Retningslinjer for brug af ODIN

Indholdsfortegnelse

Retningslinjer for brug af ODIN (herunder test- og øvelsesversionen) gælder for alle med brugeradgang til ODIN i såvel det kommunale som i det statslige redningsberedskab samt eksterne dataleverandører. Den enkelte bruger har pligt til at gøre sig bekendt med og efterleve de til enhver tid gældende retningslinjer for brug af ODIN.

For nærmere beskrivelse af proceduren for oprettelse og autorisation af brugeradgange, ændring af rettigheder m.v. henvises til dokumenterne "Adgangsstyring til ODIN – procedure for kommunale redningsberedskaber" og "Adgangsstyring til ODIN – procedure for statslige redningsberedskaber", der kan findes på Beredskabsstyrelsens hjemmeside www.brs.dk.

1. Brugeroprettelse og login

For at få adgang til ODIN kræves der, at man udfylder en brugeroprettelsesblanket og derved bliver autoriseret til brug af ODIN, og at én af følgende login-adgange opnås:

a. NemID medarbejdersignatur for brugere i det kommunale redningsberedskab.

b. Privat NemID for brugere i det kommunale redningsberedskab.
Denne metode bør alene anvendes undtagelsesvist og i givet fald som et frivilligt tilbud til brugerne. Beredskabsstyrelsen anbefaler, at der i stedet anvendes NemID medarbejdersignatur.

c. BRSNT AD konto for brugere i det statslige redningsberedskab.

d. DMZ AD konto for webservicebrugere (typisk eksterne dataleverandører).

I de følgende afsnit 2 – 4 gennemgås de retningslinjer, der knytter sig til de enkelte login-adgange, mens de øvrige afsnit 5 – 10 gælder for alle tre login-adgange, medmindre andet fremgår.

2. NemID medarbejdersignatur og privat NemID

NemID er udviklet af Nets DanID A/S i samarbejde med den danske banksektor og den danske stat. Den ansvarlige myndighed er Center for Digital Signatur i Digitaliseringsstyrelsen under Finansministeriet. For de nærmere krav til oprettelse af NemID medarbejdersignatur og privat NemID samt regler og sikkerhed i forbindelse med brug af NemID henvises til hjemmesiden www.nemid.nu.

3. BRSNT AD konto for brugere i det statslige redningsberedskab

For ansatte i det statslige redningsberedskab, der anvender en BRSNT AD konto, henvises til Beredskabsstyrelsens til enhver tid gældende retningslinjer for brug af it-produkter og udstyr på netværk i det statslige redningsberedskab, herunder krav og forholdsregler i forbindelse med adgangskode.

4. DMZ AD konto for webservicebrugere (typisk eksterne dataleverandører)

4.1. Oprettelse af DMZ AD konto

Før der kan ske oprettelse af webservicebrugere (henholdsvis konsulenter/udviklere og systemer) i ODIN, skal der oprettes en DMZ AD konto for disse, jf. "Adgangsstyring til ODIN – procedure for kommunale redningsberedskaber". Beredskabsstyrelsen sørger for oprettelse af en DMZ AD konto på baggrund af en udfyldt oprettelsesblanket, mens oprettelsen af brugeradgang og tildeling af rettigheder i ODIN sker ved det kommunale redningsberedskab.

Ved oprettelse af en DMZ AD konto for konsulenter/udviklere angives, hvor lang tid kontoen skal være aktiv dog maksimalt 3 måneder. Hvis der er behov for en forlængelse af kontoen, skal brugeren rette henvendelse til Beredskabsstyrelsen (Viden og Analyse) med henblik på forlængelse – dog tidligst 14 dage før kontoen udløber, og senest 5 dage før udløb for at sikre uafbrudt adgang – se kontaktoplysninger nedenfor.

4.2. Krav til adgangskode

I forbindelse med oprettelse af en DMZ AD konto tildeler Beredskabsstyrelsens IT Servicecenter en foreløbig adgangskode til kontoen, som bliver meddelt den enkelte bruger. Brugeren skal hurtigst muligt skifte password via følgende link https://pwdchg.brs.dk i overensstemmelse med neden-stående kriterier.

- Brugers adgangskode må ikke videregives eller udleveres til andre.
- Bruger skal undlade at nedskrive eller på anden måde lagre adgangskoden.
- Adgangskoden skal indeholde minimum 3 af følgende 4 kriterier: Store og små bogstaver, tal og specialtegn f.eks. !"#/()=?. Koden skal være minimum 10 karakterer lang. Udover dette må kodeordet ikke indeholde dele af brugernavnet.
- Systemet husker de sidste 24 koder, derfor kan man ikke genbruge de sidste 24 kodeord.

Når brugeren selv har skiftet password, kan denne tidligst skifte password igen efter 24 timer. Ved behov for skift af password inden for dette tidsrum kontaktes Beredskabsstyrelsens IT Servicecenter, se kontakt-oplysninger nedenfor.

Adgangskoden udløber efter 90 dage for konsulenter/udviklere, hvorfor disse skal sørge for udskiftning inden da på ovennævnte link. Såfremt de 90 dage overskrides skal brugeren rette henvendelse til Beredskabsstyrelsens IT Servicecenter med henblik på fornyelse.

Adgangskoden skal for systemer skiftes mindst én gang årligt på ovennævnte link.

4.3. Fejlslagne adgangsforsøg

Ved 10 sammenhængende fejlslagne adgangsforsøg fra samme DMZ AD konto låses der for yderligere forsøg. Det er nødvendigt at kontakte Beredskabsstyrelsens IT Servicecenter, før der kan låses op til systemet, se kontaktoplysninger nedenfor.

4.4. Misbrug eller kompromittering af adgangskode m.v.

Ved enhver mistanke om igangværende eller indtrufne ulovligheder, f.eks. misbrug af adgangskoden, virus- eller hackerangreb samt ved bortkomst eller tyveri af udstyr, skal bruger hvis muligt øjeblikkeligt slukke for udstyret og skifte adgangskoden. Hændelsen skal uden ugrundet ophold rapporteres til Beredskabsstyrelsens IT Servicecenter, se kontaktoplysninger nedenfor.

5. Afbrydelse af adgang (log ud)

Bruger skal sikre sig, at uautoriseret adgang til ODIN ikke sker via brugers arbejdsplads, herunder ved brug af hjemmearbejdsplads, privat PC m.v. Bruger skal derfor efter endt anvendelse af ODIN enten anvende log ud funktionen i ODIN, lukke internetbrowseren ned eller låse arbejdspladsen.

Brugere af NemID medarbejdersignatur (eller privat NemID) og webservicebrugere (DMZ AD konto) logges automatisk af, hvis systemet ikke er i brug i 30 minutter.

6. Glemt password

Beredskabsstyrelsen har ingen indflydelse på eller kontrol over adgangskoder til NemID medarbejdersignatur (eller privat NemID). Hvis adgangskoden glemmes eller på anden måde bortkommer henvises til hjemmesiden www.nemid.nu.

Brugere af BRSNT AD konto eller DMZ AD konto, der glemmer eller på anden måde mister deres adgangskode, henvises til at kontakte Beredskabsstyrelsens IT Servicecenter, se kontakt-oplysninger nedenfor.

7. Behandling af personoplysninger i ODIN

Den enkelte bruger skal sikre sig, at inddata- og uddatamateriale indeholdende personoplysninger (såvel papirbaseret som elektronisk lagret), der registreres, downloades, udskrives eller på anden måde behandles, ikke kan tilgås eller misbruges af uautoriserede personer, og at oplysningerne opbevares sikkert, f.eks. i aflåst skuffe, skab, på en PC beskyttet med password eller en BIT locket USB nøgle samt, at der anvendes en stærk kryptering for eksterne forbindelser.[1]

Disse foranstaltninger gør sig særligt gældende i forbindelse med brug af ODIN udenfor den normale arbejdsplads, f.eks. på en hjemmearbejdsplads, privat PC eller tablet samt ved anvendelse af webservices.

Udskrifter på papir eller elektronisk lagrede personoplysninger, der ikke længere anvendes med henblik på registrering eller anden behandling i ODIN, skal makuleres (papirbaseret) eller slettes (elektronisk) snarest muligt og senest 30 dage efter, behandlingen er afsluttet. Der henvises til Datatilsynets sikkerhedsvejledning.[2]

Den enkelte bruger skal sikre sig, at alene personer, der er autoriseret til de pågældende oplysninger og behandlinger i ODIN (f.eks. læsning eller indtastning), kan få adgang til disse.

Tilsvarende må data indeholdende personoplysninger ikke videregives til uautoriserede personer.

[1] Der henvises til Datatilsynets vejledning nr. 37 af 2. april 2001 (sikkerhedsvejledningen), jf. https://www.retsinformation.dk/Forms/R0710.aspx?id=1002 samt Datatilsynets definition af stærk kryptering på http://www.datatilsynet.dk/offentlig/sikkerhed/staerk-kryptering/

[2] Se endvidere http://www.datatilsynet.dk/offentlig/sikkerhed/sletning-af-datamedier/

8. Logning/registrering

Beredskabsstyrelsen foretager logning af alle behandlinger af oplysninger i ODIN herunder det anvendte søgekriterium samt alle gennemførte eller afviste adgangsforsøg til ODIN.

Loggen indeholder detaljer vedr. den enkelte handling (brugerid, tidspunkt, redningsberedskab, type af anvendelse m.v.). Loggen opbevares i 6 måneder, hvorefter den slettes. I særlige tilfælde kan loggen dog opbevares i op til 5 år.

9. Spørgsmål i forbindelse med retningslinjerne

Spørgsmål i forbindelse med nærværende retningslinjer kan rettes til Beredskabsstyrelsen, Viden og Analyse, der er ansvarlig for udarbejdelse og ajourføring af retningslinjerne.

10. Kontaktoplysninger

Beredskabsstyrelsen, Datavej 16, 3460 Birkerød, telefon 45 90 60 00, e-mail: brs@brs.dk

Beredskabsstyrelsens Viden og Analyse, telefon 45 90 60 00, e-mail: VIA@brs.dk

Beredskabsstyrelsens ODIN-hotline: ODIN@brs.dk

Beredskabsstyrelsens Sikkerhed og Drift, telefon 45 90 62 90, e-mail: SID@brs.dk