TP2B THE PLACE TO BE

ATEA

INFORMASJONSSIKKERHET OG RISIKOSTYRING: RETNINGSLINJER FOR ANSATTE

Versjon 1.0 - publisert august 2019

BREV FRA CEO

I Atea er misjonen vår «Build the future with IT».

Vi tror at informasjonsteknologi kombinert med kunnskap og kreativitet kan forbedre produktiviteten og levestandarden i hele samfunnet. Vi hjelper private selskaper og offentlige foretak i arbeidet med å utvikle digitale løsninger som setter dem i stand til å oppnå mer, og det med større effektivitet og mindre ressursbruk.

Samtidig forstår vi risikoene som følger med teknologi som lagrer og behandler stadig mer informasjon. Etter hvert som organisasjonene håndterer mer data og automatiserer flere prosesser via IT-systemene og nettverkene sine, står de overfor større trusler i form av datatyveri, identitetssvindel og driftsavbrudd som følge av nettangrep. Brudd på datasikkerheten kan også føre til at personopplysninger blir brukt uten samtykke eller blir misbrukt for å skade og krenke folks personvern.

Atea er den ledende leverandøren av informasjonsteknologi i Norden og Baltikum og har et særskilt ansvar for å sikre at selskapets operasjoner skjer i samsvar med strenge informasjonssikkerhetsstandarder. Atea utvikler, implementerer og drifter IT-infrastrukturløsninger for de største og mest vitale organisasjonene i regionene våre. De største kundene våre er nasjonale og lokale myndigheter, deriblant viktige samfunnsaktører som forsvar og politi. Vi leverer også virksomhetskritiske IT-løsninger til de største selskapene i vår region.

Dette dokumentet er veiledende for håndtering av informasjonssikkerhetsrisikoer i Atea. Det gir en oversikt over sentrale sikkerhetsrisikoer, retningslinjer for personvern og styringsprosedyrer som alle i selskapet skal følge. Ansatte som har et spesielt ansvar for IT-drift og systemadministrasjon, må gjennomføre og bestå egne tester i informasjonssikkerhet og retningslinjer for personvern, alt etter hva rollen deres krever.

Dokumentet er delt inn i fire avsnitt, hvert med en avsluttende oppsummering av hovedpunktene. De fire avsnittene er detaljerte, ettersom dette er et komplisert og forretningskritisk emne. Det er ekstra viktig at de ansatte merker seg og husker hovedpunktene i slutten av hvert avsnitt, og at de er i stand til å finne frem i resten av dokumentet ved behov.

Innholdet i dette dokumentet er obligatorisk kunnskap for alle Ateas ansatte. For å sikre at alle Ateas ansatte har forstått innholdet i dette dokumentet er det lagt til ti spørsmål om informasjonssikkerhet i avgangsprøven til det etiske regelverket (Code of Conduct), som er obligatorisk for alle Ateas ansatte. Ansatte kan ta et nettbasert kurs om Ateas retningslinjer for informasjonssikkerhet (information security policy) for å forberede seg til nevnte tester.

Atea er en stor organisasjon med nesten 90 kontorer i sju land. Det er utnevnt en Chief Information Security Officer for Atea Group og en for hvert land som skal bistå med implementeringen av retningslinjer for informasjonssikkerhet i hele organisasjonen.

Steinar Sønsteby
CEO

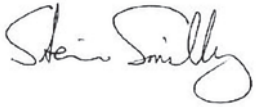
Hvis du har spørsmål eller vil ta opp noe angående informasjonssikkerheten i Atea, kan du gå frem på følgende måte:

- Hvis du tror at PC-en din er infisert av skadevare (malware) eller har spørsmål om IT-sikkerhet, kan du kontakte Ateas servicedesk
- Hvis du vil rapportere mistenkelig e-post, svindelforsøk eller noe annet som kan utgjøre en risiko for informasjonssikkerheten i Atea, kan du kontakte Ateas servicedesk
- Hvis du vil rapportere mistanke om et brudd på reglene for vern av personopplysninger eller bedriftsopplysninger (f.eks. uautorisert formidling av dette) i informasjonssystemer eller dokumenter, kan du kontakte Chief Information Security Officer i det landet du jobber i. Alternativt kan du sende en e-post direkte til infosec@atea.com.

Hvis du ønsker å snakke direkte med Chief Information Security Officer (CISO) i Atea Group eller med CISO for ditt land eller for fellestjenester, finner du navnet på Ateas nettsted for etterlevelse: atea.com/trust. E-post som sendes til infosec@atea.com, vil bli direkte videresendt til Chief Information Security Officer i Atea Group.

Vi svarer gjerne på spørsmål og tilbakemeldinger og lover at ingen vil bli utsatt for reprimander som følge av de rapporterer inn problematiske forhold. Men hvis du foretrekker å rapportere en sak anonymt, kan du sende inn en rapport via direktelinjen «Whistleblower Hotline». Du finner en link til Whistleblower Hotline på Ateas nettsted for etterlevelse: atea.com/trust. Saker som rapporteres til Whistleblower Hotline, sendes til et uavhengig advokatfirma som vil oppsummere og rapportere saken til relevante nivå i Ateas organisasjon.

Det er svært viktig at vi opprettholder strenge standarder for informasjonssikkerhet i Atea, og at vi er i stand til å samarbeide med kunder og partnere om de viktigste IT-utfordringene i vår region. Takk for at du overholder Ateas retningslinjer for informasjonssikkerhet, og for at du bidrar til å gjøre Atea til «The place to be».



Hovedpunkter:

Det er helt avgjørende at alle ansatte støtter opp om strenge standarder for informasjonssikkerhet.

Det er utnevnt en Chief Information Security Officer for Atea Group og en for hvert land som skal bistå med implementeringen av retningslinjer for informasjonssikkerhet i hele Atea. Du finner navnene til Chief Information Security Officers på Ateas nettsted for etterlevelse: atea.com/trust.

Hvis du har spørsmål eller vil ta opp noe angående informasjonssikkerheten i Atea, kan du gå frem på følgende måte:

- Hvis du tror at PC-en din er infisert av skadevare (malware) eller har spørsmål om IT-sikkerhet, kan du kontakte Ateas servicedesk
- Hvis du vil rapportere mistenkelig e-post, svindelforsøk eller noe annet som kan utgjøre en risiko for informasjonssikkerheten i Atea, kan du kontakte Ateas servicedesk
- Hvis du vil rapportere mistanke om et brudd på reglene for vern av personopplysninger eller bedriftsopplysninger (f.eks. uautorisert formidling av dette) i informasjonssystemer eller dokumenter, kan du kontakte Chief Information Security Officer i det landet du jobber i.
- Alternativt kan du sende en e-post til infosec@atea.com, som så vil bli videresendt til Chief Information Security Officer i Atea Group

Innhold

1. INFORMASJONSSIKKERHET – OVERSIKT OG RISIKOSTYRING

Informasjon er viktig for at enhver organisasjon skal fungere. Et styringssystem for informasjonssikkerhet (ISMS) er et utvalg retningslinjer, prosedyrer, verktøy og aktiviteter som en organisasjon bruker for å beskytte informasjonsressursene sine mot uautorisert tilgang og misbruk.

Opprettelse av et ISMS krever at organisasjonen identifiserer hvilke informasjonsressurser den sitter på. Dette omfatter alle data (opplysninger) som organisasjonen håndterer, uavhengig av format: digitalt, på papir eller verbalt. I Atea kan slik informasjon bli brukt internt eller bestå av eksterne data som Atea håndterer og behandler på vegne av kundene sine.

Formålet med et styringssystem for informasjonssikkerhet er å beskytte og bevare informasjonens konfidensialitet, integritet og tilgjengelighet.

- Med **konfidensialitet** menes at informasjon bare gjøres tilgjengelig for autoriserte personer.
- Med **integritet** menes at informasjonen oppbevares slik at den holdes komplett og nøyaktig.
- Med **tilgjengelighet** menes at autoriserte brukere kan få tilgang til og bruke data når det trengs.

For å nå disse målene bør en organisasjon gjennomføre en risikovurdering for å identifisere hvordan organisasjonens informasjonsressurser eksponeres for potensielle brudd på informasjonssikkerheten. Deretter kan man utvikle et styringssystem for informasjonssikkerhet som kan håndtere og kontrollere disse risikoene på en effektiv måte uten unødvendige kostnader eller tapt produksjonsevne.

Risikovurdering ved Atea

Følgende informasjonssikkerhetsrisikoer er gitt høyeste prioritet for Ateas virksomhet:

1. **Fysisk tap:**
   Informasjon lagres på fysiske enheter som kan bli mistet, stjålet eller skadet. Tilgangskontroll, kryptering og sikkerhetskopiering av data (backup) er viktig for å begrense potensielle risikoer for fysiske aktiva, for eksempel PC-er, mobiltelefoner, servere og lagringsenheter. Datasentre er særlig sårbare og må beskyttes mot trusler fra omgivelsene, herunder temperatur og brann.
2. **Identitetssvindel:**
   Atea er hele tiden utsatt for svindelforsøk fra angripere som bruker falske identiteter eller bedrageriforsøk for å utnytte de ansattes tillit. Formålet med et svindelforsøk er som regel å stjele noe fra Atea eller å få tilgang til Ateas systemer og nettverk.

   Én form for identitetssvindel mot Atea er å bruke falske eller stjålne kundeopplysninger til å bestille IT-utstyr, særlig gjennom Atea eShop. I tillegg til tilgangskontroller i eShop har Atea forretningsmessige rutiner for å granske nye kundekontoer og identifisere uvanlig kundeaktiviteter på eksisterende kontoer, slik at vi kan redusere risikoen for bedragerske transaksjoner.

   En annen svært vanlig form for identitetssvindel er såkalt «phishing», der en angriper tar direkte kontakt med en ansatt i Atea, gjerne via e-post. E-posten ser ut til å komme fra en pålitelig kilde, ofte ved at man bruker en falsk identitet, for eksempel tilhørende en annen medarbeider i Atea, en forretningsforbindelse eller en leverandør, for eksempel et teknologiselskap eller en bank. E-posten har da til formål å lure den ansatte til å utføre en bestemt oppgave, for eksempel overføre penger, taste inn brukeropplysninger, passord eller annen sensitiv informasjon, eller å klikke på en link eller et vedlegg som automatisk laster ned ondsinnet programvare («skadevare») på brukerens PC eller mobiltelefon.

   E-posten, vedlegget eller linken ser gjerne uskyldig ut: For eksempel kan den være skjult som en e-post fra en kollega, et tilbud eller en faktura fra en leverandør eller som en melding fra en nettskykonto, for eksempel OneDrive. Derfor må Ateas ansatte være på vakt for muligheten for svindel i all e-post og annen kommunikasjon, også når kommunikasjonen ser ut til å komme fra en betrodd kilde.

   Ateas ansatte bør aldri åpne linker eller vedlegg på enhetene sine hvis de er i tvil om hvorvidt en e-post eller annen kommunikasjon er legitim.

Hvis en av Ateas ansatte er usikker på om en e-post er legitim eller har kommet til skade for å svare på et mulig svindelforsøk ved åpne en mistenkelig link, bør vedkommende umiddelbart rapportere saken til Ateas servicedesk.

Selv om e-post er den vanligste metoden for såkalte phishing-angrep, bør de ansatte også være på vakt mot svindelforsøk i andre kommunikasjonskanaler, for eksempel i form av forespørsler per telefon eller invitasjoner via sosiale medier.

3. Tyveri av forretningshemmeligheter:
Hvis uautoriserte personer får tilgang til Ateas informasjonssystemer, kan de prøve å stjele proprietær informasjon som er av betydning for Ateas virksomhet. Dette kan inkludere forretningshemmeligheter som kunde- eller leverandøropplysninger, kontrakter og forretningsvilkår. Det kan også inkludere åndsverk som forretningskonsepter, produkt- eller tjenestedesign eller programvare, metoder og verktøy som er utviklet internt.

Ansatte som har tilgang til kjernesystemer, kan også tenkes å ville stjele forretningshemmeligheter fra Atea, for eksempel hvis de planlegger å slutte i selskapet. For å redusere risikoene skal informasjonstilgangen til de ansatte være behovsprøvd (altså at man må ha saklig behov for den). Systemtilgangen bør løpende granskes for å sikre at prinsippet om behovsprøving opprettholdes, og at en brukers tilganger opphører når vedkommende ikke lenger har behov for dem.

I tillegg til tilgangskontroll bruker Atea såkalte SIEM-verktøy (Security Information and Event Management) til å analysere logger og se hvilke handlinger som er utført i selskapets systemer.

4. Forstyrrelse av forretningsvirksomheten:
Ateas forretningsvirksomhet er avhengig av selskapets IT-systemer. Hvis tilgangskontrollene blir brutt, eller hvis systemene blir misbrukt, kan informasjon som tilhører ansatte eller forretningsforbindelser, lekke ut. Informasjon som er nødvendig for at Atea skal kunne drive forretninger, kan bli manipulert eller slettet. Eller forretningstransaksjoner kan bli påvirket eller godkjent av uautoriserte personer i strid med Ateas styringskontroller. Alle slike hendelser vil forstyrre Ateas forretningsvirksomhet.

Atea risikerer også forstyrrelser av virksomheten som følge av sofistikerte hackerangrep som potensielt kan slå av viktige IT-systemer eller nettverk. Systemene kan bli infisert av skadevare som blokkerer brukernes tilgang til kritiske funksjoner, eller som hindrer dem i å lese datafiler med mindre man betaler løsepenger (såkalt «ransomware» eller «løsepengevirus»). Nettverk og servere kan bli overbelastet av trafikk eller forespørsler, slik at de ikke lenger kan håndtere legitime transaksjoner («denial-of-service attack» eller «tjenestenektangrep»). Slike angrep kan ramme Atea eller kunder som Atea administrerer via sine datasentre.

5. Avtalerelaterte skader:
Atea har inngått konfidensielle avtaler med mange kunder, leverandører og forretningspartnere. Selskapet har også tjenestenivåavtaler og databehandleravtaler med kunder som nyter godt av Ateas IT-tjenester og IT-support.

Et brudd på IT-sikkerheten i Atea kan føre til at Atea bryter taushetsplikten, avtalte tjenestenivåer eller databehandleravtaler med kunder og andre forretningspartnere. Dette kan føre til at det rettes erstatningssøksmål mot Atea som følge av avtalebrudd. I tillegg til direkte skade kan et brudd på IT-sikkerheten medføre varig skade på Ateas forretningsrelasjoner med kunder og partnere.

Selv i situasjoner der Atea ikke er bundet av en bestemt avtale, kan vi bli gjenstand for rettslige krav fra selskaper eller enkeltpersoner dersom dataene deres blir stjålet eller misbrukt, med mindre vi kan godtgjøre at vi har utvist den nødvendige forsiktighet ved håndtering av dataene.

6. Bøter:

Atea er registrert ved Oslo Børs og må følge strenge rettslige krav ved håndtering av opplysninger som er ukjent for markedet, og som kan ha innvirkning på selskapets aksjekurs («kurssensitiv informasjon»). Dette kan være informasjon om store nye kontrakter eller økonomiske resultater som ennå ikke er offentliggjort.

Atea må håndtere kurssensitiv informasjon konfidensielt for å sikre at den ikke formidles til andre enn et begrenset antall registrerte «innsidere» som har et saklig behov for den. Ansatte som sitter på kurssensitiv informasjon, skal være registrert av selskapet og er underlagt særskilte krav om taushetsplikt og begrensninger på kjøp og salg av Atea-aksjer. Brudd på disse rettslige kravene kan straffeforfølges og medføre bøter i henhold til verdipapirhandelloven.

Atea kan også idømmes bøter ved brudd på personvernet (overtredelsesgebyr), slik det fremgår av den europeiske personvernforordningen (GDPR). Ettersom kravene i GDPR er ganske omfattende, er dette emnet omhandlet separat i neste avsnitt i dette dokumentet om personvern.

Hovedpunkter:

Alle ansatte må være svært forsiktige når de håndterer informasjons- og IT-systemer for å unngå brudd på sikkerheten.

IT-utstyr kan bli mistet, stjålet eller skadet. Tilgangskontroll, kryptering og sikkerhetskopiering (backup) er derfor avgjørende for å begrense informasjonssikkerhetsrisikoene.

Atea er hele tiden utsatt for svindelforsøk fra angripere som bruker falske identiteter eller bedrageriforsøk for å utnytte de ansattes tillit. Vær oppmerksom på at enhver e-post eller annen kommunikasjon du mottar, kan være et svindelforsøk, selv om den ser ut til å komme fra en legitim kilde (herunder en leder i Atea, en kunde, en teknologileverandør eller via sosiale medier).

Vær obs på all uvanlig kommunikasjon og alle uvanlige aktiviteter du kommer over. Hvis du mistenker at du blir utsatt for et svindelforsøk via e-post eller en annen melding, bør du ta opp saken med Ateas servicedesk. Ikke svar på mistenkelig kommunikasjon, for eksempel ved å åpne e-postvedlegg eller eksterne linker, eller ved å effektuere bestillinger eller betalinger.

For å redusere risikoen for tyveri eller misbruk av informasjon skal informasjonstilgangen til de ansatte være behovsprøvd. Systemtilgangen bør løpende granskes for å sikre at en brukers tilganger opphører når vedkommende ikke lenger har behov for dem.

Brudd på informasjonssikkerheten kan føre til alvorlig skade for Atea i form av forstyrrelse av forretningsvirksomheten, brudd på Ateas avtalefestede forpliktelser overfor kunder og forretningspartnere, bøter og skader på Ateas omdømme og forretningsrelasjoner.

2. PERSONVERN – OVERSIKT OG RISIKOSTYRING

Med personvern menes en persons kontroll over sine egne data eller opplysninger – særlig vedkommendes rett til å bestemme når og hvordan opplysningene samles inn, formidles (deles) og brukes. Personopplysninger er definert som informasjon, i en hvilken som helst form, som kan føres tilbake til en bestemt identifiserbar person.

Personverneteravhengigavinformasjonssikkerhet, dvs. hvordan data beskyttes mot uautorisert tilgang og misbruk. Men personvern handler også om vern av en enkeltpersons myndighet over sine egne opplysninger. Særlig hvordan en organisasjon gir den enkelte mulighet til å kontrollere bruken av personopplysningene sine når organisasjonen samler inn og behandler informasjon om vedkommende.

Atea mener at personvern er en grunnleggende menneskerett, og vi er opptatt av å håndtere personopplysninger på en måte som fullt ut respekterer denne rettigheten. Atea er underlagt strenge rettslige krav ved håndtering av personopplysninger i henhold til den europeiske personvernforordningen (GDPR).

De kravene i GDPR som er særlig viktige for Atea, kan oppsummeres slik:

Krav til innsamling av personopplysninger
Atea kan bare behandle (dvs. samle inn, lagre og bruke) personopplysninger når det foreligger en berettiget forretningsinteresse til det, og når rette vedkommende har gitt samtykke til det eller blitt informert om at personopplysningene blir behandlet. Detaljene for et slikt varsel eller samtykke er beskrevet i neste avsnitt i dette dokumentet.

Rett til kontroll av personopplysninger
Atea må etterkomme enkeltpersoners ønske om å kontrollere bruken av personopplysningene deres i samsvar med de rettighetene de har under GDPR. Under GDPR har enkeltpersoner krav på tilgang til personopplysninger om dem som Atea sitter på. Den enkelte har også rett til å få feil i personopplysningene sine rettet opp, å få dem slettet eller å begrense behandling og bruk av personopplysningene deres.

Dokumentasjon av behandlingsaktiviteter
Atea må dokumentere omfanget av sine databehandlingsaktiviteter for personopplysninger. Dette bør inkludere en beskrivelse av hva slags personopplysninger som blir behandlet, og for hvilke personkategorier. Det bør også inkludere en beskrivelse av hvilke tekniske og organisasjonsmessige tiltak som er truffet for å forhindre og minimalisere virkningen av eventuelle brudd på personvernet i Ateas databehandlingsaktiviteter («innebygd personvern»).

Databehandleravtaler med kunder/leverandører
Når Atea leverer databehandlingstjenester til kunder (f.eks. når Atea håndterer datainfrastruktur og applikasjoner for kunder, enten ute hos kunden eller fra sine egne datasentre), må Atea i tillegg ha inngått en gyldig databehandleravtale med kunden som er i overensstemmelse med kravene i GDPR.

Og når Atea på tilsvarende måte behandler personopplysninger via en underleverandør (f.eks. når Atea bruker programvare som driftes hos en leverandørs datasenter, f.eks. ved bruk av skytjenester), må Atea ha inngått en gyldig databehandleravtale som er i samsvar med GDPR, med selskapet som håndterer applikasjonen og som behandler personopplysninger på vegne av Atea. Informasjon som skal behandles utenfor EU/EØS, må behandles i et land eller innenfor et rammeverk som offentlige myndigheter anser for å ha passende sikkerhetstiltak for personvern.

Krav i tilfelle brudd på personvernet
I tilfelle det oppstår et brudd på personvernet som kan være til skade for en enkeltperson, må Atea varsle tilsynsmyndigheten (datatilsynet) i det landet der bruddet fant sted, innen 72 timer etter at man ble klar over situasjonen. Et slikt varsel må beskrive bruddets art, gi en oversikt over de berørte registrerte personene og opptegnelsene, sannsynlige konsekvenser av bruddet og hvilke tiltak som treffes.

De enkeltpersonene hvis personvern er blitt krenket, må også varsles direkte dersom det er stor fare for at hendelsen er til skade for vedkommende. Det kan være nok med en offentlig kunngjøring av forholdet dersom det ikke er mulig å varsle den enkelte.

Under GDPR kan tilsynsmyndigheten i det enkelte land ilegge et selskap store overtredelsesgebyrer i tilfelle brudd på GDPR. Overtredelsesgebyrets størrelse er avhengig av bruddets art, skadeomfanget og de tiltakene selskapet har truffet for å forebygge og håndtere bruddet. Maksimalt overtredelsesgebyr ved brudd på GDPR er 4 % av samlet global årsomsetning eller 20 millioner euro, avhengig av hvilket beløp som er høyest.

Ut fra kravene i GDPR er det helt avgjørende at Atea dokumenterer alle rutiner der man er i berøring med personopplysninger, og identifiserer alle interne applikasjoner og avtaler som medfører behandling av personopplysninger. Denne informasjonen må være tilgjengelig for Chief Information Security Officer i hvert land, slik at man kan få bekreftet at man har på plass egnede tiltak for å sikre personvernet. Du finner Chief Information Security Officer for hvert land og for konsernet på Ateas nettsted for etterlevelse (atea.com/trust).

Hovedpunkter:

Med personvern menes en persons kontroll over sine egne data eller opplysninger – særlig vedkommendes rett til å bestemme når og hvordan opplysningene samles inn, formidles (deles) og brukes. Personopplysninger er definert som informasjon, i en hvilken som helst form, som kan føres tilbake til en bestemt identifiserbar person.

Atea er underlagt strenge rettslige krav ved håndtering av personopplysninger i henhold til den europeiske personvernforordningen (GDPR).

Under GDPR:

Atea kan bare behandle (dvs. samle inn, lagre og bruke) personopplysninger når det foreligger en berettiget forretningsinteresse til det, og når rette vedkommende har gitt samtykke til det eller blitt informert om at personopplysningene blir behandlet.

Atea må etterkomme enkeltpersoners ønske om å kontrollere bruken av personopplysningene deres i samsvar med de rettighetene de har under GDPR.

Atea må dokumentere omfanget av databehandlingsaktiviteter i forbindelse med personopplysninger, herunder hvilke tiltak som er truffet for å forebygge og minimalisere virkningene av et eventuelt brudd på personvernet. Dette forutsetter at Atea dokumenterer alle rutiner der man er i berøring med personopplysninger, og alle interne applikasjoner og avtaler som medfører behandling av personopplysninger.

Atea må inngå en gyldig databehandleravtale med alle kunder som selskapet skal levere databehandlingstjenester til (f.eks. håndtering av datainfrastruktur og applikasjoner, enten ute hos kundene eller fra sine egne datasentre).

Atea må også ha en gyldig databehandleravtale med alle leverandører eller underleverandører som behandler personopplysninger på vegne av Atea (f.eks. når de leverer programvare til dette eller står for datalagring i sine egne datasentre, f.eks. i en skytjeneste).

I tilfelle det oppstår et brudd på personvernet som kan være til skade for en enkeltperson, må Atea varsle tilsynsmyndigheten (datatilsynet) i det landet der bruddet fant sted, innen 72 timer etter at man ble klar over situasjonen.

3. RETNINGSLINJER FOR PERSONVERN I ATEA

Ateas ansatte må følge selskapets retningslinjer for personvern hver gang de samler inn, håndterer og distribuerer data (opplysninger). Alle Ateas ansatte er ansvarlige for å sikre at forretningsprosessene som ligger innenfor ansvarsområdet deres, er i samsvar med Ateas retningslinjer for personvern, og at deres underordnede følger disse forretningsprosessene.

Alle ledere i Atea får utnevnt en personvernadministrator som er ansvarlig for en bestemt forretningsfunksjon i sitt land (eller avdeling for fellestjenester). Personvernadministratorens rolle er å undersøke at alle forretningsprosesser innenfor sin forretningsfunksjon er i samsvar med Ateas retningslinjer for personvern. Dette inkluderer: Salgs-/markedsavdelinger, HR, finans/økonomi, konsulenttjenester, AMS, logistikk og IT.

Personvernadministratoren for hver forretningsfunksjon skal rapportere til Chief Information Security Officer i sitt land (eller avdeling for fellestjenester). Chief Information Security Officer har det overordnede ansvaret for å implementere retningslinjer for personvern i sitt land, og skal rapportere til Chief Information Security Officer for konsernet.

Du finner kontaktinformasjon til alle nøkkelmedlemmer av informasjonssikkerhetsorganisasjonen i ditt land på Ateas nettsted for etterlevelse atea.com/trust. Du finner også en oversikt over informasjonssikkerhetsorganisasjonen i vedlegget til dette dokumentet.

Ateas retningslinjer for personvern omfatter:

- Registrering av systemer
- Dataklassifisering
- Håndtering av personopplysninger
- Kundeavtaler

En oversikt over retningslinjer for personvern følger:

Registrering av systemer
Før Ateas ansatte begynner å samle inn, håndtere eller distribuere informasjon, må de forsikre seg om at alle informasjonssystemer som skal lagre eller behandle informasjonen, er registrert og autorisert av Chief Information Security Officer for det aktuelle landet. Dette inkluderer skytjenester det abonneres på, og som administreres utenfor Atea.

Chief Information Security Officer vil gjennomføre en analyse av standardene for IT-sikkerhet og personvern i informasjonssystemet før denne registrerer at systemet er autorisert for bruk i Atea. Analysen skal bygge på en standardisert sjekkliste for IT-sikkerhet og personvern i Atea og skal utarbeides sammen med Chief Information Security Officer i Atea Group.

Chief Information Security Officer vil også vurdere hva slags data som skal lagres i systemet, basert på type og sensitivitet, når denne vurderer om systemet oppfyller Ateas krav til informasjonssikkerhet. Som en del av denne analysen vil Chief Information Security Officer også godkjenne retningslinjer for sletting av personopplysninger i systemet når Atea ikke lenger har bruk for dem (retningslinjer om «dataminimalisering»).

Dersom informasjonssystemet inneholder personopplysninger og administreres eksternt – som et skybasert HR-system – må Atea ha inngått en skriftlig databehandleravtale (DPA) med tjenesteleverandøren for å overholde GDPR. En standardisert DPA for leverandører av skytjenester er tilgjengelig på nettstedet Global Information Security på landets intranett. Chief Information Security Officer i hvert land kan svare på spørsmål om DPA og hjelpe til med å innhente en signert DPA fra tjenesteleverandøren.

Ateas ansatte må ikke lagre eller behandle selskapets data i såkalte skyggesystemer («shadow IT») som ikke er registrert av Chief Information Security Officer i det aktuelle landet. Ateas ansatte må ikke gjøre betydelige endringer i systemer eller prosesser for håndtering av data uten å informere Chief Information Security Officer, slik at man kan gjennomføre en ny evaluering av IT-sikkerheten.

Når et system er autorisert for bruk i Atea, vil det utnevnes en eier av systemet. Systemeieren er ansvarlig for å sikre at systemet blir brukt i samsvar med Ateas retningslinjer for personvern. Systemeieren har et særskilt ansvar for å sikre at

tilgangsrettighetene til informasjonssystemet er behovsprøvd og termineres så snart en bruker ikke lenger har et saklig behov for tilgangen. Systemeieren er også ansvarlig for å sikre at personopplysninger som er laget i systemet, blir slettet når det ikke lenger er bruk for dem, i samsvar med retningslinjene om dataminimering som ble vedtatt da systemet ble godkjent.

Dataklassifisering

Når et system blir autorisert for bruk i Atea, vil typen og sensitiviteten til dataene som lagres i systemet, dokumenteres for å sikre at egnede retningslinjer for personvern blir opprettholdt.

Det er mange situasjoner der Ateas ansatte vil håndtere og distribuere informasjon utenfor et autorisert IT-system. Dette inkluderer informasjon som håndteres på utskrevne dokumenter, via e-postkommunikasjon eller via fildeling (dvs. en Microsoft Word-, Excel- eller PowerPoint-fil).

For å sikre at informasjon som brukes utenfor et autorisert IT-system blir håndtert med en egnet grad av informasjonssikkerhet, må Ateas ansatte konkret merke enhver fil, dokument eller e-post som inneholder sensitive opplysninger, slik at mottakeren er klar over innholdet. En slik merking må skje i samsvar med Ateas standarder for dataklassifisering.

Ateas standarder for dataklassifisering består av fem nivåer, der informasjonen som lagres i e-posten eller filen, rangeres fra minst til mest sensitiv. Klassifiseringsstandardene er bygget direkte inn i Ateas versjoner av Microsoft Outlook og Word/Excel/PowerPoint. Alle ansatte kan automatisk merke en e-post eller fil med korrekt dataklassifisering ved å bruke en knapp på båndet eller topplinjen i disse programmene.

De fem nivåene er som følger:

1. Non-business (ikke arbeidsrelatert): Private e-postmeldinger og dokumenter som ikke har med Atea å gjøre

2. Public (offentlig): Informasjon som har med Atea å gjøre, som kan distribueres til offentligheten

3. Internal (internt): Informasjon som fritt kan distribueres internt i Atea, i andre Atea-enheter, eller til avtalefestede leverandører. Ikke tiltenkt distribusjon utenfor Atea eller til parter man ikke har inngått en avtale med.

4. Confidential (konfidensielt): Informasjon som mottakeren bør holde for seg selv, og som ikke skal deles uten samtykke fra informasjonseieren. Dette inkluderer personopplysninger, som bør merkes separat. Man kan merke personopplysninger ved å bruke en rullegardinmeny under Confidential-knappen.

5. Strictly confidential (strengt konfidensielt): Informasjon som kan få betydelige negative konsekvenser for Atea dersom den videreformidles uten lov. Slik informasjon bør lagres i et kryptert format og må ikke deles uten samtykke fra informasjonseieren. Det inkluderer det følgende:

- Sensitive personopplysninger: I henhold til GDPR må særlige kategorier av personopplysninger behandles med ekstra varsomhet. Dette inkluderer informasjon angående: etnisk opphav, politisk ståsted, livssyn, medlemskap i fagforeninger og genetiske eller biometriske data. Sensitive personopplysninger bør merkes separat. Man kan legge til slik merking ved å bruke en rullegardinmeny under Strictly confidential-knappen.
- Sensitiv forretningsinformasjon: Dette inkluderer forretningsinformasjon som nøkkelkunde- eller leverandøropplysninger, kontrakter og forretningsvilkår. Det inkluderer også informasjon som er underlagt en avtale om taushetsplikt som er inngått med en kunde eller forretningspartner. Endelig kan det inkludere svært sensitive åndsverk som forretningskonsepter og programvare, metoder og verktøy som er utviklet internt.
- Kurssensitiv informasjon: Kurssensitiv informasjon er en bestemt type konfidensiell informasjon som kan påvirke Ateas aksjekurs. Dette inkluderer betydelige økonomiske data som ennå ikke er rapportert, eller status på konfidensielle forhandlinger i forbindelse med en svært stor kundeavtale eller forretningsavtale.

  Group CFO i Atea må umiddelbart varsles om alle ansatte som sitter på kurssensitiv informasjon. Disse ansatte vil bli registrert i Ateas Computershare Insider Management System (CIMS). Du kan lese mer om samsvarsprosedyrer for kurssensitiv informasjon i det etiske regelverket, «Code of Conduct».

Du finner en full beskrivelse av Ateas standarder for dataklassifisering og prosedyrene for merking og kryptering av dokumenter og e-postkommunikasjon på «Information Security» på landets intranett.

Håndtering av personopplysninger

GDPR pålegger Atea visse rettslige forpliktelser ved håndtering av personopplysninger – altså informasjon som kan føres tilbake til en bestemt, identifiserbar person. Disse rettslige forpliktelsene krever at Atea dokumenterer at man har iverksatt tilstrekkelige tekniske og organisasjonsmessige tiltak for å overholde GDPR. Denne prosessdokumentasjonen må gjøres tilgjengelig for offentlige myndigheter på forespørsel.

Før Atea kan samle inn personopplysninger, må forretningsprosessen som personopplysningene skal håndteres med, fullt ut dokumenteres og gjennomgås av Chief Information Security Officer. Personvernombudet for hver funksjon er ansvarlig for å sikre at alle prosesser for håndtering av personopplysninger innenfor sin funksjon er dokumentert og oppdatert i henhold til GDPR.

Dokumentasjonen må vise at Atea har truffet tilstrekkelige tekniske og organisasjonsmessige tiltak for å respektere enkeltpersoners rett til sine egne opplysninger, for å forebygge og minimalisere virkningen av et eventuelt brudd på personvernet og for å opptre forskriftsmessig dersom dette skulle skje. Prosessene for innsamling av personopplysninger må også inkludere en prosedyre for dataminimering, dvs. sletting av personopplysninger når Atea ikke lenger trenger dem.

Ved innsamling av personopplysninger må Atea varsle enkeltpersonen eller innhente samtykke til at vedkommendes personopplysninger blir samlet inn og brukt. Når Atea varsler eller innhenter samtykke fra en person, må man kommunisere følgende informasjon i henhold til GDPR:

1. Hvilke kategorier av personopplysningene som skal samles inn og behandles
2. Hvilke formål og hvilket rettslig grunnlag det er for databehandlingen
3. Hvilke mottakere eller kategorier av mottakere som vil få tilgang til personopplysningene
4. Hvilken tidsperiode dataene skal brukes i, eller hvilke kriterier som bestemmer denne perioden
5. Enkeltpersonens rett til egne personopplysninger – herunder retten til å trekke tilbake et samtykke og retten til innsyn, sletting og retting
6. En enkeltpersons rett til å klage til en tilsynsmyndighet.
7. Hvis aktuelt: Et varsel om at opplysningene vil bli overført til et annet land og en bekreftelse på at enhver behandling av opplysningene i et annet land vil skje i samsvar med bestemmelsene i GDPR om tilstrekkelig grad av personvern
8. Hvis det skal samles inn personopplysninger, må Atea be om og motta eksplisitt samtykke fra vedkommende hvis opplysninger skal behandles.

En standardisert personvernerklæring for innsamling av personopplysninger er tilgjengelig under «Information Security» på landets intranett.

Atea har særlige forpliktelser under GDPR dersom det oppstår et brudd på personvernet. Et brudd på personvernet er en informasjonssikkerhetshendelse som kan føre til at uautoriserte personer får tilgang til opplysninger, eller som fører til ulovlig eller utilsiktet tap av data.

Hvis det oppstår et brudd på personvernet, bør Ateas ansatte straks varsle Chief Information Security Officer i sitt land, eller i sin avdeling for fellestjenester. Chief Information Security Officer vil undersøke bruddet på personvernet sammen med Ateas informasjonssikkerhetsorganisasjon og iverksette nødvendige korrigerende tiltak for å rapportere om og motvirke eventuelle skader som måtte ha oppstått som følge av hendelsen.

I tilfelle det oppstår et brudd på personvernet som kan være til skade for en enkeltperson, må Atea varsle tilsynsmyndigheten (Datatilsynet) i det landet der bruddet fant sted, innen 72 timer etter at man ble klar over hendelsen. Et slikt varsel må beskrive bruddets art, gi en oversikt over de berørte registrerte personene og opptegnelsene, sannsynlige konsekvenser av bruddet og hvilke tiltak som treffes.

De enkeltpersonene hvis personvern er blitt krenket, må også varsles direkte dersom det er stor fare for at hendelsen er til skade for vedkommende. Det kan være nok med en offentlig kunngjøring av forholdet dersom det ikke er mulig å varsle den enkelte.

Kundeavtaler

Atea administrerer datainfrastruktur og applikasjoner for mange kunder, enten på kundens adresse eller fra sine egne datasentre. I slike tilfeller er Atea løpende ansvarlig for behandlingen av kundens data og har en rettslig forpliktelse under GDPR til å sikre egnet beskyttelse av personvernet til de personene hvis opplysninger utgjør en del av kundens data.

For å kunne overholde GDPR må Atea ha inngått en databehandleravtale (DPA) med kunden når selskapet skal håndtere kundens datainfrastruktur og applikasjoner. Databehandleravtalen må dokumentere omfanget, arten og varigheten av de databehandlingsaktivitetene Atea påtar seg på vegne av kunden. Slik dokumentasjon må også inneholde en oversikt over hva slags personopplysninger Atea skal behandle på vegne av kunden, og hvilke kategorier av personer hvis personopplysninger vil bli behandlet.

Databehandleravtalen må inneholde følgende bekreftelse fra Atea i samsvar med GDPR:

1. Atea behandler personopplysninger utelukkende på dokumentert instruks fra kundene sine og vil alltid overholde personvernlovene
2. Ansatte i Atea som behandler personopplysninger for kunden, har påtatt seg taushetsplikt. Atea vil ikke be underleverandører behandle personopplysninger for kunden uten at kunden har godkjent dette.
3. Atea har iverksatt tilstrekkelige tekniske og organisasjonsmessige tiltak for å sikre det sikkerhetsnivået som er avtalt med kunden, og som egner seg for den risikoen dataene utsettes for under behandlingen.
4. Atea har iverksatt tilstrekkelige tiltak for å oppfylle sine rettslige forpliktelser overfor enkeltpersoners rett til å kontrollere behandlingen av sine egne opplysninger, som beskrevet i GDPR.
5. Atea vil gi kunden all informasjon som er nødvendig for å godtgjøre samsvar med personvernforpliktelsene i GDPR, og vil delta i en samsvarskontroll dersom kunden krever det
6. Atea vil informere kunden om ethvert brudd på personvernet uten unødig forsinkelse
7. Atea vil slette eller returnere alle personopplysninger til kunden ved slutten av tjenesteavtalen

Dersom Atea benytter eksterne underleverandører for å oppfylle sine forpliktelser til databehandling overfor kunden (f.eks. skytjenester fra en tredjepart, konsulenter eller infrastrukturleverandører), må Atea inngå en separat databehandleravtale med disse underleverandørene der underleverandørene gir en bekreftelse tilsvarende de skriftlige erklæringene ovenfor.

Atea har en standard databehandleravtale (DPA) som bør brukes for alle kunder og underleverandører. Databehandleravtalen er tilgjengelig på nettstedet «Information Security» på landets intranett. Chief Information Security Officer i hvert land kan svare på spørsmål om DPA og bidra med støtte i prosessen med å etablere DPA fra kunde eller underleverandør.

Dersom det oppstår et brudd på personvernet som berører dataene til en kunde, må Atea varsle kunden umiddelbart etter at man er blitt klar over hendelsen. Atea må så samarbeide med kunden og treffe rimelige tiltak for å sikre at kunden kan oppfylle sine forpliktelser om å rapportere hendelsen i samsvar med GDPR, og iverksette korrigerende tiltak for å motvirke skader som måtte ha oppstått som følge av hendelsen.

Hovedpunkter:

Registrering av systemer
Alle IT-systemer som brukes i Atea, må registreres hos Chief Information Security Officer i det landet eller den forretningsenheten som systemene brukes i. Dette inkluderer skytjenester det abonneres på, og som administreres utenfor Atea.

Chief Information Security Officer vil undersøke IT-systemet for å bekrefte at det oppfyller Ateas IT-sikkerhetsstandarder før systemet godkjennes for bruk. Når et system er registrert, vil det utnevnes en systemeier. Systemeierens rolle er å sikre at systemet blir brukt i samsvar med Ateas retningslinjer for personvern, med særlig vekt på håndtering av tilgangsrettigheter.

Dataklassifisering
For å sikre at informasjon som brukes utenfor et autorisert IT-system blir håndtert med en egnet grad av informasjonssikkerhet, må Ateas ansatte konkret merke enhver fil, dokument eller e-post som inneholder sensitive opplysninger, slik at alle mottakerne forstår dette. Merkingen må skje i samsvar med Ateas standarder for dataklassifisering.

Alle rutiner for håndtering av personopplysninger må dessuten dokumenteres og gjennomgås av Chief Information Security Officer. Alle ledere i Atea får utnevnt et personvernadministrator som er ansvarlig for en bestemt forretningsfunksjon i sitt land (eller sin avdeling for fellestjenester). Personvernombudets rolle er å undersøke at alle forretningsprosesser innenfor sin forretningsfunksjon er i samsvar med Ateas retningslinjer for personvern og med GDPR.

Håndtering av personopplysninger
Ved innsamling av personopplysninger må Atea varsle enkeltpersonen eller innhente samtykke til at vedkommendes personopplysninger blir samlet inn og brukt, i samsvar med GDPR. GDPR har flere krav til hvordan slikt skal varsles (se hovedteksten).

Et brudd på personvernet er en informasjonssikkerhetshendelse som kan føre til at uautoriserte personer får tilgang til opplysninger, eller som fører til ulovlig eller utilsiktet tap av data. Atea har særlige forpliktelser under GDPR dersom det oppstår et brudd på personvernet.

Hvis man mistenker et brudd på personvernet, bør Ateas ansatte straks varsle Chief Information Security Officer i sitt land eller i sin avdeling for fellestjenester. Alternativt kan man sende en e-post til infosec@atea.com, som så vil bli videresendt til Chief Information Security Officer i Atea Group.

Atea må ha inngått en databehandleravtale (DPA) med kunden når selskapet skal håndtere kundens datainfrastruktur og applikasjoner i samsvar med GDPR. Atea må også ha på plass en DPA med leverandører eller underleverandører som behandler data for eller på vegne av Atea. GDPR har flere krav til hva en databehandleravtale skal inneholde (se hovedteksten).

4. IT-INFRASTRUKTURSIKKERHET – OBLIGATORISK PRAKSIS FOR ALLE ANSATTE

Ateas IT-infrastruktur består av all maskinvare, programvare og nettverkskomponenter som brukes i leveringen av forretningssystemer og IT-relaterte prosesser til brukerne. Personvernet i Atea er avhengig av at alle ansatte bruker ressursene i Ateas IT-infrastruktur på en forsvarlig måte.

Følgende retningslinjer gjelder alle ansatte i Atea som bruker Ateas IT-infrastruktur, og gjelder enhetssikkerhet, systemtilgang, fillagring og nettverks-, kommunikasjons- og fysisk sikkerhet. I tillegg plikter ansatte som har ansvar for å administrere Ateas IT-drift, å gjennomgå en egen og mer omfattende opplæring i IT-sikkerhet for sin bestemte funksjon.

Utstyrssikkerhet:
Ateas ansatte må ta visse forholdsregler med arbeidsenhetene sine, f.eks. PC-er, nettbrett og smarttelefoner. Slike enheter er utsatt for tyveri, skadevare og uautorisert bruk. Det bør føres konstant tilsyn med Ateas PC-er, nettbrett og smarttelefoner, og de bør oppbevares på et trygt sted. Når de ikke er i bruk, bør enhetene låses med PIN-kode eller passord eller slås av.

Alle Ateas PC-er, nettbrett og smarttelefoner skal ha installert krypteringsløsninger for å unngå uautorisert tilgang til harddisken. Ateas PC-er med Windows er utstyrt med krypteringsløsningen BitLocker. Apple Mac-maskiner har en innebygd funksjon for å kryptere harddisken som må aktiveres. Alle iPhone- og iPad-enheter har forhåndsinstallert kryptering. Kryptering må aktiveres manuelt på mobiltelefoner og nettbrett med Android. Kryptering bør også aktiveres på flyttbare enheter som minnepinner, som det er lett å miste. Ansatte som trenger hjelp til å kryptere arbeidsenhetene sine, kan kontakte Ateas servicedesk.

Ateas ansatte bør ikke laste ned programvare til PC-ene sine som ikke er kjøpt inn via IT-avdelingen. Ateas IT-avdeling tilbyr et utvalg applikasjoner via Service Market-portalen. Disse applikasjonene oppdateres regelmessig for å ha korrekt sikkerhetsnivå. Hvis en ansatt i Atea har behov for å laste ned ekstern programvare som ikke kommer fra Service Market-portalen, bør vedkommende først få dette godkjent av sjefen sin og av den lokale IT-organisasjonen.

Ateas PC-er leveres med virus- og brannmurprogrammer. Ta kontakt med Ateas servicedesk hvis du har spørsmål om virusbeskyttelsen. Hvis du blir advart om skadevare / ondsinnet programvare, eller hvis datamaskinen oppfører seg unormalt, kan det være et tegn på at den er infisert. Tegn på en infisert PC kan være at skjermbildet fryser, at operasjonene blir svært trege, eller at det settes i gang operasjoner automatisk, for eksempel at det åpner seg nye vinduer eller skjer andre endringer på skjermen.

Hvis du mistenker at PC-en din er infisert, må du avslutte alt arbeid på maskinen og koble fra nettverket. Deretter kontakter du Ateas servicedesk og forteller hvilke symptomer det er på at PC-en er blitt angrepet av skadevare, og hvilke hendelser som kan ha gjort PC-en sårbar for infeksjon.

Alle arbeidsenheter som skal tas ut av bruk, må tømmes for alle data før de sendes til service, gjenvinning eller gjenbruk. Dette må gjøres i tråd med IT-prosedyrene som er tatt i bruk i det enkelte land. Disse prosedyrene er tilgjengelige på nettstedet Information Security på landets intranett.

Systemtilgang:
Ateas ansatte bør bare få tilgang til systemer de trenger i arbeidet. Tilgangsrettigheter til systemer bør sjekkes opp løpende for å sikre at disse retningslinjene blir fulgt, og at tilgangen opphører når det ikke lenger er behov for den. Hvis Atea-ansatte har tilgang til systemer de ikke lenger trenger, bør de straks kontakte systemeieren for å avslutte tilgangsrettighetene.

Når en Atea-ansatt innvilges tilgang til et system, skal brukernavnet og et midlertidig passord sendes ut hver for seg. Det midlertidige passordet må straks endres etter første innlogging, og man bør ikke skrive det ned eller dele det med noen. Ansatte må aldri låne ut tilgangsrettigheter til andre brukere.

Fillagring:
Alle Ateas ansatte er ansvarlige for å sikre at arbeidsfilene deres (f.eks. MS Word-, Excel- og PowerPoint-filer) håndteres på en sikker måte. Alle slags filer bør lagres på Ateas interne felles filservere, på OneDrive-kontoer eller i SharePoint-miljøet. Ingen andre eksterne lagringssteder, verken Dropbox eller Google Drive, skal brukes til å lagre Atea-filer uten uttrykkelig tillatelse fra landets IT-avdeling, ettersom Atea ikke kan garantere sikkerheten på slike lagringssteder. Ateas ansatte bør ikke lagre selskapets informasjon på lokale harddisker, ettersom det ikke blir tatt automatisk sikkerhetskopi av slik informasjon, og de derfor kan gå tapt.

Filene bør merkes i henhold til Ateas dataklassifiseringsstandard (fem nivåer). Filer som er merket strengt konfidensielle, må lagres i et kryptert format. Filer som inneholder personopplysninger, må også merkes og lagres i henhold til GDPR.

Ateas ansatte må være svært forsiktige når de lagrer personopplysninger i datafiler av hensyn til de strenge personvernreglene i GDPR. Ansatte må ikke bruke personopplysninger i datafiler til andre formål enn det som opprinnelig ble definert og kommunisert til vedkommende hvis opplysninger ble samlet inn. De ansatte må begrense deling av filer som inneholder personopplysninger for å unngå brudd på personvernet eller misbruk av opplysningene, og bør slette personopplysningene når det ikke lenger er behov for dem. Dette gjelder alle filer Ateas ansatte oppretter – inklusive MS Word-, Excel- og PowerPoint-filer.

Nettverkssikkerhet:
Det er bare Atea-klienter (datamaskiner som er konfigurert i henhold til Ateas standard) som skal kobles til ATEA-domenet. Mobile Atea-enheter må kobles til Ateas WiFi-nettverk for mobile enheter. Andre datamaskiner og mobile enheter skal kobles til ATEAs trådløse gjestenettverk.

Atea tilbyr ansatte som er borte fra kontoret, å koble seg til det interne nettverket via Cisco VPN eller Citrix. Da får de tilgang til selskapets felles filsystem og felles forretningsapplikasjoner. Tilkoblinger til Cisco VPN krever at datamaskinen tilhører Atea, er medlem av Ateas domene (ONE) og har installert et antivirusprogram.

Ateas ansatte må aldri koble seg til et kundenettverk uten at kunden har gitt tillatelse til det, med mindre det er regulert i en skriftlig avtale med kunden. Kunden bør kontaktes hver gang en Atea-ansatt kobler seg til nettverket deres, og den ansatte må alltid informere kunden om hva denne har brukt nettverket til.

Ateas ansatte må være forsiktige når de bruker offentlige WiFi-nettverk på reiser. Datatrafikken over offentlige nettverk kan bli overvåket. Før en Atea-ansatt bruker et WiFi-nettverk, bør den ansatte forsikre seg om at nettverket er trygt, og at det leveres av en pålitelig leverandør. Hvis det er grunn til å tvile på sikkerheten til et WiFi-nettverk, bør Ateas ansatte i stedet bruke mobilnettverket sitt. Ateas servicedesk kan hjelpe en med å koble PC-en til et mobilt nettverk.

Det forventes at Ateas ansatte bruker internett i det daglige arbeidet. Privat surfing er tillatt, men bør begrenses til nettsteder som egner seg for arbeidsplassen. Det er ikke tillatt å drive med spilling eller gambling, og fildeling og strømming av medier via internett bør begrenses til arbeidsrelatert materiale. Ateas ansatte skal være klar over at Atea analyserer trafikken som går gjennom internett for å avdekke angrep på Atea, og at det da også kan spores opp upassende bruk av internett.

Vær kritisk til det du finner og leser på internett, særlig hvis du omadresseres til en ny side. Du må aldri klikke på linker eller popup-meldinger som virker mistenkelige, siden de kan inneholde skadevare som lastes ned på enheten din uten at du merker det.

Kommunikasjon (e-post / sosiale medier):
E-post er et kritisk kommunikasjonsverktøy for Ateas ansatte. Det er også en stor kilde til sårbarheter, siden det setter angripere i stand til å sende Atea skadevare, svindelforsøk og andre trusler uten at det koster dem mye, og med lav risiko for å bli straffeforfulgt.

En vanlig form for identitetssvindel er såkalt «phishing», der en angriper tar direkte kontakt med en ansatt i Atea direkte via e-post. E-posten ser ut til å komme fra en pålitelig kilde, ofte ved at man bruker en falsk identitet, for eksempel tilhørende en annen medarbeider i Atea, en

forretningsforbindelse eller en leverandør, for eksempel et teknologiselskap eller en bank. E-posten har da til formål å lure den ansatte til å utføre en bestemt oppgave, for eksempel overføre penger, taste inn brukeropplysninger, passord eller annen sensitiv informasjon, eller å klikke på en link eller et vedlegg som automatisk laster ned ondsinnet programvare («skadevare») på brukerens PC eller mobiltelefon.

E-posten, vedlegget eller linken ser gjerne uskyldig ut: For eksempel kan den være skjult som en e-post fra en kollega, et tilbud eller en faktura fra en leverandør eller som en melding fra en nettskykonto, for eksempel OneDrive. Derfor må Ateas ansatte være på vakt for muligheten for svindel i all e-post og annen kommunikasjon, også når kommunikasjonen ser ut til å komme fra en betrodd kilde.

Ateas ansatte bør aldri åpne linker eller vedlegg på enhetene sine hvis de er i tvil om hvorvidt en e-post eller annen kommunikasjon er legitim. Hvis en av Ateas ansatte er usikker på om en e-post er legitim eller har kommet til skade for å svare på et mulig svindelforsøk ved åpne en mistenkelig link, bør vedkommende umiddelbart rapportere saken til Ateas servicedesk.

De ansattes e-postkontoer angripes regelmessig av personer som prøver å skaffe seg tilgang til sensitive forretningsfiler. Derfor bør man ikke bruke e-post som et lagringssted for viktig forretningsinformasjon. Forretningsinformasjon bør lagres eller distribueres via sikre forretningssystemer eller fildelingsløsninger, ikke e-post.

Privat bruk av e-post er tillatt så lenge bruken ikke kommer i konflikt med Ateas forretningsinteresser eller forstyrrer arbeidstiden. Privat e-postkorrespondanse bør egne seg for arbeidsplassen og bør merkes non-business / ikke arbeidsrelatert. Dessuten bør bruk av selskapets e-postkonto til personlig kommunikasjon ikke etterlate et inntrykk av at korrespondansen skjer på vegne av Atea eller er godkjent av Atea.

Sosiale medier er også et hyppig brukt kommunikasjonsverktøy blant Ateas ansatte. Når de brukes på en passende måte, kan sosiale medier gjøre det mulig for Ateas ansatte å innhente og overføre kunnskaper, bygge opp forretningsrelasjoner og styrke Ateas varemerke. På den annen side kan sosiale medier skade Atea og Ateas ansatte hvis de brukes på feil måte, eller hvis man deler sensitive opplysninger.

Ateas ansatte bør derfor være svært forsiktige med informasjon de deler på sosiale medier. Personopplysninger (herunder navn, fotografier osv.) kan bare deles i innlegg på sosiale medier som er tilknyttet Ateas virksomhet, dersom den berørte personen gir samtykke til at de blir brukt.

Sikkerhet på kontoret:

Ateas ansatte skal bruke adgangskort for å identifisere seg på arbeidsplassen. Alle besøkende må registrere seg og utstyres med et ID-kort for besøkende som de må bære synlig på seg. Besøkende bør tas imot ved resepsjonen idet de ankommer, og følges tilbake til resepsjonen for å levere tilbake ID-kortet når besøket er over. Ingen besøkende må overlates til seg selv inne i Ateas lokaler.

All sensitiv informasjon må fjernes fra skrivebord og oppbevares på en trygg måte når den ikke er i bruk. Man bør viske bort all informasjon fra tavler ved slutten av et møte. Konfidensielle dokumenter bør alltid makuleres eller kastes i sikrede avfallsbeholdere når det ikke lenger er bruk for dem.

Hovedpunkter – IT-infrastruktursikkerhet

Enhetssikkerhet:
Alle Ateas PC-er, nettbrett og smarttelefoner bør ha installert krypteringsløsninger for å unngå uautorisert tilgang til harddisken. Det bør føres konstant tilsyn med Ateas PC-er, nettbrett og smarttelefoner, og de bør oppbevares på et trygt sted. Når de ikke er i bruk, skal enhetene låses med PIN-kode eller passord eller slås av.

Ateas ansatte må ikke laste ned programvare til PC-ene sine som ikke er kjøpt inn via IT-avdelingen. Hvis en ansatt i Atea har behov for å laste ned ekstern programvare som ikke kommer fra Atea, bør vedkommende først få dette godkjent av sjefen sin og av den lokale IT-organisasjonen.

Ateas PC-er leveres med virus- og brannmurprogrammer. Ta kontakt med Ateas servicedesk hvis du har spørsmål om virusbeskyttelsen.

Hvis du mistenker at PC-en din er kompromittert eller infisert av ondsinnet programvare, må du avslutte alt arbeid på maskinen og koble fra nettverket. Deretter kontakter du Ateas servicedesk.

Systemtilgang:
Ateas ansatte bør bare få tilgang til systemer de trenger i arbeidet. Tilgangsrettigheter til systemer bør sjekkes opp løpende for å sikre at disse retningslinjene blir fulgt, og at tilgangen opphører når det ikke lenger er behov for den.

Fillagring:
Alle Ateas ansatte er ansvarlige for å sikre at arbeidsfilene deres (f.eks. MS Word-, Excel- og PowerPoint-filer) håndteres på en sikker måte. Filer bør merkes i henhold til Ateas dataklassifiseringsstandard (fem nivåer), og filer som inneholder personopplysninger, skal merkes separat. Filer som er merket strengt konfidensielle, må lagres i et kryptert format.

Alle slags filer bør lagres på Ateas interne felles filservere, på OneDrive-kontoer eller i SharePoint-miljøet. Ingen andre eksterne lagringssteder, verken Dropbox eller Google Drive, skal brukes til å lagre Atea-filer uten uttrykkelig tillatelse fra landets IT-avdeling. Ateas ansatte bør ikke lagre selskapets informasjon på lokale harddisker.

Nettverkssikkerhet:
Det er bare Atea-klienter (datamaskiner som er konfigurert i henhold til Ateas standard) som skal kobles til ATEA-domenet. Mobile Atea-enheter må kobles til Ateas WiFi-nettverk for mobile enheter. Andre datamaskiner og mobile enheter skal kobles til ATEAs trådløse gjeste-nettverk.

Ateas ansatte må være forsiktige når de bruker offentlige WiFi-nettverk. Før en Atea-ansatt bruker et WiFi-nettverk, bør denne forsikre seg om at nettverket er trygt, og at det leveres av en pålitelig leverandør.

Bruk av internett på en arbeidsenhet bør begrenses til nettsteder som egner seg for arbeidsplassen. Ateas ansatte skal være klar over at Atea analyserer trafikken som går gjennom internett for å avdekke angrep på Atea, og at det da også kan spores opp upassende bruk av internett.

Vær kritisk til det du finner og leser på nettsteder, særlig hvis du omadresseres til en ny side. Du må aldri klikke på linker eller popup-meldinger som virker mistenkelige, siden de kan inneholde skadevare som lastes ned på enheten din uten at du merker det.

Kommunikasjon (e-post / sosiale medier):
E-post er også en stor kilde til sårbarheter, siden det setter angripere i stand til å sende Atea skadevare, svindelforsøk og andre trusler uten at det koster dem mye, og med lav risiko for å bli straffeforfulgt.

En vanlig form for identitetssvindel er såkalt «phishing», der en angriper tar direkte kontakt med en ansatt i Atea direkte via e-post. E-posten ser ut til å komme fra en pålitelig kilde, ofte ved at man bruker en falsk identitet, for eksempel tilhørende en annen medarbeider i Atea, en forretningsforbindelse eller en leverandør, for eksempel et teknologiselskap eller en bank. E-posten har da til formål å lure den ansatte til å utføre en bestemt oppgave, for eksempel overføre penger, taste inn brukeropplysninger, passord eller annen sensitiv informasjon, eller å klikke på en link eller et vedlegg som automatisk laster ned ondsinnet programvare («skadevare») på brukerens PC eller mobiltelefon.

Ateas ansatte bør aldri åpne linker eller vedlegg på enhetene sine hvis de er i tvil om hvorvidt en e-post eller annen kommunikasjon er legitim. Hvis en av Ateas ansatte er usikker på om en e-post er legitim eller har kommet til skade for å svare på et mulig svindelforsøk ved åpne en mistenkelig link, bør vedkommende umiddelbart rapportere saken til Ateas servicedesk.

Privat bruk av e-post er tillatt så lenge bruken ikke kommer i konflikt med Ateas forretningsinteresser eller forstyrrer arbeidstiden. Privat e-postkorrespondanse bør egne seg for arbeidsplassen og bør merkes non-business / ikke arbeidsrelatert.

Ateas ansatte bør være svært forsiktige med informasjon om Atea som de deler på sosiale medier. Personopplysninger (herunder navn, fotografier osv.) kan bare deles i innlegg på sosiale medier som er tilknyttet Atea, dersom den berørte personen gir samtykke til at de blir brukt.

Sikkerhet på kontoret:
Ateas ansatte skal bruke adgangskort for å identifisere seg på arbeidsplassen. Alle besøkende må registrere seg og utstyres med et ID-kort for besøkende som de må bære synlig på seg.

All sensitiv informasjon må fjernes fra skrivebord og oppbevares på en trygg måte når den ikke er i bruk.

Holding
Atea ASA
Atea ASA
Brynsalleen 2
Postboks 6472 Etterstad
N-0605 Oslo
+47 22 09 50 00
Org.nr. 920 237 126
investor@atea.com
atea.com

Norge
Atea AS
Brynsalleen 2
Postboks 6472 Etterstad
N-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 Vantaa
+ 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

Group Logistics
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

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

ATEA