lösa dennes arbetsuppgifter.

K4.7 Alla användare ska ha och använda en unik personlig identifierare (användaridentitet) så att aktiviteter kan spåras tillbaka till ansvarig användare. Användaridentitet och lösenord eller motsvarande används för att verifiera en användares påstådda identitet. Det ska finnas regler för utformning, byte och hantering av lösenord.

K4.8 Det ska finnas en säkerhetslogg som ska omfatta användaridentitet, inloggning, utloggning, aktivitet samt datum och klockslag.

K4.9 Brevlådeoperatörer ska säkerställa spårbarheten vid all logisk och fysisk åtkomst till känsliga IT-system. Åtkomst ska kunna härledas på individnivå, och identifieringen ska ske på ett betryggande och säkert sätt.

5. Teknisk säkerhet

K5.1 Brevlådeoperatören ska kunna visa att de tekniska kontroller som finns införda är tillräckliga för att uppnå den skyddsnivå som behövs med hänsyn till verksamhetens art, omfattning och övriga omständigheter, och att dessa kontroller fungerar och är effektiva.

K5.2 Kommunikation över allmänna telekommunikationsnät eller andra kommunikationslänkar som inte är fysiskt skyddade ska begränsas och ömsesidigt identifieras, samt skyddas mot insyn, manipulation och återuppspelning.

K5.3 Innehåll i brevlådor ska lagras krypterat med AES och minst 128 bits nyckellängd och en mode som är lämpad för ändamålet.

K5.4 Känsligt kryptografiskt nyckelmaterial ska skyddas så att:

(a) åtkomst begränsas, logiskt och fysiskt, till de roller och de tillämpningar som oundgängligen kräver det,

(b) nyckelmaterialet aldrig lagras i klartext på beständigt lagringsmedia,

(c) **Skyddsklass 3:** nyckelmaterial som brevlådeoperatören hanterar för brevlådeinnehavares räkning ska skyddas när det inte är under användning, direkt eller indirekt, via kryptografisk hårdvarumodul med aktiva säkerhetsmekanismer som skyddar mot både fysiska och logiska försök att röja nyckelmaterialet.

(d) **Skyddsklass 3:** säkerhetsmekanismerna för skydd av nyckelmaterial enligt K5.4(c) ovan är genomlysta och baserade på erkända och väletablerade standarder.

K5.5 Brevlådeoperatören ska ha kontinuerlig omvärldsbevakning av de produkter och tekniker som används i tjänsten, samt ändamålsenlig beredskap för förändrade risknivåer.

K5.6 Säkerhetsuppdateringar av all programvara i utrustning för tjänsterna ska göras skyndsamt så snart de finns tillgängliga.

K5.7 Leverantören ska ha dokumenterade rutiner för säker hantering, lagring och destruktion av flyttbara media i syfte att skydda data från obehörig åtkomst.

K5.8 Leverantören ska tillse att data raderas eller görs otillgänglig före kassering eller återanvändning i syfte att skydda data för obehörig åtkomst.

K5.9 Leverantören ska ansvara för att det finns upptäckande och förebyggande kontroller för skydd mot skadlig kod (virus, etc.) i den utrustning inom leverantörens domäner som används för tjänsterna. Dessa skydd ska alltid vara uppdaterade till senaste version.

6. Hantering av användare

Information om användaravtal och villkor

K6.1 Brevlådeoperatören ska tillhandahålla uppgifter om användaravtal, villkor samt anknytande uppgifter och eventuella begränsningar i användandet av tjänsten till anslutna användare.

K6.2 En brevlådeoperatör ska utforma sina användarvillkor tydligt och i enlighet med de Allmänna villkoren. Brevlådeoperatören ska även säkerställa att villkoren kommer användaren tillhanda innan denne undertecknar eller annars ingår avtal med brevlådeoperatören.

Registrering

K6.3 Brevlådeoperatören ska, beaktat reglerna för personuppgiftshantering, föra register över anslutna användare och de kopplade elektroniska brevlådorna, och hålla detta register aktuellt.

Identifiering och åtkomst

K6.4 Efter att behörig Brevlådeanvändare har identifierat sig enligt tillitsnivå 2 eller högre får Brevlådeoperatören ge denne:

a) åtkomst till brevlådan, dess inställningar och anknytande uppgifter

b) möjlighet att läsa och ta bort meddelanden av skyddsklass 1 och 2.

K6.5 Efter att behörig Brevlådeanvändare har identifierat sig enligt tillitsnivå 3 får Brevlådeoperatören ge denne möjlighet att läsa och ta bort meddelanden av skyddsklass 3.

K6.6 En Brevlådeanvändare är direkt behörig gällande en specifik Brevlådeinnehavare endast om Brevlådeanvändaren uppfyller minst ett av följande villkor:

- Brevlådeanvändaren är Brevlådeinnehavare (gäller endast för fysisk person och enskild firma)
- Brevlådeanvändaren är verkställande direktör (VD) för Brevlådeinnehavaren (gäller endast för aktiebolag och ekonomisk förening). Ska kontrolleras mot Bolagsverkets register över juridiska personer.

- Brevlådeanvändaren är extern verkställande direktör (EVD) för Brevlådeinnehavaren (gäller endast för aktiebolag och ekonomisk förening). Ska kontrolleras mot Bolagsverkets register över juridiska personer.
- Brevlådeanvändaren är firmatecknare för Brevlådeinnehavaren (gäller endast för aktiebolag, handelsbolag, kommanditbolag och ekonomisk förening). Ska kontrolleras mot Bolagsverkets register över juridiska personer.

K6.7 Brevlådeoperatören kan tillåta att Brevlådeinnehavare ger indirekt behörighet till annan Brevlådeanvändare att läsa och hantera meddelanden i Brevlådan samt administrera inställningar.

Uppsägning, avregistering och borttag av uppgifter

K6.8 På användares begäran ska meddelanden som lagras i dennes brevlåda tas bort på ett säkert sätt.

K6.9 Brevlådeoperatören ska tillhandahålla en funktion där användaren kan säga upp tjänsten. Brevlådeoperatören ska då en sådan begäran mottagits avregistrera användaren samt ta bort meddelanden och andra lagrade uppgifter i brevlådan.

K6.10 En brevlådeoperatör som upphör med sin verksamhet kring anslutningen till infrastrukturen för Mina Meddelanden ska informera anslutna användare och erbjuda dem möjlighet och skälig tid att föra ut meddelanden från brevlådan.

7. Granskning och uppföljning

Granskning och uppföljning

K7.1 Brevlådeoperatören ska säkerställa att dokument som stöder efterlevnaden av de krav som ställs på brevlådeoperatören, och som visar att de säkerhetskritiska processerna finns och fungerar ständigt är uppdaterade.

K7.2 Ledningssystemet för informationssäkerhet och efterlevnaden av samtliga krav som ställs på brevlådeoperatören ska under en treårsperiod vara föremål för internrevision, utförd av oberoende intern kontrollfunktion, såvida inte organisationens storlek eller annan försvarbar orsak motiverar att revision sker på annat sätt.

Rapporteringsskyldighet

K7.3 Resultatet av den egenkontroll som ska utföras i enlighet med 7.2 samt den dokumentation som i övrigt stöder efterlevnaden av de krav som följer av de Allmänna villkoren enligt 7.1, ska på förfrågan tillhandahållas Skatteverket.

K7.4 Skulle sådan säkerhetsincident inträffa, där det inte kan uteslutas att sekretessbrott eller annan allvarlig störning förekommit, ska sådan incident omgående rapporteras till Skatteverket.