TP2B THE PLACE TO BE

ATEA

RISKHANTERING FÖR INFORMATIONSSÄKERHET: POLICYER FÖR MEDARBETARNA

Version 1.0 - publicerad i augusti 2019

VÅR VD HAR ORDET

Ateas ambition är att ”bygga framtiden med it”.

Vi menar att it i kombination med kunskap och kreativitet kan bidra till samhällets produktivitet och levnadsstandard. Vi hjälper företag och offentliga organisationer att bygga upp digitala lösningar som gör att de kan åstadkomma mer, bli effektivare och förbruka mindre resurser.

Samtidigt är vi medvetna om de inbyggda riskerna med tekniker som lagrar och behandlar mer och mer information. Eftersom organisationer hanterar mer data och automatiserar processer via sina it-system och nätverk ökar hoten om datastöld, identitetsbedrägeri och driftstörningar genom cyberattacker. Ett dataintrång kan också ge åtkomst till en persons information utan dennes medgivande och informationen kan missbrukas för att skada den personen och kränka dennes rätt till integritet.

Atea är ledande leverantör av it i Norden och Baltikum och har ett särskilt ansvar för att säkerställa att vår verksamhet uppfyller stränga krav på informationssäkerhet. Atea designar, implementerar och sköter lösningar för it-infrastruktur åt de största och vitalaste organisationerna i våra regioner. Vi säljer mest till nationella och lokala myndigheter, inklusive mycket känsliga kunder som militär och polis. Vi förser också de största företagen i våra regioner med viktiga it-lösningar.

Det här dokumentet är en vägledning för hur vi ska hantera informationssäkerhetsrisker på Atea. Det ger en översikt över de viktigaste säkerhetsriskerna, dataskyddspolicyer och styrningsrutiner som påverkar alla i företaget. De medarbetare som har särskilt ansvar för it-verksamhet och systemadministration måste genomgå separata och mer omfattande tester när det gäller informationssäkerhets- och dataskyddspolicyer, i enlighet med vad som krävs i deras funktion.

Dokumentet är uppdelat i fyra avsnitt, och de viktigaste punkterna sammanfattas i slutet av varje avsnitt. Eftersom det här är ett komplicerat ämne som är oerhört viktigt för vår verksamhet är de fyra avsnitten väldigt detaljerade. Medarbetarna bör i synnerhet komma ihåg ”de viktigaste punkterna” i slutet av varje avsnitt och kan konsultera resten av dokumentet vid behov.

Alla medarbetare måste känna till innehållet i det här dokumentet. För att säkerställa att medarbetarna förstår innehållet i det här dokumentet har vi lagt till tio frågor om informationssäkerhet i testet om uppförandekoden, ett test som är obligatoriskt för alla medarbetare på Atea. Det finns en onlinekurs tillgänglig för medarbetarna så att de kan studera Ateas informationssäkerhetspolicy och förbereda sig på testet om uppförandekoden.

Atea är en stor organisation som är spridd över sju länder och nästan 90 kontor. Vi har utsett en Chief Information Security Officer för koncernen och en för varje land, som ska hjälpa till med implementeringen av informationssäkerhetspolicyn i hela Ateas organisation.

Steinar Sønsteby
CEO

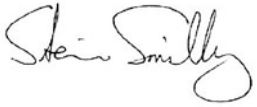
Om du har frågor som rör informationssäkerheten på Atea ber vi att du hanterar dina problem enligt följande:

- Om du oroar dig för att din dator kanske har infekterats med skadlig programvara eller har allmänna frågor om it-säkerhet, kontaktar du Ateas servicedesk
- Om du vill rapportera ett misstänkt e-postmeddelande, bedrägeriförsök eller annan händelse som kan utgöra en informationssäkerhetsrisk för Atea, kontaktar du Ateas servicedesk
- Om du vill rapportera ett misstänkt intrång (obehörigt yppande) av personuppgifter eller affärsdata från informationssystem och dokument, kontaktar du landets Chief Information Security Officer. Alternativt kan du skicka ett e-postmeddelande direkt till infosec@atea.com.

Om du vill tala direkt med koncernens Chief Information Security Officer (CISO) eller med landets eller den delade service-enhetens CISO finns deras namn på på Ateas compliance-sida: atea.com/trust. Alla e-postmeddelanden som skickas till infosec@atea.com vidarebefordras direkt till koncernens Chief Information Security Officer.

Vi tar gärna emot dina frågor och din återkoppling, och vi lovar att det inte blir några repressalier i samband med problem som rapporteras. Men om du hellre vill rapportera ett problem anonymt, går det också bra att rapportera till Whistleblower Hotline. En länk till Whistleblower Hotline finns också på Ateas compliancesida: atea.com/trust. Problem som rapporteras till Whistleblower Hotline skickas till en oberoende advokatbyrå som sammanfattar och rapporterar ditt problem till lämplig nivå i Ateas organisation.

Det är mycket viktigt att vi upprätthåller strikta normer kring informationssäkerhet för vår verksamhet och för att vi ska kunna arbeta med kunder och partners kring de viktigaste it-utmaning-arna i vår region. Tack för att du följer Ateas policyer om it-säkerhet och för att du gör vårt företag till ”The Place to Be”.



De viktigaste punkterna:

Det är mycket viktigt för Atea att alla medarbetare upprätt-håller strikta normer för informationssäkerhet.

Vi har utsett en Chief Information Security Officer för koncernen och en för varje land, som ska hjälpa till med implementeringen av informationssäkerhetspolicyn i hela Atea. Namnen på Chief Information Security Officers finns på Ateas compliancesida: atea.com/trust.

Om du har frågor som rör informationssäkerheten på Atea ber vi att du hanterar dem enligt följande:

- Om du oroar dig för att din dator kanske har infekterats med skadlig programvara eller har allmänna frågor om it-säkerhet, kontaktar du Ateas servicedesk
- Om du vill rapportera ett misstänkt e-postmeddelande, bedrägeriförsök eller annan händelse som kan utgöra en informationssäkerhetsrisk för Atea, kontaktar du Ateas servicedesk
- Om du vill rapportera ett misstänkt intrång (obehörigt yppande) av personuppgifter eller affärsdata från informationssystem och dokument, kontaktar du landets Chief Information Security Officer.
- Alternativt skickar du ett e-postmeddelande till infosec@atea.com, som vidarebefordras direkt till koncernens Chief Information Security Officer.

Innehåll

1. INFORMATIONSSÄKERHET – ÖVERSIKT OCH RISKHANTERING

Information är avgörande för att organisationer ska kunna fungera. Ett system för hantering av informationssäkerhet (ISMS) är den uppsättning policyer, rutiner, verktyg och aktiviteter som en organisation använder för att skydda sin information från obehörig åtkomst och missbruk.

För att kunna skapa ett ISMS krävs det att organisationen identifierar vilken information man har. Det gäller all information som organisationen hanterar, oavsett form: digital, på papper eller verbal. När det gäller Atea kan den här informationen vara avsedd för internt bruk, eller vara extern information som företaget hanterar och bearbetar som en tjänst till våra kunder.

Syftet med ett system för hantering av informationssäkerhet är att skydda och bevara informationens konfidentialitet, integritet och tillgänglighet.

- **Konfidentialitet** innebär att informationen endast är tillgänglig för behöriga personer.
- **Integritet** innebär att informationen underhålls så att den är komplett och korrekt.
- **Tillgänglighet** innebär att behöriga användare har åtkomst till och kan använda informationen när de behöver.

För att uppnå detta bör organisationen göra en riskbedömning för att avgöra på vilka sätt informationen är utsatt för potentiella hot mot informationssäkerheten. Därefter kan man utforma ett system för hantering av informationssäkerheten som effektivt kan hantera och kontrollera dessa risker, utan onödiga kostnader eller förlorad produktivitet.

Riskbedömning på Atea

Följande informationssäkerhetsrisker har högsta prioritet för Ateas verksamhet:

1. **Fysisk förlust:**
   Information lagras på fysiska enheter, som kan förloras, stjälas eller skadas. Det behövs åtkomstkontroll, kryptering och databackup för att begränsa de potentiella riskerna för fysiska tillgångar, t.ex. datorer, mobiltelefoner, servrar och lagringsmedia. Datacenter är särskilt känsliga och måste skyddas från miljöfaror, inklusive temperatur och brand.

2. **Identitetsbedrägeri:**
   Atea är ständigt utsatt för bedrägeriförsök av angripare som använder falsk identitet eller bedrägliga metoder för att utnyttja en medarbetares förtroende. Syftet med bedrägeriförsöket är att stjäla från Atea eller att få obehörig åtkomst till Ateas system och nätverk.

   En typ av identitetsbedrägeri mot Atea är användning av falsk eller stulen kundkontoinformation för att beställa it-utrustning, i synnerhet genom Atea Eshop. Utöver åtkomstkontroller på Eshop har Atea affärsrutiner för att kontrollera nya kundkonton och identifiera ovanlig aktivitet på befintliga konton, allt för att minska risken för bedrägliga kundtransaktioner.

   Ytterligare en vanligt förekommande typ av identitetsbedrägeri (”phishing”) är när en angripare kontaktar en av våra medarbetare direkt, ofta via e-postkommunikation. E-postmeddelandet ser ut att komma från en betrodd källa, vanligen genom användning av falsk identitet, som t.ex. en annan medarbetare på Atea, en affärskontakt, eller en leverantör som ett teknikföretag eller en bank. E-postmeddelandet försöker lura medarbetaren att agera, till exempel att överföra pengar, ange inloggnings-/lösenordsdata eller annan känslig information, eller att klicka på en länk eller bilaga som laddar hem skadlig programvara (”malware”) till medarbetarens dator eller mobil.

   Meddelandet, bilagan eller länken verkar oskyldig – det kan till exempel se ut som e-post från en kollega, en offert/faktura från en leverantör eller som ett meddelande från ett molnkonto som OneDrive. Därför måste medarbetarna vara mycket vaksamma på potentiella bedrägerier i alla e-postmeddelanden eller annan kommunikation, även om den verkar komma från en betrodd källa.

   Medarbetarna bör aldrig öppna länkar eller bilagor på sina enheter om de tvivlar på ett e-postmeddelandes eller en kommunikations

legitimitet. Om en medarbetare är osäker på ett e-postmeddelandes legitimitet, eller om denne av misstag har svarat på ett möjligt bedrägeriförsök genom att öppna en misstänkt länk eller bilaga, bör de omedelbart rapportera till Ateas servicedesk.

Visserligen är e-post den vanligaste metoden för ”phishing” relaterat till arbetet, men medarbetarna bör också vara uppmärksamma på andra former av bedräglig kommunikation, inklusive telefonförfrågningar eller inbjudningar i sociala medier.

3. Stöld av affärshemligheter:

Om obehöriga personer får åtkomst till Ateas informationssystem kan de försöka stjäla konfidentiell information som är känslig för Ateas verksamhet. Det kan vara hemlig affärsinformation som kund- eller leverantörsinformation, kontrakt eller kommersiella villkor. Det kan också röra sig om immateriella tillgångar, som affärskoncept, design på produkter eller tjänster och internt utvecklade programvaror, metodiker och verktyg.

Medarbetare med tillgång till viktiga system kan också försöka stjäla affärshemligheter från Atea, särskilt om de planerar att lämna företaget. För att minska riskerna får medarbetare endast beviljas åtkomst till information på behovsbasis. Man bör kontinuerligt kontrollera åtkomsten till systemet för att se till att principen om ”behov” upprätthålls, och att en användares åtkomsträttigheter avbryts när de inte längre behövs.

Utöver åtkomstkontroll använder Atea Security Information and Event Management (SIEM)-verktyg för att analysera logginformation och analysera vad som har skett i systemen.

4. Störning av affärsverksamheten:

Ateas affärsverksamhet är beroende av dess it-system. Vid överträdelser av åtkomstkontroller eller missbruk av system kan privat information om medarbetare eller affärskontakter potentiellt läckas. Information som är nödvändig för att Atea ska kunna sköta sin verksamhet kan manipuleras eller raderas. Slutligen kan affärstransaktioner matas in eller godkännas av obehöriga personer, trots Ateas ledningskontroller. Alla dessa händelser är störande för Ateas affärsverksamhet.

Företaget riskerar också störningar i verksamheten genom en sofistikerad hackningsattack som stänger ner viktiga it-system eller nätverk. System kan infekteras med skadlig programvara som hindrar användarna från att få åtkomst till viktiga funktioner eller från att läsa datafiler om inte en lösensumma betalas ut (”ransomware”). Nätverk eller servrar kan bombarderas med trafik eller förfrågningar så att de inte längre kan hantera legitima transaktioner (”denial-of-service”-attack). Sådana attacker kan vända sig mot antingen Atea eller de kunder Atea hanterar från sitt datacenter.

5. Skador på kontrakt:

Atea har sekretessavtal med många kunder, leverantörer och affärspartners. Företaget har också servicenivåavtal och personuppgiftsbiträdesavtal med kunder som använder Ateas it-tjänster och support.

En it-säkerhetsincident på Atea kan leda till att företaget bryter mot sina sekretess-, servicenivå- och personuppgiftsbiträdesavtal med kunder och andra affärspartners. Detta kan leda till rättsprocesser mot Atea och skadestånd på grund av kontraktsbrott. Utöver direkta skador, kan en it-säkerhetsincident orsaka varaktig skada på Ateas affärsrelationer med kunder och partners.

Atea kan drabbas av rättsliga krav även i situationer där företaget inte har ett specifikt kontrakt, om företag eller individer har fått sin information stulen eller missbrukad på grund av att Atea inte har uppvisat tillräcklig försiktighet vid hanteringen av informationen.

6. Straffpåföljd:

Eftersom Atea är noterat på Oslobörsen, måste företaget följa strikta juridiska krav vid hantering av information som inte är känd på marknaden och som kan påverka dess aktiepris (”kurspåverkande information”). Detta kan vara information om stora nya kontrakt eller finansiella resultat som ännu inte rapporterats offentligt.

Atea måste hantera kurspåverkande information konfidentiellt för att säkerställa att informationen inte sprids utanför ett begränsat antal registrerade insiders på ”behovsbasis”. Medarbetare som innehar kurspåverkande information måste registreras av företaget och är måste uppfylla särskilda sekretesskrav och restriktioner mot handel med Ateas aktier. Brott mot dessa lagkrav kan leda till åtal och straffpåföljd enligt den norska lagen om värdepappershandel.

Atea riskerar också möjlig straffpåföljd i händelse av dataintrång som rör personuppgifter, i enlighet med EU:s dataskyddsförordning (GDPR). Eftersom kraven i GDPR är ganska uttömmande, tas detta ämne upp separat i nästa avsnitt av det här dokumentet om datasekretess.

De viktigaste punkterna:

Alla medarbetare måste vara mycket försiktiga när de hanterar information och it-system för att förebygga brott mot säkerheten.

It-utrustning kan förloras, stjälas eller skadas. Det behövs åtkomstkontroll, kryptering och databackup för att begränsa de potentiella riskerna för informationssäkerheten.

Atea är ständigt utsatt för bedrägeriförsök av angripare som använder falsk identitet eller bedrägliga metoder för att utnyttja en medarbetares förtroende. Tänk på att alla e-postmeddelanden och kommunikationer du får kan vara ett bedrägeriförsök, även om det verkar komma från en legitim källa (till exempel e-post från en chef, en kund, en teknikleverantör eller ett konto på sociala medier).

Var försiktig med ovanliga kommunikationer eller aktiviteter du får ögonen på. Om du misstänker att du är utsatt för bedrägeri via ett e-postmeddelande eller annat meddelande, kontakta Ateas servicedesk och berätta om detta. Svara inte på misstänkt kommunikation – till exempel genom att öppna e-postbilagor och externa länkar, eller genom att behandla order och betalningar.

För att minska riskerna för informationsstöld eller missbruk får medarbetarna endast beviljas åtkomst till information på behovsbasis. Man bör kontinuerligt kontrollera åtkomsten till systemet för att se till att användares åtkomsträttigheter avbryts när de inte längre behövs.

En informationssäkerhetsincident kan leda till allvarlig skada för Atea genom störning av företagets affärsverksamhet, brott mot dess kontraktsåtaganden gentemot kunder och affärspartners, straffpåföljder och skada på Ateas anseende och affärsrelationer.

2. DATAINTEGRITET – ÖVERSIKT OCH RISKHANTERING

Dataintegritet omfattar en persons kontroll över sin egen information – särskilt möjligheten att avgöra när och hur den egna informationen samlas in, delas och används. Personuppgifter definieras som information i vilken som helst form, som kan hänföras till en specifik och identifierbar person.

Dataintegritet är beroende av informationssäkerhet, dvs. hur information skyddas mot obehörig åtkomst och missbruk. Men dataintegriteten sträcker sig också bortom informationssäkerheten och till skyddet av individens rätt till sin egen information. Specifikt – hur ger en organisation varje person möjlighet att styra användningen av de egna personuppgifterna när organisationen samlar in och behandlar information om den personen.

Vi anser att dataintegritet är en grundläggande mänsklig rättighet och vi hanterar personuppgifter på ett sätt som till fullo respekterar den rättigheten. Atea måste följa strikta lagkrav vid hantering av personuppgifter i enlighet med EU:s dataskyddsförordning (GDPR).

De krav i GDPR som gäller Atea kan sammanfattas som följer:

Krav vid insamling av personuppgifter
Atea kan endast behandla (dvs. samla in, lagra och använda) personuppgifter när företaget har ett legitimt affärsintresse av detta, och när den aktuella personen har givit sitt samtycke eller meddelats om att personuppgifterna behandlas. Innehållet i detta meddelande eller samtycke beskrivs i nästa avsnitt i det här dokumentet.

Personers rätt att kontrollera sina personuppgifter
Atea måste efterleva en individs begäran att styra användningen av personuppgifterna, i enlighet med dennes rätt till dataintegritet enligt GDPR. Enligt GDPR har individer rätt till åtkomst till de egna personuppgifterna som innehas av Atea. Individer har också rätt att korrigera fel i sina personuppgifter, att få sina personuppgifter raderade, eller begränsa behandlingen och användningen av sina personuppgifter.

Dokumentation av behandling
Atea måste dokumentera i vilken utsträckning man behandlar personuppgifter. I detta bör ingå en beskrivning av vilken typ av personuppgifter som behandlas och för vilka kategorier av personer. Det bör också omfatta en beskrivning av vilka tekniska och organisatoriska åtgärder som har vidtagits för att förebygga och minimera effekterna av ett datintrång i Ateas databehandlingsaktiviteter (”inbyggt dataskydd”).

Personuppgiftsbiträdesavtal med kunder/leverantörer
När Atea tillhandahåller databehandlingstjänster till kunder (t.ex. när företaget hanterar datainfrastruktur och applikationer för kunders räkning, antingen hos kunden eller från sina egna datacenter), måste företaget också ha ett giltigt personuppgiftsbiträdesavtal med kunden som uppfyller kraven i GDPR.

På samma sätt måste företaget, när det behandlar personuppgifter via en underleverantör eller leverantör (dvs. när man använder programapplikationer som körs i en leverantörs datacenter, t.ex. molntjänster), ha ett giltigt personuppgiftsbiträdesavtal som uppfyller GDPR med det företag som hanterar applikationen och som behandlar personuppgifter för Ateas räkning. Information som behandlas utanför EU/EEA måste finnas i ett land eller under ett ramverk där myndigheterna har godkänts som innehavare av tillräckliga säkerhetsåtgärder för dataskydd.

Krav i händelse av en personuppgiftsincident
I händelse av en personuppgiftsincident som kan leda till risk för skada för en individ måste Atea meddela tillsynsmyndigheten i det land där incidenten uppträdde inom 72 timmar från det att man blev medveten om incidenten. Meddelandet måste beskriva indicentens natur, en sammanfattning av de berörda datasubjekten och

uppgifterna, de sannolika konsekvenserna av incidenten och vilka åtgärder som vidtagits.

Individer vars personuppgifter är inblandade i incidenten måste också meddelas direkt om det finns stor risk för skada för den personen. Ett offentligt meddelande kan räcka om det inte är möjligt att meddela individuellt.

Enligt GDPR kan landets tillsynsmyndighet utfärda höga viten för ett företag i händelse av brott mot GDPR. Vitets belopp bygger på incidentens natur, utsträckningen av skada på rätten till dataintegritet och vilka åtgärder företaget har vidtagit för att förebygga och hantera intrånget. Det maximala vitet i händelse av brott mot GDPR är 4 % av de årliga globala intäkterna eller 20 miljoner euro, vilket som är högst.

Utifrån kraven i GDPR, är det ytterst viktigt att Atea dokumenterar alla rutiner som rör personuppgifter, och identifierar alla interna applikationer och kontrakt som rör behandlingen av personuppgifter. Denna information måste vara tillgänglig för Chief Information Security Officer i varje land, för att bekräfta att lämpliga åtgärder har vidtagits till skydd för datasekretessen. Alla länders och koncernens Chief Information Security Officer återfinns på Ateas compliancesida.

De viktigaste punkterna:

Dataintegritet omfattar en persons kontroll över sin egen information – särskilt möjligheten att avgöra när och hur den egna information samlas in, delas och används. Personuppgifter definieras som information i vilken som helst form, som kan hänföras till en specifik och identifierbar person.

Atea måste följa strikta lagkrav vid hantering av personuppgifter i enlighet med EU:s dataskyddsförordning (GDPR).

Enligt GDPR:
Atea kan endast behandla (dvs. samla in, lagra och använda) personuppgifter när företaget har ett legitimt affärsintresse av detta, och när den aktuella personen har givit sitt samtycke eller meddelats om att personuppgifterna behandlas.

Atea måste efterleva en individs begäran att styra användningen av personuppgifterna, i enlighet med dennes rätt till dataintegritet enligt GDPR.

Atea måste dokumentera i vilken utsträckning man behandlar personuppgifter, inklusive vilka åtgärder som har vidtagits för att förhindra och minimera effekterna av ett dataintrång. Det innebär att Atea måste dokumentera alla rutiner som rör personuppgifter, och identifiera alla interna applikationer och kontrakt som rör behandlingen av personuppgifter.

Företaget måste ha ett giltigt personuppgiftsbiträdesavtal med alla kunder för vilka man utför databehandlingstjänster (t.ex. Hantering av datainfrastruktur och applikationer, antingen hos kunden eller från sina egna datacenter).

Företaget måste också ha ett giltigt personuppgiftsbiträdesavtal med underleverantörer eller leverantörer som behandlar personuppgifter för Ateas räkning (t.ex. tillhandahåller programapplikationer och datalagring i en leverantörs datacenter, t.ex. molntjänster).

I händelse av en personuppgiftsincident som kan leda till risk för skada för en individ måste Atea meddela tillsynsmyndigheten i det land där incidenten uppträdde inom 72 timmar från det att man blev medveten om incidenten.

3. DATASKYDDSPOLICYER PÅ ATEA

Medarbetarna måste alltid följa företagets dataskyddspolicyer när de samlar in, hanterar och distribuerar data. Alla chefer är ansvariga för att säkerställa att affärsprocesser inom deras ansvarsområde följer Ateas dataskyddspolicyer, och att deras medarbetare arbetar enligt dessa affärsprocesser.

Alla regioner utser en dataskyddsadministratör som ansvarar för en viss affärsfunktion i landet (eller delade serviceenheten). Dataskyddsadministratörens roll är att kontrollera att alla affärsprocesser i deras affärsfunktion följer Ateas dataskyddspolicyer. Dessa funktioner omfattar: Försäljning/marknadsföring, HR, Ekonomi, Konsulttjänster, AMS, Logistik och It.

Dataskyddsadministratören för varje affärsfunktion rapporterar till landets (eller delade serviceenhetens) Chief Information Security Officer. Varje lands Chief Information Security Officer har övergripande ansvar för implementeringen av dataskyddspolicyerna i sitt land, och rapporterar till koncernens Chief Information Security Officer.

Kontaktinformation för alla viktiga medlemmar i informationssäkerhetsorganisationen i ditt land finns på compliancesidan: atea.com/trust. En sammanfattning av informationssäkerhetsorganisationen finns också i bilagan till detta dokument.

Ateas dataskyddspolicyer omfattar:

- Systemregistrering
- Dataklassificering
- Personuppgiftshantering
- Kundavtal

En översikt över dataskyddspolicyer följer:

Systemregistrering
Innan medarbetarna inleder en process för att samla in, hantera eller distribuera information måste de bekräfta att alla informationssystem som ska lagra eller behandla informationen är registrerade och godkända av landets Chief Information Security Officer. Detta omfattar även alla molntjänster som köps via en prenumeration och som sköts utanför Atea.

Chief Information Security Officer gör en analys av it-säkerheten och dataintegriteten för ett informationssystem innan systemet registreras och godkänns för användning på Atea. Analysen bygger på en checklista över it-säkerhets- och dataskyddsstandarder på Atea, och sammanställs tillsammans med koncernens Chief Information Security Officer.

Chief Information Security Officer tar också hänsyn till typen och känsligheten hos de data som ska lagras i systemet vid analysen av huruvida systemet uppfyller Ateas krav på informationssäkerhet. Som en del av analysen godkänner Chief Information Security Officer också en policy för radering av personuppgifter i systemet när Atea inte längre behöver dem (en ”dataminimeringspolicy”).

Om informationssystemet hanteras externt och innehåller personuppgifter – till exempel ett molnbaserat HR-system – måste Atea ha ett undertecknat personuppgiftsbiträdesavtal med tjänsteleverantören för att uppfylla GDPR. Ett standardiserat personuppgiftsbiträdesavtal för användning med en molntjänstleverantör finns på den globala informationssäkerhetssidan i landets intranät. Varje lands Chief Information Security Officer kan besvara frågor som rör personuppgiftsbiträdesavtalet och kan hjälpa till med processen med att erhålla ett undertecknat personuppgiftsbiträdesavtal från serviceleverantören.

Medarbetarna får inte lagra eller behandla företagsinformation i ”skugg-it-system” som inte är registrerade av landets Chief Information Security Officer. Medarbetarna får inte göra avsevärda förändringar i system eller processer för hantering av information utan att informera Chief Information Security Officer så att en ny utvärdering av it-säkerheten kan göras.

När ett system är godkänt för användning inom Atea ska en systemägare att tilldelas systemet. Systemägaren ansvarar för att se till att systemet används i enlighet med Ateas dataskyddspolicyer. Systemägaren är i synnerhet ansvarig för att se till att åtkomsträttigheterna till informationssystemet är begränsade enligt behovsprincipen och tas

bort så snart de inte längre behövs. Systemägaren ansvarar också för att se till att personuppgifter som lagras i systemet raderas när Atea inte längre behöver dem, i enlighet med dataminimeringspolicyn som överenskoms när systemet godkändes för användning.

Dataklassificering

När ett system är godkänt för användning på Atea ska typen och känsligheten hos de data som ska lagras i systemet dokumenteras för att säkerställa att lämpliga policyer för dataskydd upprätthålls.

Det finns många fall där medarbetarna hanterar och distribuerar information utanför ett godkänt it-system. Detta omfattar information som hanteras via utskrivna dokument, via e-postkommunikation eller genom fildelning (t.ex. en Microsoft Word/Excel/Powerpoint-fil).

För att se till att information som hålls utanför ett godkänt it-system hanteras med lämplig nivå av informationssäkerhet måste medarbetarna särskilt märka alla filer, dokument eller e-postmeddelanden som innehåller information i enlighet med dess känslighet, så att mottagaren av informationen är medveten om detta. Den här märkningen måste göras i enlighet med Ateas standarder för dataklassificering.

Ateas dataklassificeringsstandarder består av fem nivåer, som värderar informationen i e-postmeddelandet eller filen från minst känslig till mest känslig. Klassificeringsstandarderna är inbyggda i Ateas versioner av Microsoft Outlook och Word/Excel/Powerpoint. Medarbetarna kan automatiskt märka ett e-postmeddelande, dokument eller en fil med en korrekt dataklassificeringsmärkning genom att välja en knapp högst upp i dessa program.

De fem nivåerna är följande:

1. Icke affärsrelaterad:
Privata e-postkonversationer och dokument som inte är relaterade till Atea

2. Offentlig:
Atea-relaterad information som kan distribueras offentligt

3. Intern:
Information som fritt kan distribueras internt på Atea eller till Atea affärsområden och kontrakterade tredjeparts leverantörer. Inte avsedd för distribution utanför Atea eller ej kontrakterade parter.

4. Konfidentiell:
Information som bör hållas privat för mottagaren, och som inte får delas utan godkännande från ägaren till informationen. Detta omfattar personuppgifter, som bör märkas separat. En märkning för personuppgifter kan läggas till via en rullgardinsmeny under Konfidentiellt-knappen.

5. Strikt konfidentiell:
Information som kan ha avsevärt negativa konsekvenser för Atea om de yppas utan godkännande. Bör lagras i krypterat format och får inte delas utan godkännande från ägaren till informationen. Omfattar följande:

- Känsliga personuppgifter: Enligt GDPR måste vissa kategorier av personuppgifter hanteras med extra säkerhetsåtgärder. Det gäller information som rör: etniskt ursprung, politisk åsikt, religion, fackföreningsmedlemskap och genetisk eller biometrisk information. Känsliga personuppgifter bör märkas separat. Denna märkning kan läggas till via en rullgardinsmeny under Strikt konfidentiellt-knappen.

- Känslig affärsinformation: Detta är affärsinformation som till exempel viktig kund- eller leverantörsinformation, kontrakt och kommersiella villkor. Det omfattar också information som täcks av ett sekretess- eller konfidentialitetsavtal med en kund eller affärspartner. Slutligen kan det omfatta mycket känslig immateriell egendom, till exempel affärskoncept och internt utvecklade programvaror, metodiker och verktyg.

- Kurspåverkande information: Kurspåverkande information är en viss typ av konfidentiell information som kan påverka priset på Ateas aktier. Detta kan vara viktig finansiell information som ännu inte har rapporterats, eller hur det ligger till med konfidentiella förhandlingar som rör ett mycket stort kundkontrakt eller kommersiellt avtal.

- Koncernens CFO måste genast informeras om alla medarbetare som innehar kurspåverkande information. Dessa medarbetare registreras i Computershare Insider Management System (CIMS) som används av Atea. Ytterligare information om efterlevnad av rutiner för kurspåverkande information återfinns i uppförandekoden.

En fullständig beskrivning av Ateas klassificeringsstandarder och rutiner för märkning och kryptering av dokument och e-postkommunikation finns på den globala informationssäkerhetssidan i landets intranät.

Personuppgiftshantering

Enligt GDPR har Atea särskilda juridiska skyldigheter vid hantering av personuppgifter – information som kan hänföras till en specifik och identifierbar person. Dessa juridiska skyldigheter kräver att Atea dokumenterar att företaget har vidtagit tillräckliga tekniska och organisatoriska åtgärder för att uppfylla GDPR. Denna processdokumentation måste vid behov göras tillgänglig för offentliga myndigheter.

Innan Atea kan samla in personuppgifter måste affärsprocessen som personuppgifterna ska hanteras för bli fullt dokumenterad och granskad av Chief Information Security Officer. Varje funktions dataskyddsadministratör ansvarar för att se till att alla processer för hantering av personuppgifter i deras funktion är dokumenterade och aktuella i enlighet med GDPR.

Dokumentationen måste uppvisa att Atea har vidtagit tillräckliga tekniska och organisatoriska åtgärder för att uppfylla en individs rätt till sina personuppgifter, för att förhindra och minimera effekterna av en personuppgiftsincident, och för att agera lagenligt i händelse av en personuppgiftsincident. Processer för insamling av personuppgifter måste också omfatta en rutin för dataminimering, dvs. radering av personuppgifter som inte längre behövs.

Vid insamling av personuppgifter måste Atea meddela individen eller erhålla dennes samtycke till att personuppgifterna samlas in och används. Vid meddelande eller erhållande av samtycke från en person måste Atea förmedla följande information enligt GDPR:

1. Kategorier av personuppgifter som samlas in och behandlas
2. Syfte och rättslig grund för databehandlingen
3. Personuppgifternas mottagare eller kategorier av mottagare
4. Tidsperiod som informationen används under, eller vilka kriterier som avgör den här tidsperioden
5. Individens rätt till sina personuppgifter – inklusive rätten att återta samtycke och rätten till åtkomst, radering och korrigering
6. Individens rätt att klaga till en tillsynsmyndighet.
7. I tillämpliga fall, meddelande om att informationen kommer att överföras till ett annat land, och en bekräftelse på att eventuell behandling av uppgifterna i ett annat land sker i enlighet med bestämmelserna om lämpligt dataskydd i GDPR
8. Om känsliga personuppgifter insamlas måste Atea begära och erhålla uttryckligt samtycke från den individ vars information behandlas.

Ett standardsekretessavtal för insamling av personuppgifter finns på den globala informationssäkerhetssidan i landets intranät.

Atea har särskilda skyldigheter enligt GDPR i händelse av ett dataintrång som omfattar personuppgifter. Ett dataintrång är en informationssäkerhetsincident som leder till att obehöriga personer får åtkomst till information eller som leder till olaglig eller oavsiktlig förlust av information.

I händelse av ett dataintrång bör medarbetarna genast meddela landets eller den delade serviceenhetens Chief Information Security Officer. Chief Information Security Officer undersöker dataintrånget tillsammans med Ateas informationssäkerhetsorganisation och vidtar nödvändiga åtgärder för att rapportera och begränsa eventuell skada som orsakats av dataintrånget.

Om dataintrånget omfattar personuppgifter och leder till risken för skada för en individ måste Atea meddela tillsynsmyndigheten i det land där incidenten uppträdde inom 72 timmar från det att man blev medveten om incidenten. Meddelandet måste beskriva indicentens natur, en sammanfattning av de berörda datasubjekten och uppgifterna, de sannolika konsekvenserna av incidenten och vilka åtgärder som vidtagits.

Individer vars personuppgifter är inblandade i incidenten måste också meddelas direkt om det finns stor risk för skada för den personen. Ett offentligt meddelande kan räcka om det inte är möjligt att meddela individuellt.

Kundavtal

Atea hanterar datainfrastruktur och applikationer för många kunder, antingen hos kunden eller från sina egna datacenter. I dessa fall är Atea kontraktsmässigt ansvarigt för behandling av kundens information, och har ett juridiskt åtagande enligt GDPR för att säkerställa att man på lämpligt sätt skyddar datasekretessrättigheterna för alla individer vars personuppgifter ingår i kundens data.

För att uppfylla GDPR måste Atea ha ett personuppgiftsbiträdesavtal (DPA) med sina kunder vars datainfrastruktur och applikationer man hanterar. Personuppgiftsbiträdesavtalet måste dokumentera omfattningen, naturen och varaktigheten hos de databehandlingsaktiviteter som Atea utför enligt kundens instruktioner. Dokumentationen måste också omfatta en sammanfattning av vilka typer av personuppgifter som Atea behandlar för kundens räkning och vilka kategorier av personer som får sina personuppgifter behandlade.

Personuppgiftsbiträdesavtalet måste enligt GDPR innehålla följande bekräftelse från Atea:

1. Atea behandlar personuppgifter endast i enlighet med dokumenterade instruktioner från sin kund, och efterlever dataskyddslagstiftningar
2. Medarbetare som behandlar personuppgifter för kundens räkning är bundna av sekretess. Atea utser inga underleverantörer för att behandla personuppgifter för kundens räkning utan godkännande av kunden.
3. Atea har vidtagit tillräckliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsgrad som avtalats med kunden och som är avpassad efter risken för de uppgifter som behandlas.
4. Atea har vidtagit tillräckliga åtgärder för att uppfylla sina juridiska åtaganden när det gäller personers rättighet att kontrollera behandlingen av den egna informationen, enligt beskrivning i GDPR
5. Atea ger kunden den information som är nödvändig för att uppvisa sin efterlevnad av datasekretessåtaganden enligt GDPR och medverkar i en compliancerevision om kunden så önskar
6. Atea informerar kunden om eventuella personuppgiftsincidenter utan onödigt dröjsmål
7. Atea raderar eller återlämnar alla personuppgifter till kunden när tjänsteavtalet löper ut

Om Atea använder externa underleverantörer för att uppfylla sina databehandlingsåtaganden gentemot kunden (t.ex. tredje parts molntjänster, konsulter eller infrastrukturleverantörer), måste Atea först ha ett separat personuppgiftsbiträdesavtal med dessa underleverantörer, i vilket underleverantören tillhandahåller en liknande bekräftelse på uttalandena som uppges ovan.

Atea har ett standardiserat personuppgiftsbiträdesavtal som rekommenderas för användning med alla kunder och underleverantörer. Personuppgiftsbiträdesavtalet finns på den globala informationssäkerhetssidan i landets intranät. Varje lands Chief Information Security Officer kan besvara frågor som rör personuppgiftsbiträdesavtalet och kan hjälpa till med processen att erhålla ett undertecknat personuppgiftsbiträdesavtal från kunden eller underleverantören.

I händelse av en personuppgiftsincident som omfattar en kunds information måste Atea meddela kunden utan dröjsmål efter att man blivit medveten om incidenten. Atea måste därefter samarbeta med sin kund och vidta rimliga åtgärder för att säkerställa att kunden kan uppfylla sina åtaganden att rapportera incidenten enligt kraven i GDPR, och kan vidta korrigerande åtgärder för att minska den skada som orsakas av incidenten.

De viktigaste punkterna:

Systemregistrering
Alla it-system som används på Atea måste registreras hos Chief Information Security Officer i det land eller den affärsenhet där systemet används. Detta omfattar även molntjänster som köps via en prenumeration och som sköts utanför Atea.

Chief Information Security Officer granskar it-systemet för att bekräfta att det uppfyller Ateas it-säkerhetsstandarder innan systemet godkänns för användning. När systemet är registrerat utses en systemägare. Systemägarens roll är att säkerställa att systemet används i enlighet med företagets dataskyddspolicyer, med särskilt fokus på hantering av åtkomsträttigheter.

Dataklassificering
För att se till att information som hålls utanför ett godkänt it-system hanteras med lämplig nivå av informationssäkerhet måste medarbetarna särskilt märka alla filer, dokument eller e-postmeddelanden som innehåller information i enlighet med dess känslighet så att alla mottagare förstår detta. Markeringen måste vara i enlighet med Ateas standarder för dataklassificering.

Alla rutiner för hantering av personuppgifter måste också dokumenteras och granskas av Chief Information Security Officer. Varje region utser en dataskyddsadministratör som ansvarar för en viss affärsfunktion i landet (eller delade serviceenheten). Dataskyddsadministratörens roll är att kontrollera att alla affärsprocesser i deras affärsfunktion följer Ateas dataskyddspolicyer i enlighet med GDPR.

Personuppgiftshantering
Vid insamling av personuppgifter måste Atea enligt GDPR meddela individen eller erhålla dennes samtycke till att personuppgifterna samlas in och används. GDPR har många informationskrav som rör innehållet i meddelandet (se huvudtexten).

Ett dataintrång är en informationssäkerhetsincident som leder till att obehöriga personer får åtkomst till information eller som leder till olaglig eller oavsiktlig förlust av information. Atea har särskilda skyldigheter enligt GDPR i händelse av ett dataintrång som omfattar personuppgifter.

I händelse av ett misstänkt dataintrång bör medarbetarna genast meddela landets eller den delade serviceenhetens Chief Information Security Officer. Alternativt kan ett e-postmeddelande skickas till infosec@atea.com som vidarebefordras direkt till koncernens Chief Information Security Officer.

Atea måste enligt GDPR ha ett personuppgiftsbiträdesavtal (DPA) med sina kunder när företaget hanterar en kunds datainfrastruktur och applikationer. Atea måste också ha ett personuppgiftsbiträdesavtal med sina underleverantörer som behandlar information för Ateas räkning. GDPR har många informationskrav som rör innehållet i personuppgiftsbiträdesavtalet (se huvudtexten).

4. IT-INFRASTRUKTURSÄKERHET – OBLIGATORISKA RUTINER FÖR ALLA MEDARBETARE

Ateas it-infrastruktur består av all hårdvara, programvara och nätverkskomponenter som stöder leverans av affärssystem och it-processer till användare. Dataskyddet på Atea är beroende av att alla medarbetare använder företagets it-infrastrukturtillgångar på ett ansvarsfullt sätt.

Följande policyer rör alla medarbetare som användare av Ateas it-infrastruktur, och omfattar enhetssäkerhet, systemåtkomst, fillagring, nätverkssäkerhet, kommunikationer och fysisk säkerhet. Dessutom måste medarbetare med ansvar för hantering av Ateas it-verksamhet genomgå separat, mer uttömmande utbildning i it-säkerhet som motsvarar deras funktion.

Enhetssäkerhet:
Medarbetarna måste vidta säkerhetsåtgärder för sina arbetsenheter, t.ex. datorer, surfplattor och smarttelefoner. Dessa enheter är känsliga för stöld, skadlig programvara och obehörig användning. Företagets datorer, surfplattor och smarttelefoner bör alltid hållas under uppsikt eller förvaras på en säker plats. När de inte används bör enheterna låsas med en PIN/ett lösenord eller stängas av.

Alla företagets datorer, surfplattor och smarttelefoner bör ha krypteringslösningar installerade för att förhindra obehörig åtkomst till hårddisken. Ateas Windowsdatorer aktiveras med krypteringslösningen Bitlocker. För Apple Mac-modeller finns det en inbyggd funktion för kryptering av hårddisken som måste aktiveras vid användning. Kryptering är förinstallerat på alla iPhone- och iPad-enheter. Kryptering måste möjliggöras manuellt på Android-mobiler och surfplattor. Kryptering bör också aktiveras på borttagbara minnen som USB-minnen, som lätt kan tappas bort. Medarbetare som behöver hjälp med att kryptera sina arbetsenheter kan kontakta Ateas servicedesk.

Medarbetare bör inte ladda hem programvara som inte kommer från Ateas it-avdelning till sina datorer. Ateas it-avdelning erbjuder en rad programvaruapplikationer via sin Accelerator-portal. Dessa applikationer uppdateras regelbundet för att upprätthålla korrekt säkerhetsnivå. Om en medarbetare behöver ladda hem extern programvara som inte kommer från Accelerator-portalen till sin dator, bör denne först få godkännande av sin chef och sin lokala it-organisation.

Företagets datorer är förinstallerade med virusskydd och brandvägg. Om du undrar över ditt virusskydd, kontakta Ateas servicedesk. Om du får en varning om skadlig programvara om din dator uppträder på ett ovanligt sätt kan det vara ett tecken på att din dator har blivit smittad. Tecken på skadlig programvara på en dator kan vara att den ofta fryser eller blir ovanligt långsam, eller att operationer sker utan att du startat dem, inklusive popup-meddelanden eller andra ändringar på skärmen.

Om du misstänker att din dator har blivit smittad, avbryt först allt arbete på datorn och koppla bort den från nätverket. Kontakta sedan Ateas servicedesk, och berätta om vilka symtom som skapat misstankar om att datorn attackerats av skadlig programvara, och vilka händelser som kan ha lett till att datorn blivit smittad.

Alla arbetsenheter som tas ur bruk måste rensas från all information innan de skickas från Ateakontoret för service, återvinning eller återanvändning. Detta bör ske i enlighet med landets it-rutiner. Dessa rutiner finns på den globala informationssäkerhetssidan i landets intranät.

Systemåtkomst:
Medarbetare bör endast medges åtkomst till system när det krävs för deras arbete. Åtkomsträttigheter till system måste övervakas kontinuerligt för att säkerställa att den här policyn upprätthålls och att åtkomsten avbryts så snart den inte längre är nödvändig. Om en medarbetare har åtkomst till system denne inte längre behöver, bör personen genast kontakta systemägaren för att avbryta åtkomsträttigheterna.

När systemets åtkomsträttigheter medges till en medarbetare måste användarnamnet och det tillfälliga lösenordet distribueras separat. Det tillfälliga lösenordet måste genast ändras efter den första inloggningen och bör inte skrivas ner eller delas med någon. Medarbetare får inte låna ut åtkomsträttigheter till andra användare.

Lagring av filer:
Alla medarbetare är ansvariga för att se till att deras arbetsfiler (t.ex. MS Word/Excel/Powerpoint-filer) hanteras säkert. Alla slags filer bör lagras på Ateas interna delade filservrar, OneDrive-konton eller i Sharepoint-miljön. Inga andra externa lagringssajter, inklusive Dropbox eller Google Drive får användas för att lagra filer utan uttryckligt godkännande från landets it-avdelning, eftersom Atea inte kan garantera dessa lagringssajters säkerhet. Medarbetare bör inte lagra företagsinformation på hårddisken i sina lokala enheter, eftersom den informationen inte backas upp automatiskt och det därför finns risk för dataförlust.

Filer bör märkas enligt Ateas dataklassificeringsstandard (5 nivåer). Filer som märks med strikt konfidentiellt måste lagras i krypterat format. Filer som innehåller personuppgifter måste märkas och underhållas enligt GDPR.

Medarbetarna måste vara mycket försiktiga när de lagrar personuppgifter i filer, på grund av de strikta datasekretessreglerna i GDPR. Medarbetare får inte använda personuppgifter i filer utanför det ursprungliga syfte som definierades och meddelades till den individ vars data samlades in. Medarbetare måste begränsa delningen av filer som innehåller personuppgifter för att förhindra intrång eller missbruk av informationen och bör radera personuppgifter så snart de inte behövs. Detta gäller alla filer som skapas av medarbetare – inklusive MS Word/Excel/Powerpoint-filer.

Nätverkssäkerhet:
Endast Atea-klienter (datorer som konfigurerats enligt företagets standard) ska vara anslutna till ATEAs domän. Ateas mobila enheter ska endast anslutas till Ateas wifi-nätverk för mobila enheter. Andra datorer eller mobila enheter hänvisas till wifi-nätverket ATEA-guest.

Atea erbjuder medarbetare utanför kontoret möjligheten att ansluta till sitt interna nätverk via Cisco VPN eller via Citrix. Detta ger åtkomst till vårt gemensamma filsystem liksom våra gemensamma affärsapplikationer. För att ansluta till Cisco VPN krävs att datorn tillhör Atea, är medlem i Ateas domän (ONE) och har virusskydd installerat.

Medarbetare bör aldrig ansluta till en kunds nätverk utan föregående medgivande från kunden, om inte annat specificeras i ett kundavtal. Kunden bör kontaktas varje gång en medarbetare ansluter till deras nätverk och medarbetaren måste alltid rapportera till kunden vad som har gjorts i kundens nätverk.

Medarbetare bör vara försiktiga vid användning av offentliga wifi-nätverk under resor. Datatrafik över offentliga nätverk kan vara övervakad. Innan en medarbetare använder ett wifi-nätverk bör denne bekräfta att nätverket är säkert och från en legitim leverantör. Om det finns någon anledning att misstro säkerheten hos ett offentligt wifi-nätverk ska medarbetaren istället använda det mobila nätverket. Ateas servicedesk kan ge support för att ansluta en dator till det mobila nätverket.

Det förväntas att medarbetare använder internet i sitt dagliga arbete. Privat surfning är tillåten, men bör begränsas till sajter med innehåll som lämpar sig för arbetsplatsen. Onlinespel eller dobbel är inte tillåtet, och fildelning eller mediaströmning via internet bör begränsas till arbetsrelaterat innehåll. Alla medarbetare bör vara medvetna om att Atea analyserar trafiken via internet för att upptäcka attacker mot företaget, och detta spårar även olämplig användning av internet.

När du går till webbsidor på internet, var noggrann med att kontrollera att webbplatsen är korrekt – särskilt om du skickas från en annan sida. Klicka aldrig på länkar eller popup-meddelanden på webbplatser om de verkar misstänkta, eftersom dessa kan innehålla virus som kan laddas hem till din enhet.

Kommunikationer (e-post/sociala medier):
E-post är ett viktigt digitalt kommunikationsverktyg för medarbetarna. Det är också en viktig risk för informationssäkerheten, eftersom den ger angripare möjlighet att attackera Atea med skadlig programvara, bedrägeri eller andra hot, till en låg kostnad och med liten risk för åtal.

En vanligt förekommande typ av identitetsbedrägeri (”phishing”) mot Atea är när en angripare kontaktar en av våra medarbetare direkt via e-postkommunikation. E-postmeddelandet ser ut att komma från en betrodd källa, vanligen genom användning av falsk identitet, som t.ex. en annan medarbetare på Atea, en affärskontakt, eller en leverantör som ett teknikföretag eller en bank. E-postmeddelandet försöker lura medarbetaren att agera, till exempel att överföra pengar, ange inloggnings-/lösenordsdata eller annan känslig

information, eller att klicka på en länk eller bilaga som laddar hem skadlig programvara (”malware”) till medarbetarens dator eller mobil.

Meddelandet, bilagan eller länken verkar oskyldig – det kan till exempel se ut som e-post från en kollega, en offert/faktura från en leverantör eller som ett meddelande från ett molnkonto som OneDrive. Därför måste medarbetarna vara mycket vaksamma på potentiella bedrägerier i alla e-postmeddelanden eller annan kommunikation, även om den verkar komma från en betrodd källa.

Medarbetarna bör aldrig öppna länkar eller bilagor på sina enheter om de tvivlar på ett e-postmeddelandes eller en kommunikations legitimitet. Om en medarbetare är osäker på ett e-postmeddelandes legitimitet, eller om denne av misstag har svarat på ett möjligt bedrägeriförsök genom att öppna en misstänkt länk eller bilaga, bör de omedelbart rapportera till Ateas servicedesk.

Medarbetarnas e-postkonton angrips ofta av angripare som försöker få tillgång till en medarbetares känsliga affärsfiler. Av den anledningen bör e-post inte användas för lagring av viktig affärsinformation. Affärsinformation bör lagras eller distribueras via säkra affärssystem eller fildelningslösningar istället för via e-post.

Privat användning av e-post är tillåten om användningen inte står i konflikt till Ateas affärsintressen eller inkräktar på arbetstiden. Privat e-postkorrespondens bör alltid vara lämplig för arbetsplatsen, och bör märkas som ”Inte affärsrelaterad”. Dessutom bör användning av företagets e-postkonto för personlig kommunikation inte ge intryck av att korrespondensen sker för Ateas räkning eller är godkänd av företaget.

Sociala medier är också ett vanligt kommunikationsverktyg för medarbetarna. När de används korrekt ger sociala medier medarbetarna möjlighet att förvärva och överföra kunskap, att bygga upp kommersiella relationer och att stärka Ateas varumärke. Å andra siden kan sociala medier var mycket skadliga för Atea och dess medarbetare om de används olämpligt eller om känslig information delas.

Medarbetarna bör därför vara mycket försiktiga med vilken information de delar i sociala medier. Personuppgifter (inklusive namn, foton etc.) kan endast delas i sociala medier som hör till Ateas verksamhet om personen vars information delas samtycker till användningen.

Kontorssäkerhet:
Medarbetarna bör bära id-brickor för identifiering. Alla besökare på Atea måste registrera sig i receptionen och utrustas med en id-bricka för besökare som de bör bära väl synlig. Besökare bör mötas i reception i början av besöket och följas tillbaka till receptionen för att återlämna sin bricka i slutet av besöket. Besökare bör inte lämnas ensamma i Ateas lokaler.

All känslig information bör avlägsnas från skrivbord och förvaras säkert när den inte används. Alla information på whiteboards bör raderas i slutet av möten. Konfidentiella dokument bör alltid förstöras i dokumentförstörare eller kastas i speciella sekretesspapperskorgar när de inte längre behövs.

De viktigaste punkterna – it-infrastruktursäkerhet:

Enhetssäkerhet:
Alla företagets datorer, surfplattor och smarttelefoner bör ha krypteringslösningar installerade för att förhindra obehörig åtkomst till hårddisken. Företagets datorer, surfplattor och smarttelefoner bör alltid hållas under uppsikt eller förvaras på en säker plats. När de inte används bör enheterna låsas med en PIN/ett lösenord eller stängas av.

Medarbetare bör inte ladda hem programvara som inte kommer från Ateas it-avdelning till sina datorer. Om en medarbetare behöver ladda hem extern programvara som inte kommer från Atea till sin dator, bör denne först få godkännande av sin chef och sin lokala it-organisation.

Företagets datorer är förinstallerade med virusskydd och brandvägg. Om du undrar över ditt virusskydd, kontakta Ateas servicedesk.

Om du misstänker att din dator har blivit smittad med skadlig programvara eller är utsatt för risk, avbryt först allt arbete på datorn och koppla bort den från nätverket. Kontakta sedan Ateas servicedesk.

Systemåtkomst:
Medarbetare bör endast medges åtkomst till system när det krävs för deras arbete. Åtkomsträttigheter till system måste övervakas kontinuerligt för att säkerställa att den här policyn upprätthålls och att åtkomsten avbryts så snart den inte längre är nödvändig.

Lagring av filer:
Alla medarbetare är ansvariga för att se till att deras arbetsfiler (t.ex. MS Word/Excel/Powerpoint-filer) hanteras säkert. Filer bör märkas enligt Ateas dataklassificeringsstandarder (5 nivåer), med en separat märkning för filer som innehåller personuppgifter. Filer som märks med strikt konfidentiellt måste lagras i krypterat format.

Alla slags filer bör lagras på Ateas interna delade filservrar, OneDrive-konton eller i Sharepoint-miljön. Inga andra externa lagringssajter, inklusive Dropbox eller Google Drive, får användas för att lagra filer utan uttryckligt godkännande från landets it-avdelning. Medarbetare bör inte lagra företagsinformation på hårdisken på sin lokala enhet.

Nätverkssäkerhet:
Endast Atea-klienter (datorer som konfigurerats enligt företagets standard) ska vara anslutna till ATEAs domän. Ateas mobila enheter ska endast anslutas till Ateas wifi-nätverk för mobila enheter. Andra datorer eller mobila enheter hänvisas till wifi-nätverket ATEA-guest.

Medarbetare bör vara försiktiga vid användning av offentliga wifi-nätverk. Innan en medarbetare använder ett wifi-nätverk bör denne bekräfta att nätverket är säkert och från en legitim leverantör.

Åtkomst till internet från en arbetsenhet bör begränsas till sajter med innehåll som lämpar sig för arbetsplatsen. Alla medarbetare bör vara medvetna om att Atea analyserar trafiken via internet för att upptäcka attacker mot företaget, och detta spårar även olämplig användning av internet.

När du går till webbplatser bör du vara noggrann med att kontrollera att webbplatsen är korrekt – särskilt om du skickas från en annan sida. Klicka aldrig på länkar eller popup-meddelanden på webbplatser om de verkar misstänkta, eftersom dessa kan innehålla virus som kan laddas hem till din enhet.

Kommunikationer (e-post/sociala medier):
E-post är också en viktig risk för informationssäkerheten, eftersom den ger angripare möjlighet att attackera Atea med skadlig programvara, bedrägeri eller andra hot, till en låg kostnad och med liten risk för åtal.

En vanligt förekommande typ av identitetsbedrägeri ("phishing") mot Atea är när en angripare kontaktar en av våra medarbetare direkt via e-postkommunikation. E-postmeddelandet ser ut att komma från en betrodd källa, vanligen genom användning av falsk identitet, som t.ex. en annan medarbetare på Atea, en affärskontakt, eller en leverantör som ett teknikföretag eller en bank. E-postmeddelandet försöker lura medarbetaren att agera, till exempel att överföra pengar, ange inloggnings-/lösenordsdata eller annan känslig information, eller att klicka på en länk eller bilaga som laddar hem skadlig programvara ("malware") till medarbetarens dator eller mobil.

Medarbetarna bör aldrig öppna länkar eller bilagor på sina enheter om de tvivlar på ett e-postmeddelandes eller en kommunikations legitimitet. Om en medarbetare är osäker på ett e-postmeddelandes legitimitet, eller om denne av misstag har svarat på ett möjligt bedrägeriförsök genom att öppna en misstänkt länk eller bilaga, bör de omedelbart rapportera till Ateas servicedesk.

Privat användning av e-post är tillåten om användningen inte står i konflikt till Ateas affärsintressen eller inkräktar på arbetstiden. Privat e-postkorrespondens bör alltid vara lämplig för arbetsplatsen, och bör märkas som "Inte affärsrelaterad".

Medarbetarna bör vara mycket försiktiga med vilken information rörande Atea som de delar i sociala medier. Personuppgifter (inklusive namn, foton etc.) kan endast delas i sociala medier som hör till Atea om personen vars information delas samtycker till användningen.

Kontorssäkerhet:
Medarbetarna bör bära id-brickor för identifiering. Alla besökare på Atea måste registrera sig i receptionen och utrustas med en id-bricka för besökare som de bör bära väl synlig.

All känslig information bör avlägsnas från skrivbord och förvaras säkert när den inte används.

Innehav
Atea ASA
Atea ASA
Brynsalleen 2
Box 6472 Etterstad
NO-0605 Oslo
+47 22 09 50 00
Org.nr 920 237 126
investor@atea.com
atea.com

Norge
Atea AS
Brynsalleen 2
Box 6472 Etterstad
NO-0605 Oslo
+47 22 09 50 00
Org.nr 976 239 997
info@atea.no
atea.no

Sverige
Atea AB
Kronborgsgränd 1
Box 18
SE-164 93 Kista
+46 (0)8 477 47 00
Org.nr 556448-0282
info@atea.se
atea.se

Danmark
Atea A/S
Lautrupvang 6
DK-2750 Ballerup
+45 70 25 25 50
Org.nr 25511484
info@atea.dk
atea.dk

Finland
Atea Oy
Jaakonkatu 2
PL 39
FI-01621 Vanda
+ 358 (0)10 613 611
Org.nr 091 9156-0
customercare@atea.fi
atea.fi

Litauen
Atea Baltic UAB
J. Rutkausko st. 6
LT-05132 Vilnius
+370 5 239 7899
Org.nr 300125003
info@atea.lt
atea.lt

Koncernlogistik
Atea Logistics AB
Smedjegatan 12
Box 159
SE-351 04 Växjö
+46 (0)470 77 16 00
Org.nr 556354-4690
customer.care@atea.se

Koncernens gemensamma tjänster
Atea Global Services SIA
Mukusalas Street 15
LV-1004 Riga
+371 67359600
Org.nr 50203101431
rigainfo@atea.com
ateaglobal.com

ATEA