Dataskydds- och informationssäkerhetspolicy

1 Inledning

Som anställd hos Citymail AB, nedan kallat CM eller företaget, är du en del av CM. Allt du gör inom ramen för din anställning är CM och när du agerar gör du det i egenskap av representant för företaget. De lagar och regler som CM är skyldig att följa gäller således även dig som anställd och eventuella misstag från din sida kommer att belasta CM.

Denna policy beskriver de skyldigheter CM och du som anställd har i förhållande till dataskyddslagstiftning och postlagen samt de skyldigheter, utöver detta, som du som anställd har i förhållande till CM inom området data- och informationssäkerhet samt integritetsskydd för avsändare och postmottagare.

Genom denna policy avser företaget att göra det enklare för dig som anställd att veta hur du skall agera. Instruktionerna i policyn är generella och deras avsikt tillsammans med ditt egna tänkande ger ett gott skydd av verksamheten och dess tillgångar.

Om du upplever att policyn har brister, saknar något eller om något verkar felaktigt, så uppmuntrar vi dig till att kontakta Kvalitetschef.

2 Brott mot CityMail dataskydds- och informationssäkerhetspolicy

Denna policy gäller alla medarbetare och alla delar inom organisationen. Det finns inte utrymme att besluta om lokala regler som avviker från denna.

Brott mot denna policy kan medföra att vi tvingas ompröva ditt anställningsförhållande eller vidta andra rättsliga eller disciplinära åtgärder.

Brott mot tystnadsplikt såväl som att bryta brevhemligheten är allvarliga lagöverträdelser och kan enligt brottsbalken straffas med böter eller fängelse.

3 Informationssäkerhet

Information är en av CM:s viktigaste tillgångar. Hanteringen av den är en viktig del i arbetet att säkerställa vår förmåga att fullfölja det vi åtagit oss samt hantera möjligheter och risker.

Utgångspunkter i vårt arbete med informationssäkerhet är:

- Lagar och förordningar
- Våra egna krav och informationssäkerhetsmål
- Avtal

Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av i vilken form eller miljö den

förekommer. Informationssäkerheten omfattar CM:s informationstillgångar utan undantag. Med informationssäkerhet avses:

- att rätt information är tillgänglig för rätt person när den behövs och på ett behörighetsstyrt sätt
- att information inte lämnas ut eller görs tillgänglig för obehöriga
- att informationen är och förblir riktig

Informationssäkerheten är en integrerad del av vår verksamhet. Företagshemligheter kan användas för att skada CM och om information som vi har om andra, t ex postmottagare, hamnar i orätta händer kan leda till stor skada för den enskilde. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt både verka för en positiv attityd till säkerhetsarbetet såväl som till de rutiner som syftar till att hålla våra informationstillgångar uppdaterade och korrekta.

Var och en ska vara uppmärksam på och rapportera händelser som kan påverka säkerheten för våra informationstillgångar. Exempel på detta kan vara telefonsamtal med frågor kring vår IT-miljö och våra informationstillgångar. Hänvisa sådana samtal och sådana misstankar direkt till Kvalitetschef.

4 Behandling av personuppgifter

Behandling av personuppgifter är strängt reglerat i dataskyddsförordningen (GDPR), EU 2016/679.

4.1 Vad är en personuppgift?

En personuppgift definieras som:
- varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet

4.2 Vad är en behandling?

En behandling definieras på motsvarande sätt som:
- en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

4.3 Vad krävs för att få göra en behandling av personuppgifter?

Grunden i vårt förhållande till integritetsskydd av personuppgifter är att vi aldrig behandlar personuppgifter om vi inte måste för att lösa en arbetsuppgift.

Vid behandling av personuppgifter inom CM gäller att behandlingen ska vara laglig, följa företagets uppsatta regelverk (t ex denna policy) och vara korrekt dokumenterad. All annan personuppgiftsbehandling är förbjuden.

Detta innebär att varje behandling som görs, t ex i ett databehandlingsverktyg som Excel bara är tillåten om det finns en dokumenterad rutin som beskriver behandlingen. Vidare att information om postmottagare och kunder endast ska behandlas i CM:s produktions- och affärssystem eftersom rutiner och processer för behandlingen då blir systematiskt prövade mot lagstiftningen, möjliga att gallra och dokumenterade genom vår förvaltningsprocess för IT-system.

4.4 Kan vi lämna ut information till utomstående?

Om en registrerad önskar att få de personuppgifter vi har registrerad om hen så har hen rätt till det givet att vissa villkor uppfylls. Hanteringen av sådana ärenden och bedömningen av vad som kan/ska lämnas ut görs alltid av vårt dataskyddsombud (DSO) och får aldrig görs av enskild medarbetare. För mer information se *Integritetspolicy för postmottagare* respektive *Integritetspolicy för kontaktpersoner* på CM:s externa webbsida.

4.5 Incidentrapportering

En personuppgiftsincident är en säkerhetshändelse som har påverkat sekretessen, integriteten eller tillgängligheten till personuppgifter. En personuppgiftsincident har inträffat om personuppgifter har förstörts, om de oavsiktligt eller olagligt gått förlorade eller ändrats, eller om de röjts till någon obehörig. Exempel på incidenter kan vara förlust av en dator som innehåller personuppgifter, eller att någon obehörig part har fått tillgång till personuppgifter t ex för att uppgifterna skickats till en mottagare som inte skulle ha uppgifterna eller någon haft en systembehörighet den inte skulle ha.

När en incident har inträffat ska detta omedelbart rapporteras till CM:s dataskyddsombud (DSO) så att en bedömning av riskerna och huruvida incidenten ska rapporteras till tillsynsmyndigheten kan göras.

4.6 Hur behandlas personuppgifter om anställda?

Som arbetsgivare behandlar CM dessa personuppgifter om dig i din roll som anställd:

Namn, adress, kontaktuppgifter inklusive anhöriguppgifter, personnummer, lön, bank och bankkontoinformation, information om indrivningsärende hos Kronofogden, skatteuppgifter, närvaro- och frånvaroinformation, inklusive orsak till frånvaro. I förekommande fall information kring hälsotillstånd i samband med rehabilitering, information om facklig tillhörighet, prestation och information om ev.

misskötsel. Utöver detta sparas information om användning av CM IT-system, utrustning och inpasseringar i lokaler.

Skälen till behandlingarna är för att CM som arbetsgivare ska kunna fullgöra sina åtaganden mot dig som anställd, leda och fördela arbetet, och att följa gällande lagstiftning.

Vi sparar uppgifterna så länge vi behöver för att fullfölja våra åtaganden enligt avtal och lagstiftning. Vill du veta mer om vilka uppgifter vi har om dig, rätta en felaktig uppgift eller ta bort en uppgift kan du vända dig till vårt *Dataskyddsombud*.

5 Tillförlitlighet, skydd av integritet och tystnadsplikt i samband med post och paketbefordring

Post är en juridisk valid och integritetsskyddad kommunikationsform mellan två parter. Postbefordran regleras i postlagen och får bara utföras av organisationer med tillstånd så kallade postoperatörer. PTS är den myndighet som beslutar om tillstånd och utfärdar villkoren för dessa.

Postoperatörens ansvar är att med hög tillförlitlighet befordra brevförsändelser, enligt överenskommelse med avsändaren, till rätt mottagare. Försändelser under befordring av en postoperatör är avsändarens/mottagarens egendom. Postoperatören ansvar för att skyddet av avsändarens och mottagarens integritet upprätthålls genom hela befordringsprocessen. Postoperatören ska också värna den lagstadgade brevhemligheten som är en rättighet mottagare av post har och som innebär att dennes post inte läses eller öppnas innan den nått mottagaren.

CM är en postoperatör och som anställd är du därför bunden av de lagar och villkor som reglerar postbefordran. Kravet att skydda avsändarens och mottagarens integritet medför en lagstadgad tystnadsplikt gällande avsändare, mottagare och förhållanden dem emellan. Brott mot tystnadsplikt såväl som att bryta brevhemligheten är allvarliga lagöverträdelser och kan enligt brottsbalken straffas med böter eller fängelse.

Tystnadsplikten och ansvaret att skydda integriteten och brevhemligheten innebär:

- att du inte får nyttja uppgifter om mottagare eller om de försändelser som befordras på annat sätt än vad som motiveras av arbetsuppgiften
- att information i CM:s system endast får användas i arbete som hänger samman med postbefordran
- att information om avsändare, mottagare, adressändringar och övriga adressuppgifter inte får lämnas till obehörig.
- att endast personal som behöver informationen för att utföra sitt arbete får ha tillgång till de system som innehåller information om avsändare och mottagare

- att alla försändelser ska hanteras på ett sådant sätt att obehöriga inte kan få tillgång till dem. Detta innebär bland annat att bunthanteringsrutiner och packningsrutiner för fordon och cyklar följs samt att dörrar till CMC, terminaler och andra lokaler hålls låsta
- att alla utskrifter innehållande information om kunder, adresser eller mottagare (kamremsor, eftersändningsetiketter mm) ska hanteras på ett sådant sätt att obehöriga inte kan få tillgång till dem. Då dessa utskrifter kasseras ska avfallet hanteras som sekretessavfall
- att det inte är tillåtet att avslöja vilken typ av försändelse som skickas till mottagare och inte heller vem som är avsändare. Detta gäller även i de fall vi sökt en mottagare och denne ringer upp oss
- att försändelser ska delas till avsedd postanordning (postfack, brevinkast eller brevlåda) eller lämnas i reception och därmed aldrig överräckas till person som väntar i t ex porten. Detta innebär även att en försändelse aldrig får fästas på portens anslagstavla eller liknande i fall då mottagare inte kunnat lokaliseras
- att information om portkoder eller motsvarande endast ska användas i utdelning och inte får lämnas till obehöriga med undantag för blåljuspersonal (polis, sjukvård och räddningstjänst) och kronofogden
- att försändelser vi hanterar i vår postbefordran aldrig får öppnas, förstöras eller kastas.

Undantag
I vissa fall görs undantag från tystnadsplikten när myndighet begär uppgifter. Alla sådana begäran hänvisas till, och hanteras av, Kvalitetschef.

Ett annat undantag är när man som anställd i postverksamhet i sin yrkesutövning får tillgång till uppgift som gör att man misstänker brott som kan ge fängelse. Då får man, men är inte tvingad att, anmäla misstanken till berörd myndighet. Även i dessa fall ska Kvalitetschef kontaktas.

6 IT-utrustning och användning

Den IT-utrustning CM tillhandahåller dig är till för att du skall kunna utföra dina arbetsuppgifter. Allt som skapas, lagras eller kommuniceras på företagets utrustning ägs av företaget. Företaget kan när som helst och utan att informera om det ta del av informationen.

CM:s utrustning och system får inte användas på sätt som innebär förstörelse för utrustning, system, information eller strider mot svensk lag.

Du får inte ändra inställningar på utrustningen som påverkar säkerheten på den eller utsätter vårt nätverk för säkerhetsrisker. Exempel på sådant som inte är tillåtet är att stänga av skärmsläckaren som låser datorn eller att ta bort låskoden på en mobil enhet. Du får inte heller ändra inställningar på utrustningen som hindrar IT att komma åt utrustningen.

Det är inte tillåtet att installera licensbaserade program på företagets utrustning utan tillstånd från IT. Det är inte tillåtet att installera program som saknar angivna licensvillkor eller utan tillstånd kopiera licensierade program *(Lag om upphovsmannarätt till litterära och konstnärliga verk (SFS 1960:729))*.

Det är tillåtet att installera appar från Google Play alternativt App Store på av företaget tillhandahållen mobil enhet.

Var försiktig med utrustningen du använder. Ha t ex inte kaffekoppen eller annan vätska där det finns risk att innehållet hamnar i elektronik. Allmän aktsamhet ska iakttagas.

6.1 Privat utrustning

Privat utrustning får inte anslutas till vårt nätverk. Med nätverk avses det fasta och trådlösa nätverk som företaget tillhandahåller för våra anställda.

Företagets mail, filer och dokument får inte sparas på privat utrustning eftersom företaget då inte kan garantera säkerheten på utrustningen eller kontrollera spridningen av informationen.

6.2 Inloggningsuppgifter

Du får inte lämna ut dina inloggningsuppgifter till någon. Undantaget är till IT i samband med supportärende. När supportärendet är avslutat ska du omgående byta ut ditt lösenord. Du är ansvarig för konsekvenserna av ett otillåtet utlämnande av inloggningsuppgifter.

Lösenordet är det primära skyddet mot att obehöriga kommer åt information och andra resurser i våra system. Ett svagt lösenord som t ex ord och nummerföljder är mycket lätt att knäcka, det handlar om sekunder för en hacker. CM har därför som krav att lösenord måste bestå av minst 8 tecken, och ska innehålla tecken från minst tre av följande kategorier: gemener, versaler, siffror och specialtecken (t.ex.*@$). Lösenordet ska bytas minst var 12:e månad.

USB-minne

Upphittade eller utdelade USB-minnen eller annan hårdvara skall inte anslutas till företagets utrustning. Var misstänksam även mot USB-minnen märkta med vår egen logotyp.

6.3 Mobil enhet

Mobila enheter, som telefon, surfplatta och liknande, som företaget tillhandahåller är ett arbetsredskap. Uppgifter kring mobil enhet t ex appar och användning av dessa, koordinater vid bland annat utdelning av försändelser samt samtalslistor kan företaget samla in för att förbättra våra tjänster samt för att undersöka eventuell för företaget skadlig användning.

6.4 Trådlösa nätverk

Datorn är utrustad med skydd mot intrång. Användning av trådlösa nätverk utanför hemmet och arbetsplatsen bör trots detta undvikas. I hemmiljö skall en router användas mellan dator och internet.

Om du saknar möjlighet att ansluta till företagets nätverk ska du i första hand använda din mobila enhets *Hot Spot* för anslutning. Ansluter du utrustning till okänt nätverk finns risk att trafiken avlyssnas. Används VPN höjs säkerheten varför VPN alltid ska användas vid sådana tillfällen.

6.5 Internet

Att ladda ned filer från Internet är riskfullt eftersom de kan innehålla virus eller skadlig kod. Undvik därför detta om du inte litar på källan.

6.6 Våra egna affärsverksamhetssystem

Privat användning av företagets affärsverksamhetsystem är inte tillåten. Detta inkluderar alla system som innehåller bolagets data eller uppgifter om anställda och andra t ex Citybase, Navision och personalsystemet. För dessa system är användande uttryckligen förbjudet för andra syften än vad som ingår i arbetsuppgifterna.

6.7 E-post

Din e-postadress är knutet till att du jobbar för företaget. När du skickar e-post så framgår företagsnamnet och du representerar då företaget. Allt du skickar kan vidarebefordras, men ursprungsadressen står kvar och innehållet kan påverka företaget negativt. Använd alltid en trevlig ton när du skickar e-post.

Registrera inte din e-postadress hos aktörer för privat kommunikation t ex skola eller nyhetsbrev från föreningar som inte rör arbetet.

Undvik att öppna e-post som du misstänker är spam och svara absolut inte på sådana meddelanden. Det är normalt oklokt att klicka på en länk för att säga upp sig från sändlistan, ”unsubscribe”. Om du vet att avsändaren är seriös kan du naturligtvis göra det men annars bekräftar du bara att din e-postadress existerar.

Var misstänksam när du får bifogade filer. Om du är osäker på innehållet, kontakta avsändaren för bekräftelse.

Allmänt gäller att kommunikation via e-post kan avlyssnas och är därför inte att betraktas som en säker kommunikationsmetod. När vi skickar e-post inom företagets domän är kommunikationen, men inte innehållet, krypterad och kan då betraktas som säker.

Skicka inte filer med personuppgifter i e-post om inte åtgärden är en del av en fastställd och dokumenterat rutin. Skälet till detta är svårigheten att garantera gallring av personuppgifter enligt gällande regler när information duplicerats i e-postsystemet. Om du själv får sådan fil och misstänker att den inte borde skickats via e-post, meddela detta till avsändaren samt meddela vårt *Dataskyddsombud*.

Kommer filen från extern part, ta bort e-postmeddelandet direkt och meddela avsändaren. Fråga *Dataskyddsombudet* eller närmaste chef om du är tveksam.

Känsliga personuppgifter får aldrig skickas via e-post även om kommunikation och utrustning är krypterad.

Rikta e-postmeddelanden till de som verkligen berörs och undvik massutskick.

6.8 Lagring och delning av information

Arbetsinformation som andra än du själv har intresse av ska som regel lagras på avsedd plats i verksamhetsledningssystemet eller någon av de samarbetsytor som avdelningar och enheter använder. Lagra inte arbetsinformation på lokal hårddisk.

Personlig information som du använder i arbetet alternativt sådan som är privat ska i första hand lagras i företagets moln-lösning, OneDrive. Genom lagring på OneDrive säkerställs att data inte försvinner om datorn kraschar. OneDrive ger dig också möjlighet att dela med dig av informationen till andra. Informationen i OneDrive kan synkroniseras med lokal hårddisk vilket möjliggör offline-arbete. Information in din personliga OneDrive är bara tillgänglig för dig själv och vid behov, IT:s administratörer.

7 Tillträde till våra lokaler

7.1 Nyckel och taggsystem

Om du fått en nyckel (fysisk eller digital) för att komma in i CM:s lokaler så får du inte låna ut den. Du får inte heller berätta för andra vilken kod du har. Om du tappar bort din nyckel måste du så fort du upptäckt detta anmäla det till din chef alternativt till nyckelansvarig så att nyckeln kan spärras eller låset bytas.

För att vid behov se vem som vistats i en lokal vid ett specifikt tillfälle, loggas inpasseringar som görs med digital nyckel.

7.2 Besökare

Besök till CM:s lokaler ska vara motiverade av arbetet och godkända av ansvarig chef. Denna är också ansvarig för besökaren under besöket.