

IT-instruks for NRK

Publisert 30.11.2017 av Infotjenester AS
Sist endret 30.11.2017 av Infotjenester AS
#27

Personalhåndbok/ Generelle retningslinjer/ IT-instruks for NRK

IT-instruks for NRK.

Enhver som jobber i eller for NRK har et selvstendig ansvar for å medvirke til at informasjon som NRK eier eller har ansvar for, beskyttes og ikke kommer på avveie, uavhengig av hvor informasjonen befinner seg. Dette betyr at når du behandler informasjon skal du vise aktsomhet.

IT-instruksen er utarbeidet som hjelp for den enkelte i dette arbeidet.

1. Definisjoner

Med informasjon menes for eksempel upublisert materiale, publisert materiale, kildeopplysninger, personopplysninger, forretningssensitiv informasjon, kontrakter, konkurransevridene informasjon, kode, systemdokumentasjon, etc. i form av tekst, bilder, video eller lyd.

Informasjonssikkerhet handler om å sikre at informasjonen:

- ikke blir kjent for uvedkommende (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkommende (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

2. Brukerkontoer og passord

Personlige brukerkontoer skal ikke lånes bort, passord skal holdes hemmelig og ikke gjenbrukes andre steder.

Brukernavn og passord på brukerkontoer og felleskontoer skal følge retningslinjer i passordpolicyen.

To-faktor pålogging skal aktiveres, der dette er mulig, på alle NRK-tilknyttede kontoer.

Din nrk.no e-postadresse skal kun brukes på jobbrelaterte nettkontoer.

Det skal ikke være tvil om at du uttaler deg som privatperson eller som NRK-ansatt i sosiale medier.

3. Bruk av sosiale medier

Tjenestlige behov styrer hvilken informasjon du har tilgang til, og du har plikt til å si fra om du oppdager at du har tilganger du ikke trenger.

Informasjon du har tjenstlig tilgang til skal kun brukes til NRK-formål og taushetsplikten gjelder som beskrevet i arbeidskontrakten din.

4. Fysisk utstyr

Utstyr eid av andre enn NRK, skal ikke koples til NRKs nettverk uten etter særskilt avtale med Servicetorget 2300. Dine besøkende skal benytte NRKs trådløse gjestenettverk. Du finner informasjon i Portalen om passord til gjestenettet.

Fysisk utstyr skal ikke forlates ulåst.

Løse lagringsmedium (minnepinner, løse harddisker, etc) som du ikke kjenner innholdet på, skal ikke kobles til NRK-utstyr.

Det gjelder egne regler for fysisk utstyr på reise i land der NRK-ansatte kan være et etterretningsmål.

5.Lagring og deling

Lagring av informasjon skal skje på NRK-godkjente lagringsløsninger. Du har plikt til å vurdere om informasjonen du har krever ekstra høy beskyttelse når den deles eller lagres.

Jobbrelatert e-post skal sendes til og fra din nrk.no-adresse.

Velg fortrinnsvis å sende lenke til et dokument i Office 365, fremfor å sende dokumentet som vedlegg.

Du kan ikke distribuere NRK-innhold eller rettighetsbelagt materiale som NRK ikke har tilgjengeliggjort for deling.

Vær kritisk til lenker og vedlegg i e-post. Tenk alltid før du klikker! Vær kritisk til hvilke apper som får tilgang til din kontaktliste og dine bilder.

Filmer, bilder og spill som ikke kan knyttes til din jobb i NRK, skal ikke lagres på NRKs lagringsløsninger. Det er ikke tillatt å bruke NRKs utstyr til kryptomining, dataspill eller tilsvarende. NRK-utstyr skal ikke benyttes til å bruke, oppbevare eller dele materiale i strid med norsk lov, ei heller pornografisk innhold eller spredning av politisk, rasistisk eller religiøs propaganda.

6.Innsyn

"Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale" regulerer arbeidsgivers rett til innsyn i opplysningene lagret i e-postkasse, i personlige områder i virksomhetens datanettverk eller annet elektronisk utstyr, som arbeidsgiver har stilt til arbeidstakers disposisjon til bruk i arbeidet, slik som PC, mobil eller nettbrett.

Innsyn praktiseres i tråd med prosedyrer beskrevet i nevnte forskrift.

7. Unntak

Redaksjonell virksomhet vil unntaksvis ha behov for avvik fra IT-instruksen. Alle avvik meldes Servicetorget 2300, og alle avvik loggføres.

8. Brudd på IT-instruksen

Brudd på IT-instruksen kan føre til at din brukertilgang blir sperret. Hovedregel er at brukere skal informeres om sperring. Nærmeste leder får alltid informasjon om sperring og årsak til dette.

Brudd på instruksjonen kan få følger for ditt ansettelsesforhold med NRK.

9. Slik melder du fra

Har du mistanke om at en brukerkonto eller NRKs systemer er kompromittert, ta straks kontakt med Servicetorget 2300.

Tap av fysisk utstyr skal raskest mulig meldes til Servicetorget 2300 og til din leder.

Utstyr du ikke lenger bruker, skal returneres i henhold til beskrivelser publisert i Portalen.

Det kan oppstå behov eller situasjon som ikke er nevnt i dette dokumentet, men som likevel sorterer under definisjonen av informasjon og de generelle kravene til informasjonssikkerhet overnfor. Innspill til neste revisjon av IT-instruksjonen kan sendes til sikkerhet@nrk.no.

10. Fakta om IT-instruksen

IT-instruksjonen inngår i NRKs personalhåndbok og eies av ODIV.

Informasjonssikkerhetsansvarlig i NRK er faglig ansvarlig for instruksjonen.

Forskrift om arbeidsgivers innsyn i e-postkasse mv sier

Arbeidsgiver kan i visse situasjoner åpne og lese e-post i arbeidstakers e-postkasse. Reglene om dette er tatt inn i [forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale](#).

Vilkårene for å gjennomføre slikt innsyn er at:

- Det er nødvendig for å ivareta
 - den daglige driften av virksomheten, eller
 - andre berettigede interesser ved virksomheten
- Det er begrunnet mistanke om at arbeidstaker bruker e-post på en måte som innebærer grovt brudd på de pliktene som gjelder i arbeidsforholdet

Dersom arbeidsgiver skal gjennomføre innsyn i e-post skal som hovedregel arbeidstaker varsles om dette og ha mulighet til å være tilstede. Arbeidstaker har i den forbindelse rett til å la seg bistå av en tillitsvalgt eller annen representant. I de tilfeller det ikke er mulig å varsle arbeidstaker før innsyn gjennomføres skal arbeidsgiver gi melding til arbeidstaker etter at innsyn er gjennomført.

Reglene om innsyn i e-post gjelder tilsvarende for arbeidsgivers rett til å gjennomføre innsyn i arbeidstakers personlige område på virksomhetens datanettverk og i andre elektroniske kommunikasjonsmedier som er stilt til rådighet for bruk i arbeidet.