AcadeMedia

Informationssäkerhetspolicy

Dokumentägare: IT-chef
Skapad: 2018-03-21
Reviderad: 2019-01-11

AcadeMedias verksamhet innefattar daglig hantering av stora informationsmängder. Då vi behandlar både känslig information om individer och information som kan påverka vår börskurs, krävs en säker och genomtänkt hantering.

Ansvaret för en bra informationssäkerhet vilar på oss alla inom AcadeMedia, både anställda och övriga sysselsatta (såsom konsulter). Denna policy beskriver hur vi ska agera och vilka generella krav som AcadeMedias ledning och styrelse ställer på samtliga verksamheter inom koncernen**.**

Mål och säkerhetsaspekter

Målet för AcadeMedias informationssäkerhetsarbete är att skydda den information som finns inom verksamheten i syfte att den endast kan användas för det tänkta användningsområdet. Skyddet ska vara anpassat till behoven med avseende på typ, känslighet, risk, lagkrav och andra styrande regelverk eller dokument för våra verksamheter.

Informationssäkerhet inom AcadeMedia utgår från fyra aspekter:

Konfidentialitet: Endast den som för sitt arbete behöver och därför tilldelats behörighet till viss information ska få tillgång till den och ingen annan.

Riktighet: Information ska inte förändras genom misstag, obehörig tillgång eller tekniska fel.

Tillgänglighet: Information ska kunna nås och användas av de som är behöriga inom önskad tid och från rätt plats.

Spårbarhet: Bearbetning av och åtkomst till väsentlig information ska kunna spåras.

Samtidigt är transparens ett ledord i AcadeMedias kommunikationspolicy. Det gäller därför att noga avgöra om information är konfidentiell eller känslig ur något perspektiv, om det inte är så ska vi eftersträva att vara så transparenta som möjligt.

Övergripande roller och ansvar

Samtliga medarbetare, och andra sysselsatta i AcadeMedias verksamheter, har ansvar för att hantera information korrekt. Ytterst vilar ansvaret på den som är informationsägare, tvärs hela koncernen. Ansvaret kan delas upp och delegeras vid behov. De huvudsakliga konfidentiella och känsliga informationsområden som AcadeMedia hanterar listas nedan med sina respektive informationsägare:

- Personuppgifter om barn, elever, vårdnadshavare, deltagare, kunder och samarbetspartners – ansvarig chef för enhet/verksamhet/avtal.

- Verksamhetens tillståndspliktiga huvudman/styrelse. Generell delegation till rektor för vår skolverksamhet, till verksamhetschef för vuxenverksamheten och förskolechef inom förskolorna.
- Personuppgifter om anställda, såsom löneuppgifter, behörighetsinformation, ledarprofil, NMI och övriga personalnyckeltal – HR-direktör och respektive chef.
- Ekonomisk information – CFO.
- Kommersiella anbud och konfidentiella avtal – undertecknande/ansvarig chef.
- Tillsynslogg samt anmälningar till tillsynsmyndigheter – respektive segmentschef.
- Juridisk information samt riskrapportering – koncernens chefsjurist.

En stor del av vår information lagras i för ändamålet avsedda IT-system för vilka det ofta finns en utsedd systemägare. (För en översikt av AcadeMedias IT-system se bilaga 1, *AcadeMedias IT-system – översikt.* Varje systemägare är ansvarig för säkerheten för den information som lagras inom respektive system. Detta ansvar kan vid behov delegeras inom AcadeMedias verksamheter. Systemägaren ska rapportera risker och dess hantering samt incidenter till ovan beskrivna informationsägare (som bär det övergripande ansvaret för informationssäkerheten inom sitt informationsområde) med kopia till chefen för IT-funktionen på koncernnivå.

Chefen för IT-funktionen på koncernnivå är ansvarig för koncernens samlade informationssäkerhet. I detta ingår att säkerställa att koncernens tekniska infrastruktur möjliggör och har en tillförlitlig och säker informationshantering. I ansvaret ingår löpande uppföljning och efterlevnad av policyn med avseende på systems användning och säkerhetsmässiga funktion. Chefen för IT-funktionen på koncernnivå ansvarar även för att säkerställa att verksamhetskritiska system har en utsedd systemägare som förstår sitt ansvar. En förteckning över verksamhetskritiska IT-system och dess systemägare visas i bilaga 2, *Förteckning över verksamhetskritiska IT-system*. Varje landschef (eller motsvarande) har i ansvar att ge chefen för IT-funktionen på koncernnivå underlag för utvärdering av verksamhetskritiska system inom respektive land.

Riskbedömning och riskhantering

Det åvilar respektive informationsägare och systemägare att regelbundet genomföra riskbedömningar och hantera de informationsrisker som identifieras. I de fall man upptäcker brister eller risker avseende informationssäkerhet ska överordnad funktion/ansvarig och chefen för IT-funktionen på koncernnivå omgående informeras på ett tydligt sätt och åtgärder vidtas.

Informationssystem (IT)

Mycket av verksamhetens information finns i digitala system och arkiv. Det är därför viktigt att processer runt tillgång och behörigheter är väl definierade. Även informationssäkerhet i form av backuper och kontinuitetsplaner är väsentligt.

Tillgång: tillgången till IT-baserade system sker via användarkonton. Konton ska vara personliga vid hantering av väsentlig information för att möjliggöra spårbarhet. Konton ska endast skapas efter beställning och godkännande av behörig beställare. Varje system- och informationsägare ska säkerställa att säkerhetsnivån för inloggning (autentisering) motsvarar känsligheten i den information som lagras i respektive system.

Varje chef är personligen ansvarig att säkerställa att konton beställs, uppdateras och avbeställs för medarbetare när dessa börjar, byter eller avslutar sin anställning.

Säkerhetskrav på lösenord bör följa best practice.

Behörigheter: behörigheter till olika funktioner och information ska endast ges till dem som behöver detta i sitt arbete och kan ges efter beställning och godkännande av respektive informationsägare eller på dennes delegation. Behörighet till centrala ekonomi-, faktura- och personalsystem ska tilldelas enligt fastslagen rutin och ska följa gällande attestnivåer.

Samtliga ärenden rörande tillgång och behörigheter ska vara spårbara och dokumenteras i ärendehanteringssystem. Varje informationsägare och systemägare ska säkerställa att det minst en gång per år görs en översyn av behörigheterna i respektive system.

Antalet personer med höga behörigheter (så kallade fulla administratörsrättigheter) ska begränsas så långt det går. Höga behörigheter får endast användas för att fullgöra nödvändiga arbetsuppgifter kopplade till ärenden och problem.

Lagring: Det åligger respektive systemägare att säkerställa att information säkerhetskopieras och arkiveras enligt god praxis samt gällande lagar och regler. För de system som driftas i AcadeMedias egna centrala miljö, är det den tekniske systemägaren som ansvarar för att följa upp och vid behov kravställa säkerhetskopiering av systemet. Systemägare ska rapportera om det finns eventuella brister eller risker kring detta till respektive informationsägare samt chefen för IT-funktionen på koncernnivå.

Kontinuitetsplanering: För all verksamhetskritisk information ansvarar informationsägaren för att det finns en kontinuitetsplan som motsvarar behoven vid allvarligare haverier eller driftstopp. För varje verksamhetskritiskt system ska systemägaren säkerställa att motsvarande kontinuitetsplan finns och till informationsägaren rapportera eventuella brister eller risker.

Personligt ansvar för informationssäkerhet

Utgångspunkten är att varje individ är ansvarig för att hålla sina lösenord och IT-utrustning säker. Bilaga 3, *Policy för användning av digitala verktyg* beskriver vad som gäller för alla medarbetare eller konsulter i den svenska verksamheten. Motsvarande policy ska finnas för övriga länder.

Just lösenord är en viktig del av vår digitala säkerhet och ska aldrig lämnas ut till annan person. Lösenord som används till AcadeMedias system får inte användas i något annat system eller tjänst då det kraftigt ökar risken för intrång. Om vi lämnar dator/platta/telefon utan övervakning ska den låsas eller stängas av så att obehörig åtkomst förhindras.

Förlust av utrustning eller misstanke om obehörigt användande av lösenord eller annan åtkomst ska anmälas direkt till AcadeMedia IT.

Vissa medarbetare har tillgång till extra känslig information som kan påverka börskurs och omfattas därför av särskilda skyddsåtgärder. Dessa medarbetare ska intyga och följa de riktlinjer som finns i bilaga 4 , *Riktlinje för skydd av mobila enheter för individer med högsta säkerhetsklassing*. Utgångspunkten är att detta gäller samtliga i koncernledning, koncerncontrolling, investor relations och medarbetare på insynslista. Därutöver omfattas vissa medarbetare inom bland annat koncernekonomi och AcadeMedia IT. Vilka som ska omfattas av detta avgörs vid varje tillfälle av koncernens CFO.

Informationsklassificering och utskrifter

I samband med hantering av projekt med kurspåverkande information, som exempelvis förvärv, ska rutiner gällande loggbok och sekretessförbindelser följas. Se vidare i Insiderpolicyn. Utskrifter inom

AcadeMedias olika huvudkontor kräver personlig inloggning med egen säkerhetsbricka. Motsvarande säkerhetsfunktion kan fås efter beställning inom alla svenska verksamheter.

Känsliga personuppgifter

Känsliga personuppgifter (exempelvis information om hälsa eller facklig tillhörighet) eller personuppgifter som kan uppfattas som integritetskänsliga (exempelvis löneuppgifter, barns utveckling eller pedagogiska utredningar) ska alltid hanteras med extra varsamhet och i system/lösningar anpassade till detta. Inloggning till dessa system/lösningar ska i normalfallet ske med säker inloggning (tvåfaktorsinloggning). Koncernens dataskyddspolicy beskriver hantering av personuppgifter i mer detalj.

Varje vårdgivare inom AcadeMedia ska ha ett väldokumenterat ledningssystem som tydligt anger ansvaret för medicinska och psykologiska insatserna samt innehåller en Informationssäkerhetspolicy. Informationssäkerhetspolicyn ska stämmas av med chefen för IT-funktionen på koncernnivå och efterlevnaden ska regelbundet följas upp av ansvarig inom verksamheten. Som exempel på sådan policy finns bilaga 5, *Informationssäkerhetspolicy för elevhälsans medicinska insats - AcadeMedias gymnasiesegment.*

Finansiell information

AcadeMedias centrala ekonomisystem innehåller både väsentlig och känslig information om koncernens verksamhet. Systemen omfattas därför av höga krav på behörighetshantering och åtkomst. Åtkomst kräver att man är uppkopplad via AcadeMedias nätverk eller via VPN (Virtual Private Network) för åtkomst.

Finansiell information av känslig eller väsentlig natur får endast sändas med e-post som krypterad bilaga där nyckeln lämnas ut på annat sätt än epost (ex SMS). Personer som löpande arbetar med sådan känslig finansiell information ska ha datorer och telefoner utrustade med krypterad lagring samt iaktta extra vaksamhet med sina digitala arbetsredskap. Allt styrelsematerial distribueras via en säker styrelseportal (Directors Desk) där också särskilt känslig information kan kräva lösenord eller förhindras att printa.

Fysiskt arbetsmaterial med väsentlig information hanteras genom att personer i insynsställning ska låsa in sådana utskrifter och att deras arbetsplatser ska förses med lås på dörrar.

IT-infrastruktursäkerhet

Ytterst ansvarig för IT-säkerheten är chefen för IT-funktionen på koncernnivå. I ansvaret ingår säkerhet i form av relevanta brandväggar som skydd mot intrång och grundläggande skydd för information som lagras i system inom AcadeMedias centrala driftsmiljö. Det ingår även i ansvaret att säkerställa att leverantörer av centralt upphandlade IT-tjänster svarar upp mot koncernens krav på informationssäkerhet avseende både data och fysisk säkerhet (skydd av datahallar).

AcadeMedia IT har ett ansvar att säkerställa att de kommunikationslösningar som används inom koncernen uppfyller en marknadsmässig nivå vad avser kommunikationssäkerhet och tillgänglighet. AcadeMedia IT har möjlighet att styra åtkomst och behörigheter till kommunikationsnät i syfte att skydda verksamheten. AcadeMedia IT har även mandat att vid behov begränsa åtkomst både på individ- och gruppnivå till alla IT-system och infrastruktur, exempelvis vid yttre angrepp (exempelvis attacker och virus).

AcadeMedia

Övervakning och loggar

Systemägare ansvarar för kravställande av övervaknings- och loggningsfunktioner för respektive system utifrån aktuell behovsbild.

Vid inhämtning av information av utredningskaraktär ska rutinen för digitala efterforskningar följas, alltså bilaga 7, *Rutin för digitala efterforskningar*. Varje land har i ansvar att upprätta motsvarande dokument efter avstämning med trygghetsdirektör eller chefsjurist.

Hantering av informationssäkerhetsincidenter

Respektive informationsägare och systemägare är ansvarig för att hantera och följa upp eventuella säkerhetsincidenter och åtgärda dessa skyndsamt samt vidta åtgärder för att minska dess konsekvenser.

I de fall då verksamheter eller personer kan påverkas ska relevant ansvarig involveras från berörd verksamhet. Är incidenten av polisiär eller annan allvarlig natur ska person i segments- eller koncernledning involveras. Chefen för IT-funktionen på koncernnivå ska alltid informeras vid incidenter som inte är av trivial karaktär. I det fall en incident gäller integritetskänsliga eller känsliga personuppgifter ska dessutom verksamhetens dataskyddsombud meddelas skyndsamt, vartefter hen beslutar om rapportering till Datainspektionen ska göras.

Om en incident riskerar att påverka AcadeMedias verksamhet (helt eller i delar) på ett affärsmässigt sätt ska respektive verksamhets krisledning alternativt koncernens krisledning involveras. Om informationssäkerhetsincidenten är av sådan karaktär att kurspåverkande information kan ha spridits eller riskerar att spridas ska CFO och IR-ansvarig informeras omgående.

Uppföljning och revision

I samband med den årliga revisionen granskas även IT-området och uppföljning av informationssäkerheten sker via genomgångar med berörda, samt genom uppföljning av specifika ärenden.

Bilagor

- **Bilaga 1 – Översikt av AcadeMedias IT-system**
- **Bilaga 2 – Förteckning över verksamhetskritiska IT-system med systemägare**
- **Bilaga 3 – Policy för användning av digitala verktyg (AcadeMedia Sverige)**
- **Bilaga 4 – Säkerhetsrutin mobila enheter**
- **Bilaga 5 – Informationssäkerhetspolicy för elevhälsans medicinska insats - AcadeMedias gymnasiesegment**
- **Bilaga 6 – Informationssäkerhetspolicy för elevhälsans medicinska och psykologiska insats - för- och grundskoloesegmentet**
- **Bilaga 7 – Digitala efterforskningar**