Retningslinje for tilgangsstyring i Agder fylkeskommune

Versjon/dato: 1.0, 07.03.2024	**Godkjent/vedtatt av:** Sikkerhets- og beredskapsleder
Dokumentnummer: 24/09048-1	**Beskrivelse:** Retningslinja er en del av styringssystemet for informasjonssikkerhet og personvern. Den gir føringer for å styre tilganger til fylkeskommunens informasjonssystemer på en sikker og kontrollert måte.
Neste versjon: Fortløpende etter behov	**Ansvar for revisjon:** Informasjonssikkerhetsrådgiver
Første gang vedtatt: 07.03.2024	**Gjelder for:** Alle informasjonssystemer i Agder fylkeskommune

Innledning

Denne retningslinja definerer rammer og prinsipper for å styre tilganger til fylkeskommunens nettverk, IT-utstyr, IT-systemer og informasjonsverdier på en sikker og kontrollert måte.

Formålet er å

- sikre autorisert tilgang til informasjon
- forhindre uautorisert tilgang, endring, ødeleggelse eller manipulering av informasjon
- sikre at tilgang til informasjon begrenses til et minimum og er nødvendig etter behov
- sikre at tilgangsstyringen er proporsjonal med informasjonsverdiene

Dette vil gi lavere risiko for uautorisert tilgang til informasjon.

Ansvar

Tjenesteeier / systemeier er ansvarlig for at denne retningslinjen blir fulgt for sine informasjonssystemer, informasjonsverdier og IT-utstyr.

Systemansvarlige er ansvarlige for å opprette, gjennomgå og avslutte tilganger i egne systemer.

Tjenesteleverandør på fylkeskommunens sentrale identitetskatalog har det praktiske ansvaret for livsløpet i den sentrale identitetsforvaltningen (Active Directory).

Sikkerhets- og beredskapsleder er ansvarlig for å følge opp tjenesteleverandør på den sentrale identitetskatalogen i tråd med retningslinje for informasjonssikkerhet i leverandørforhold.

Tilgang til informasjon og informasjonssystemer

Alle informasjonssystemer skal følge disse grunnleggende prinsippene:

- Alle informasjonssystemer skal ha systemeiere som klassifiserer informasjonen i systemene og definerer korrekte tilgangsnivåer. Klassifisering skal gjennomføres i henhold til retningslinje for klassifisering og verdivurdering av informasjon.
- Tilganger skal baseres på tjenstlig behov.
- Tilganger skal baseres på så lave rettigheter som nødvendig.
- Tilganger skal baseres på rollestyring (Role Based Access Control - RBAC).
- Tilganger skal gjennomgås jevnlig av systemeier.
- Tilgang til informasjon med middels og høyere beskyttelsesbehov skal alltid skje med en brukerkonto som er knyttet til en medarbeider eller innleid ressurs.
- Føderering av brukerkontoer bør brukes der det er mulig.

Oppretting og sletting av brukerkontoer

Alle brukerkontoer har en livssyklus, fra de blir opprettet, endret, og til slutt slettet. Tilgangsstyring skal sikre at brukernes tilganger til enhver tid er korrekt og oppdatert.

- Bestilling av tilganger skal skje gjennom «Brukertilgang» (https://brukertilgang.ikt-agder.no/) , eller «Roller og tilganger» via «Internhjelpen» på intranettet, eventuelt direkte til systemeier. Ingen leder eller medarbeider skal kunne godkjenne tilganger for seg selv.
- Når behov for tilgang ikke lengre er til stede, så skal tilgang straks opphøre.
- Systemeiere skal sikre en rutine for jevnlig gjennomgang av tilganger i egne informasjonssystemer.
- Alle privilegerte tilganger som gir brukeren mulighet til å overstyre systemkontroller skal kontrolleres særskilt.
- Oppretting og sletting av brukerkontoer bør automatiseres basert på en relevant kilde (for eksempel HR-systemet).

Privilegerte brukerkontoer

Privilegerte kontoer (administratorkontoer) har mange rettigheter, og derfor er de attraktive for trusselaktører. Det er derfor viktig at antall privilegerte kontoer begrenses, og at de enkelte privilegerte kontoene ikke har mer rettigheter enn nødvendig.

- Privilegerte brukerkontoer skal ikke ha høyere privilegier enn det som er nødvendig for å utføre relevante administrative oppgaver.
- Ingen brukere skal kunne logge inn som privilegerte brukere på egne datamaskiner.
- Tilgang til privilegerte kontoer bør være tidsavgrenset.

Sikker autentisering

Sikker autentisering handler om å verifisere identiteten til brukere eller systemer. Det gjøres med forskjellige autentiseringsmetoder (for eksempel bruk av passord, koder eller biometri). Svak autentisering bruker bare én metode, mens sterk autentisering bruker flere metoder. Sikker autentisering bidrar til å forhindre uautorisert tilgang til informasjon.

- Autentiseringsstyrken skal ta utgangspunkt i informasjonens klassifiserings-nivå. Tilgang til informasjon med høgt beskyttelsesnivå krever for eksempel sterk autentisering.
- Påloggінger skal ikke lekke informasjon om allerede opprettede brukere (for eksempel at en brukerkonto eller e-postadresse allerede er registrert).
- Det skal kontrolleres om pålogging er gyldig og inndata skal kontrolleres.
- Ved gjentatte feile påloggінger, så skal brukerkonto sperres, eventuelt skal autentiseringsstyrken økes.

Overvåking av systemtilganger og bruk

All bruk av brukerkontoer må overvåkes og logges.

- Tilganger i informasjonssystemer skal overvåkes for å avdekke avvik fra denne retningslinja.
- Det skal være mulig å spore uautoriserte forsøk på bruk av systemer, i tillegg til normal bruk av systemene, for å sikre bevis i forbindelse med sikkerhetsbrudd. Slik sporing skal gjennomføres i tråd med retningslinje for logging.

Relaterte retningslinjer

- Tildeling av ansvar for sikkerhet og personvern i Agder fylkeskommune
- Rollebeskrivelse tjeneste, systemeier og systemansvarlig
- Retningslinje for autentiseringsinformasjon (passordpolicy).
- Retningslinje for klassifisering og verdivurdering av informasjon.
- Retningslinje for logging.

Referanser

- ISO 27002:2022 5.1 «Policyer for informasjonssikkerhet»
- ISO 27002:2022 5.15 «Tilgangskontroll»
- ISO 27002:2022 5.16 «Identitetshåndtering»
- ISO 27002:2022 5.18 «Tilgangsrettigheter»
- ISO 27002:2022 8.2 «Privilegerte tilgangsrettigheter»
- ISO 27002:2022 8.3 «Begrensninger på informasjonstilgang»
- ISO 27002:2022 8.5 «Sikker autentisering»