# Anvisning för informations- och IT-säkerhet för medarbetare inom Inera

Ver 1.6

Inera

# Innehåll

inera



| Version | Datum | Författare | Kommentar |
|---|---|---|---|
| 1.0 | | Leif Carlsson | Fastställd version 2011 |
| 1.14 RC1 | | Fredrik Rosenberg | Revidering 2017 |
| 1.5 | | Fredrik Rosenberg | Revidering 2018 |
| 1.6 | 2019-02-01 | Fredrik Rosenberg | Förtydligande gällande utlämnande av information<br>Förtydligande lokal lagring<br>Förtydligande vidarebefordran e-post |

inera

# 1. Allmänt

Denna anvisning gäller hantering av Ineras information, oavsett i vilken form den finns. Anvisningen gäller dig som medarbetare samt dig som konsult verksam inom Inera. Anvisningen är kopplad till Ineras riktlinje för kvalitet och informationssäkerhet.

# 2. Som anställd eller konsult på Inera

Information är en viktig tillgång för Inera. För att skydda de värden som informationen representerar krävs en säkerhetsmedvetenhet hos alla.

Du som medarbetare har därför en viktig del av ansvaret för säkerheten i informationshanteringen. Det gäller oavsett om informationen behandlas muntligt, via en dator, en surfplatta eller en smartphone.

Samtidigt som informationen måste vara skyddad mot obehöriga måste den också vara tillgänglig när den behövs.

# 3. Riskmedvetenhet

Det är viktigt att ha ett riskmedvetet tankesätt när man som anställd hanterar information. När det gäller känslig information måste man alltid tänka på om det arbetssätt man har innebär risker att informationen kommer på avvägar eller blir otillgänglig.

Finns det arbetssätt och rutiner som innebär risker ska detta rapporteras till närmaste chef, så att det kan ändras. Ett riskabelt arbetssätt kan påverka patienter, anställda eller Inera som företag negativt.

Tänk alltså på att även om en specifik risk inte i sig kan leda till en fysisk skada eller att information kommer på villovägar så kan Ineras varumärke ändå skadas om negativ publicitet förekommer i media. Det kan räcka med att en tidning får vetskap om ett riskabelt arbetssätt där känslig information hanterats felaktigt för att en negativ bild av företaget ska börja spridas. Kunders förtroende för Inera kan också skadas.

# 4. Hantering av känslig information

Om uppgifter som Inera ansvarar för begärs ut av media eller någon annan ska en sekretessprövning alltid göras. Vid minsta osäkerhet om huruvida uppgifterna kan lämnas ut eller inte ska jurist kontaktas.

Inera

Stora delar av den information som Inera hanterar ägs av våra kunder. Det gäller exempelvis alla patientuppgifter som hanteras av våra tjänster. Beslut om huruvida dessa ska lämnas ut eller inte ska tas av den som äger informationen, dvs i de flesta fall kunden.

Även internt inom Inera ska försiktighet iakttas vid spridning av känslig information. Innan information delges kollegor eller arbetslag ska en bedömning göras om dessa har behov och behörighet att del av informationen. Även om alla har skrivit på ett sekretessavtal betyder inte det per automatik att alla behöver få tillgång till all information.

Det är inte tillåtet att ta med sig information som rör Ineras verksamhet vid anställningens upphörande. Även om du som anställd skapat informationen ägs den av Inera AB. Undantag från detta kan beviljas av närmaste chef som vid förfrågan gör en bedömning om informationen kan tas med eller inte.

# 5. Allmänt om IT-säkerhet

Tekniska skydd upplevs ofta som ett visst mått av hinder i arbetet. Men det är ett medvetet hinder för att Inera ska kunna skydda sin information. Målsättningen är att vald skyddsnivå ändå ska innebära att du som anställd kan utföra dina arbetsuppgifter effektivt.

## 5.1 Intrång

Olaga intrång, eller som vi vardagligt kallar intrång, sker för att någon vill ha något, men det är kanske inte du som anställd som är slutmålet utan endast en väg in till något. Kriminaliteten har flyttat från den fysiska världen till Internetvärlden pga. att det blir svårare och svårare för kriminella att stjäla fysiska pengar.

Pengar är idag elektroniska. Information är också pengar vilket innebär att kriminella försöker lura dig att lämna över person- eller kontoinformation via exempelvis e-post, sms, sociala medier eller telefonsamtal. Med hjälp av den information som den kriminelle får tillgång till kan denne komma åt dina eller företagets pengar (kreditkortsinformation, banköverföringar), utföra en ID stöld, stjäla information (företags- eller immaterialrättsliga tillgångar, IPR), utföra sabotage etc. Eller kanske det som är mest intressant för en hacker; att kunna ta över och använda din PC som ett verktyg för att komma åt konfidentiell eller integritetskänslig information, alternativt som en del i sabotage eller överbelastningsattacker.

Lämna således aldrig ifrån dig lösenord, kontouppgifter, bankkortsnummer etc.

# 6. Virus och skadlig kod

Virus och annan skadlig kod är idag ett stort problem. De vanligaste sätten en dator blir smittad på är via:

- bifogade filer eller länkar i e-post
- program hämtade från Internet
- USB-minnen

Du kan som användare minimera risken genom att vara mycket återhållsam med vilka filer eller länkar du öppnar i e-posten. Vid minsta misstanke om att din dator är smittad ska du kontakta it-supporten.

Anslut aldrig ett USB-minne till din dator som du fått eller hittat. Detta är ett vanligt sätt att sprida skadlig kod.

## 6.1 Din privata information

Det måste finnas en tydlig gräns mellan det privata och arbetet och det är därför inte tillåtet att blanda ihop företagets information med din privata information genom att exempelvis använda samma tjänster. Företagets information ska hållas inom företaget.

Inera har ingen kontroll över din privata it-miljö dvs. att din hemmamiljö har ett tillfredsställande perimeterskydd och att alla dina inkopplade datorer och annan utrustning är skyddade mot skadlig kod och intrång. Därför kan ett företag inte förlita sig på en anställds säkerhetsnivå i hemmet. Skadlig kod eller virus mycket väl kan sprida sig från ett dåligt underhållet hemmanätverk eller från privat utrustning över till Ineras nät, om en tydlig gräns inte finns.

Ytterligare en anledning är att Inera, om du skulle lagra information i en privat tjänst, inte kan komma åt den. Skulle du avsluta din anställning eller förolyckas kan informationen gå förlorad för Inera som företag.

Det är alltså inte tillåtet att använda delade ytor i exempelvis din privata OneDrive eller Dropbox, som du sedan använder för att kopiera eller flytta filer till företagets OneDrive.

De it-stöd som ska användas är de som erbjuds av Inera via it-avdelningen. Saknas något ska behov meddelas till din närmaste chef.

# 7. Behörighetstilldelning

Det är respektive chefs ansvar att besluta om tilldelning av behörigheter.

Som anställd eller konsult inom Inera ska du ha tillgång till den information som krävs för att du effektivt ska kunna genomföra dina arbetsuppgifter. Det betyder att behörighetstilldelningen ska begränsas så att du inte har en teknisk behörighet till sådant som du egentligen inte behöver. Meddela din chef både om du anser att du saknar vissa behörigheter, men även om du har kvar behörigheter som borde tagits bort.

Vid anställningens upphörande eller vid byte av tjänst ska behörighetstilldelningen tas bort eller revideras.

# 8. Lagring och bärbara media

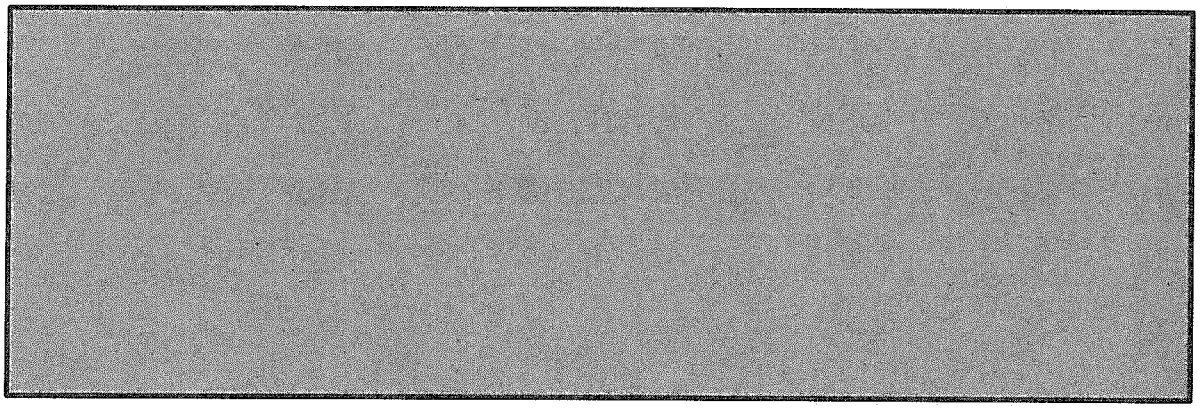
Lagring av viktig eller känslig information ska alltid ske på en lagringsplats som är säker och där säkerhetskopiering (backup) sker. Lagring av patientuppgifter ska enbart ske i den tjänst som tillhandahåller patientuppgifterna och inte på Ineras filytor. Finns trots allt behov av detta ska kontakt tas med IT-avdelningen för att hitta en lösning.

All lagring ska ske i de IT-system som är anmodade av Inera. Detta för att Inera ska ha kontroll över var information finns, men även för att minimera licenskostnader.

## 8.1 Lagring eller hantering inom EU/EES

Uppgifter om patienter eller andra känsliga personuppgifter får aldrig lagras eller hanteras utanför EU/EES. Det krävs också en stark autentisering för åtkomst till lagring eller hantering där åtkomsten sker över internet, som räknas som ett osäkert, öppet nätverk. Speciellt viktigt är detta när det gäller molntjänster, där det ibland kan vara svårt att veta var lagringen sker.

## 8.2 Lagringsytor



inera

## 8.3 Lokal lagring

På en dators lokala hårddisk ( C:\ ) ska normalt ingen lagring av personliga filer ske. En del program kan cachelagra information på hårddisken, men som medarbetare ska du inte aktivt lagra något i mappar du skapat på den lokala hårddisken. Detta gäller även datorns Skrivbord.

Förutom stöldrisken finns det lokalt på datorn ingen säkerhetskopiering, vilket innebär att informationen är borta om datorn går sönder eller blir stulen. Måste känsliga uppgifter i undantagsfall lagras lokalt, tex för test, ska dessa krypteras så att de alltid är krypterade när de inte används. IT-avdelningen kan bistå med teknisk lösning för detta.

## 8.4 Flyttbara lagringsmedia

På flyttbara lagringsmedia som USB-minnen och portabla hårddiskar får ingen lagring ske av känsliga uppgifter. Även en mobiltelefons interna minne räknas som flyttbart lagringsmedia.

Dessa lagringsmedia ska betraktas som mycket osäkra eftersom det är lätt att tappa bort ett USB-minne. Istället för att ta med sig filer på ett USB-minne kan funktionaliteten att dela filer användas.

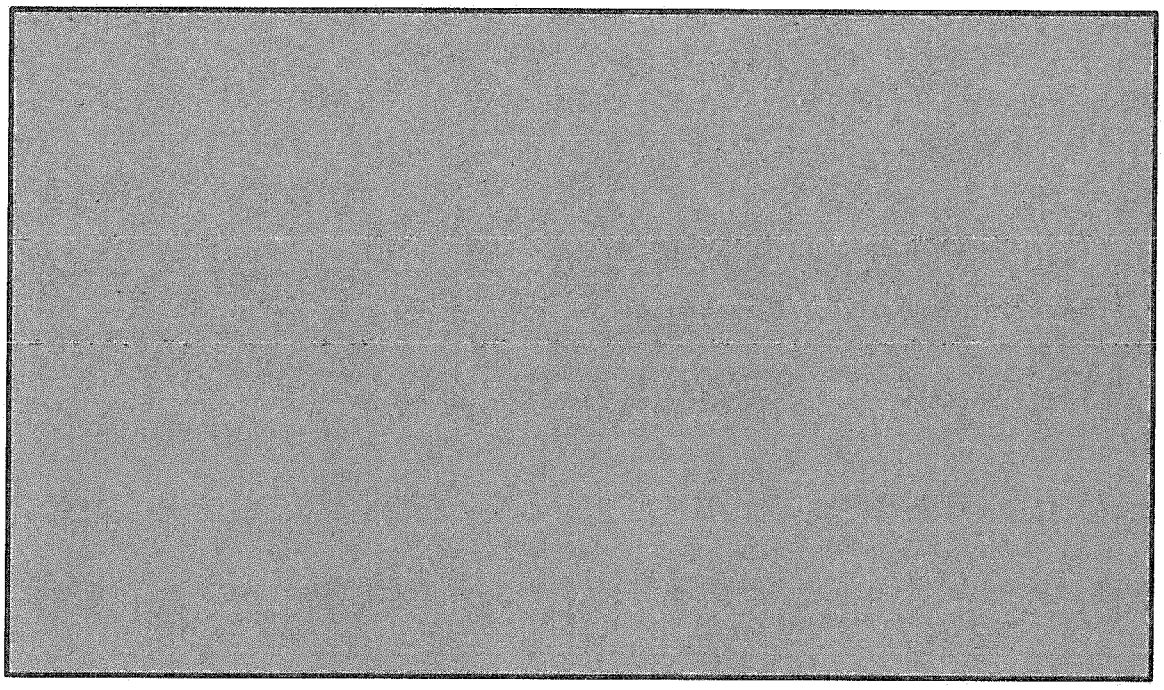
Flyttbara lagringsmedia är som tidigare beskrivits ett vanligt sätt att sprida skadlig kod. Undvik därför i det längsta att ansluta lagringsmedia, som ett usb-minne du fått på en konferens, till din dator. Och framför allt inte om du hittat ett usb-minne utanför företaget, vilket är ett vanligt sätt för en angripare att försöka föra in skadlig kod.

Som generell regel ska lagring av uppgifter på flyttbara lagringsmedia undvikas i det längsta.

# 9. Anslutning av enheter till trådlösa nätverk

Ineras har ett antal olika trådlösa nätverk som är avsedda för olika typer av enheter. Anledningen till det är att en mobiltelefon exempelvis har lägre säkerhet än en bärbar dator, vilket gör att de inte ska vara inkopplade i samma trådlösa nätverk.

## 9.1 Ineras olika trådlösa nätverk



# 10. Internetanvändning

Internet är ett arbetsverktyg och får för privat bruk endast användas i sådan omfattning att det inte inskränker på arbetet eller medför merkostnader för Inera. Sunt förnuft räcker långt.

## 10.1 Oetisk användning av internet

Internetanvändning ska ske med hänsyn till etik och moral. Det är inte tillåtet att för privata syften besöka sidor med oetiskt innehåll. Det kan exempelvis vara sidor som stödjer terrorism, innehåller grovt våld eller pornografi. Detsamma gäller webbplatser med extrempolitiska åsikter. Det är åsikter som speglar en missaktning av folkgrupp med anspelning på ras, kön, hudfärg, nationalitet, etniskt ursprung eller trosbekännelse. Även sidor för fildelning, sidor som bryter mot upphovsrättslagen eller sidor som strider mot svensk lagstiftning är att betrakta som oetiska. Vilka webbplatser som besöks loggas.

## 10.2 Nedladdning av material från internet

Nedladdning av exempelvis bilder, musik, filer eller installation och uppdatering av program från internet innebär en risk för Inera. Virus eller annan skadlig kod kan spridas och leda till driftstörningar eller att information sprids. Om nedladdning av material från internet behövs får

detta endast ske av sådant material som är relevant för arbetet. Installation och uppdatering av programvara via internet ska bara ske efter samråd med IT-avdelningen.

# 11. E-post

## 11.1 Känsliga personuppgifter

Känsliga personuppgifter, till exempel uppgifter om hälsa, får endast skickas krypterade. Därför lämpar sig e-postsystemet inte för hantering av denna typ av uppgifter, E-postsystemet ska som huvudregel inte innehålla några känsliga personuppgifter. Om sådana mottagits via mail ska de snarast tas bort, både från Inkorgs- och Borttagna objektsmappen.

## 11.2 Privata mailkonton

Det är på datorer inte tillåtet att installera privata mailkonton i Ineras e-postprogram. Detta pga. att det är lätt att blanda samman e-post som har med arbetet att göra och den privata. Det ökar också risken att få in skadlig kod i Ineras nätverk. Om andra e-postkonton måste kommas åt ska det primärt ske via webklienter. Gällande mobila enheter är det tillåtet, om den används även privat, att installera privata mailkonton. Det ska dock undvikas i den mån det går.

## 11.3 Delegering av brevlåda

Det är tillåtet att delegera sin brevlåda åt en specifikt utsedd person. Detta kan gälla exempelvis till en sekreterare eller då en medarbetare är sjuk under längre tid och frånvaromeddelanden inte antas kunna ersätta delegeringen. Det är däremot inte tillåtet att automatiskt vidarebefordra sin e-post till en annans brevlåda. Det är inte heller tillåtet att automatiskt vidarebefordra sin e-post till en brevlåda som inte är Ineras, till exempel din privata eller annat e-postkonto som inte är Ineras. Anledningen är att känslig information av misstag inte ska lagras utanför Inera.

## 11.4 Privat användning

Privat användning av Ineras e-postsystem är tillåten i begränsad omfattning och får inte inverka på ditt arbete. Registrering av din ineraadress i t ex diskussionsgrupper eller vid prenumerationer av information, får endast ske om det är relevant för arbetet. Detsamma gäller sociala medier.

## 11.5 Bilagor och länkar

Stor försiktighet ska iakttas då bifogade filer eller länkar inkommit via e-post. Detta är en vanlig orsak till att skadlig kod sprids vilket sedan kan resultera i intrång, virusangrepp eller s.k. ransomwareangrepp (som krypterar och gör din information otillgänglig). Vid minsta misstanke, kontakta IT-avdelningen innan bilagan öppnas eller länken används. För att kontrollera om en länk verkligen går dit den verkar gå till, kan muspekaren hållas över länken. Dock utan att klicka. Den verkliga adressen visas då och ger i många fall en ledtråd om huruvida det är en länk som utan risk kan användas eller inte.

Det är inte heller tillåtet att:

- skicka eller spara stötande information innehållande våld, pornografi, diskriminerande ord och bilder
- skicka eller vidarebefordra skräppost (s k spam) och kedjebrev oavsett syfte
- skicka exekverbara programfiler (t ex exe)
- öppna exekverbara program, inkl komprimerade programfiler

# 12. Loggning och spårbarhet

Loggning av dina aktiviteter som användare görs. Det primära syftet är att kunna följa upp incidenter som exempelvis virusutbrott eller dataintrång. Loggningen används inte för att bevaka personal och ligger inte heller till grund för att mäta din arbetsprestation. Som användare måste man dock känna till man lämnar spår efter sig. Vid utredningar kan loggen användas, men beslut av detta tas av närmaste chef tillsammans med HR-chef

# 13. Användarnamn, lösenord och SITHS-kort

Användaridentiteter, lösenord och SITHS-kort är personliga och får inte lånas ut. Vid misstanke om att dit lösenord kommit i fel händer ska det bytas omgående. Om ditt SITHS-kortet tappats bort måste det rapporteras så att kortet kan spärras.

För att förhindra obehörig åtkomst till IT-system ska datorn låsas när den inte används. Den får inte lämnas öppen och inloggad.

Alla handdatorer och mobiltelefoner ska förses med en PIN-kod eller ett kvalificerat lösenord.

## 13.1 Lösenordshantering

Användarnamn och lösenord krävs för information som är skyddsvärd vilket innebär att du måste logga in och identifiera dig till Ineras företagsnät. Det finns även krav på att du måste byta lösenord med jämna mellanrum pga. att lösenord kan röjas men också, som är den viktigaste anledningen, att det är vanligt att människor återanvänder både kontoinfo, lösenord

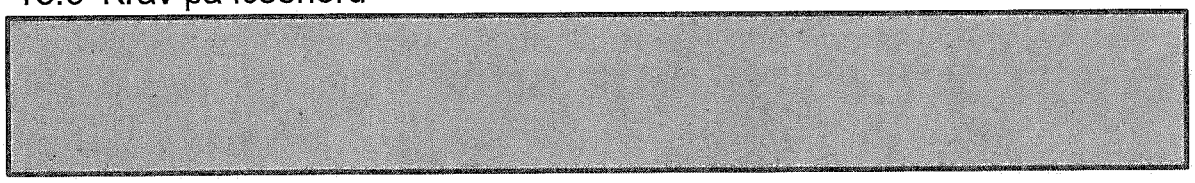
och även PIN-koder till andra konton. Om en sajt blir hackad och lösenord kommer på drift så kan dessa med stor sannolikhet användas på andra ställen där du har ett konto.

Det är av den anledningen inte tillåtet att använda samma lösenord privat som du använder i Ineras tjänster och du ska bör inte återanvända lösenord för inloggning till olika tjänster. Anledningen till att privata lösenord inte ska användas i arbetet är att IT-säkerhetsnivån kan vara mycket lägre i en tillämpning som är avsedd för privat bruk. Exempel på detta kan vara idrottsföreningens hemsida eller konton till olika webbutiker. Ett flertal privata tillämpningar har historiskt blivit hackade och ett stort antal lösenord har sedan exponerats på internet. Det är då viktigt att ett sådant hackat lösenord inte kan användas i Ineras tjänster.

## 13.2 Lösenordstips

Använd inte lösenord baserat på familjemedlemmar, ett husdjurs namn eller PIN-koder eller annat man kan koppla till dig själv eller familjemedlemmar, det är det första en hackare provar med. Vi vill att Du ska skapa och använda säkra lösenord men som ändå är relativt enkelt att komma ihåg.

## 13.3 Krav på lösenord



## 13.4 Förslag på hur lösenord kan skapas

Ett förslag är att Du kan skapa en mening av något du ser eller har runt omkring dig. Det ska vara lätt att komma ihåg och det kan också vara t.ex. en mening ur en bok eller några ord från en dikt. Det är relativt enkelt och komma ihåg ett lösenord som är:

*Jaghar,enkulpenna2*

som 18 tecken långt än att skriva:

*hkGk+gTt#d*

som är 10 tecken långt.

Skriv din lösenordsmening utan mellanslag eller blandat med någon siffra och lägg gärna in ett skiljetecken.

Ett annat förslag är att ta en lång mening, som är lätt att komma ihåg, där du plockar ut inledande bokstaven i varje ord t.ex.:

”I min värld ska alla på Inera ha ett bra lösenord 2018” ger lösenordet

*ImvsaplhebI2018*

som då blir 15 tecken långt vilket är ett mycket bra lösenord.

# 14. Distansarbete

Anslutning från annan plats till Inera:s nätverk ska ske genom en kommunikationslösning som är godkänd av Inera.

Utomstående får inte hantera Ineras datorer. Det betyder bland annat att familjemedlemmar inte får använda företagets dator, surfpaddor eller mobiltelefoner för att surfa på Internet eller att spela spel på. Detta kan vara en källa till att Inera får in skadlig kod som ger grunden till intrång eller att ransomware kommer in i Ineras IT-miljö

Tänk även på vad andra kan se och höra när du arbetar i öppna miljöer såsom på tåget eller på en konferens. Använd skärmskydd om du arbetar på distans med känsliga uppgifter.

# 15. Sammanfattande korta punkter

Som medarbetare på Inera ska du:

- vara försiktig och vaksam på bilagor och länkar i mail.
- undvika att ansluta USB minnen, speciellt okända
- följa tidigare presenterad lösenordsrekommendation
- tydligt skilja privat användning från användning kopplad till arbetet
- använda olika lösenord privat och på jobbet.

Tänk på att:

- människan är den svagaste länken vid ett intrångsförsök
- ha ett kritiskt och säkerhetsmedvetet arbetssätt
- inte lita på allt och alla på internet