

# National eID-gateway

---

Marts 2022  
Version 1.1

## Beredskabspolitik

Dette dokument beskriver en fælles beredskabsprocedure for varsling og recovery i forbindelse med eventuelt driftsnedbrud af eID-gateway eller i forbindelse med eventuel kompromittering af denne.

Målgruppen for dette dokument er Digitaliseringsstyrelsen, driftsleverandøren af eID-gatewayen (NNIT) og alle offentlige tjenesteudbydere, der enten allerede er tilsluttet eID-gateway eller ønsker at blive tilsluttet løsningen.

## Indholdsfortegnelse

1. Beredskab hos Digitaliseringsstyrelsen.....	3
1.1 Ansvar.....	3
1.2 Kontaktinformationer .....	3
1.3 Varslinger.....	3
1.4 Recovery og datatab.....	4
2. Beredskab hos tjenesteudbydere .....	4
2.1 Ansvar.....	4
2.2 Varslinger.....	4
3. Versionshistorik .....	4

## 1. Beredskab hos Digitaliseringsstyrelsen

### 1.1 *Ansvar*

Digitaliseringsstyrelsen er forpligtet til at sikre et beredskab, således at eventuel nedetid af den fællesoffentlige log-in-løsning minimeres i størst muligt omfang.

### 1.2 *Kontaktinformationer*

Kontakt til Digitaliseringsstyrelsen i forbindelse med opfyldelse af beredskabsplan kan ske direkte til Digitaliseringsstyrelsens eID-gateway-team eller leverandøren NNIT.

Digitaliseringsstyrelsens eID-gateway-team, kan kontaktes pr. e-mail på følgende kontaktoverflade:

### **Digitaliseringsstyrelsens eID-gateway-team**

E-mail: [cidas@digst.dk](mailto:cidas@digst.dk)

Åbningstid:

Mandag-torsdag: 9:00-16:00

Fredag: 9:00-15:00

Lørdag, søn- og helligdage samt øvrige lukkedage: Lukket

Såfremt Digitaliseringsstyrelsens eID-gateway-team ikke svarer umiddelbart, eller der er brug for eskalering uden for åbningstiden, kan driftsleverandørens (NNIT) servicedesk kontaktes i forbindelse med driftsnedbrud af eID-gateway.

### 1.3 *Varslinger*

Digitaliseringsstyrelsens eID-gateway-team varsler direkte til administratorer for myndigheder og it-leverandører tilsluttet eID-gateway ved konstatering af:

- Kompromittering af IdP samt øvrige eID-gatewaykomponenter.
- Udefrakommende målrettede angreb mod eID-gateway af en væsentlig karakter.

eID-gateway-teamet er ansvarlig for, at alle tjenesteudbydere på eID-gateway bliver varslet om hændelser i forbindelse med kompromittering, ikke-planlagte systemnedbrud og udefrakommende systemangreb. eID-gateway-teamet vil meddele om utilsigtede hændelser, samt service- og lukkevinduer vedr. eID-gateway på [digitaliser.dk](http://digitaliser.dk) via gruppen "National eID-gateway", som er tilgængelig her:

<https://www.digitaliser.dk/group/3003373>

eID-gateway-teamet er ansvarlig for, at alle opkoblede tjenesteudbydere varsles mindst 5 dage før planlagte service- og lukkevinduer.

#### 1.4 Recovery og databab

I forbindelse med eventuelt systemnedbrud, hvor alvorlige fejl har har fatal indvirkning på løsningen, eller løsningen ikke kan anvendes, er driftsleverandøren (NNIT) kontraktuelt forpligtet til at igangsætte en løsning inden for 15 minutter samt rapportere til Digitaliseringsstyrelsen hver 2. time.

## 2. Beredskab hos tjenesteudbyder

### 2.1 Ansvar

Det er tjenesteudbyders eget ansvar at vurdere, hvorvidt der udarbejdes beredskabsplaner for egne systemer, men det vil være formålstjenligt, at der i alle tilfælde udarbejdes interne procedurer for varsling af eIDAS support i forbindelse med aktivering af beredskabet.

Myndigheden skal som led i tilslutningen til eID-gatewayen udpege en administrator, som er ansvarlig for varslinger i henhold til beredskabsplanen over for eIDAS support eller driftsleverandøren (NNIT).

### 2.2 Varslinger

Serviceudbyder er ansvarlige for hurtigst mulig efter konstatering af væsentlige driftsforstyrrelser eller mistanke om sikkerhedsbrud relateret til eID-gateway at meddele dette.

Tjenesteudbydere skal meddele til eID-gateway-teamet eller leverandøren af eID-gateway (NNIT).

I kontrakten med driftsleverandøren (NNIT) sondres mellem følgende kategorier af fejlforstyrrelser:

- Alvorlig fejl er defineret ved, at problemet har fatal indvirkning på løsningen, eller løsningen kan ikke anvendes, hvorfor log-in ikke muligt.
- Betydelig fejl er defineret ved, at problemet har stor indvirkning på en eller flere dele af løsningens anvendelse, hvorfor login er mulig, men væsentlige funktioner ikke er til rådighed.
- Mindre betydelig fejl er defineret som en mindre væsentlig fejl, som kan undgås ved alternativ arbejdsgang.

## 3. Versionshistorik

Version	Dato	Initialer	Indhold / ændringer
1.0	29.06.2018	OSBUH	Første version til offentliggørelse



1.1	09.03.2022	IDAWI	Tilpasninger i anvendt terminologi.
-----	------------	-------	-------------------------------------