Digitaliserings-
styrelsen

Notat

28. juni 2024

Bilag 1 – Oversigt over de primære ændringer i de reviderede NSIS-dokumenter

Nedenfor fremgår oversigter over de primære ændringer, som er indført i National Standard for Identiteters Sikringsniveauer (NSIS), Vejledning til National Standard for Identiteters Sikringsniveauer (NSIS) samt den nye Anmeldelses- og revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS). Ændringerne træder i kraft den 30. juni 2024.

National Standard for Identiteters Sikringsniveauer (NSIS)
Opdateret på baggrund af evaluering og erfaringsopsamling med revisorer og andre interessenter: • Terminologiafsnittet er udbygget med forklaring af centrale begreber (Lokal IdP og FullService IdP), og der er indført en ny illustration af begreberne Entitet, Digital Identitet og Identifikationsmiddel. • Der er indført et afsnit om 'tillidskæden for digitale identiteter' med henblik på at forklare roller og ansvar for de forskellige parter, der håndterer digitale identiteter. • Der er indført en præcisering af, hvornår et eksisterende identifikationsmiddel kan anvendes til at udstede et nyt identifikationsmiddel. • Krav 4.1.1 punkt 2) om overholdelse af lovgivning undtages fra revisionspligten, da der ikke føres tilsyn fra Digitaliseringsstyrelsen med overholdelse af generel lovgivning. • Forhold omkring oplysningspligten er præciseret. • Revisionserklæringer kan udformes af registrerede revisorer og statsautoriserede revisorer med relevante faglige kompetencer (4.1.7). • I afsnit 7.2 er det præciseret, at man ved nedlukning af en ID-tjeneste skal aflevere en afsluttende revisionserklæring for at undgå, at der findes længere perioder uden revision og dermed mulig tvivl om sikkerheden i perioden. • I afsnit 7.3 er formuleringen omkring ansvar bragt i overensstemmelse med standardens krav, herunder at erhvervsansvarsforsikringer i visse sammenhænge kan erstattes af andre ordninger.

- Henvisninger til NemID er fjernet.

Opdateret på baggrund af offentlig høring:

- Link til nyhedsbrev opdateret i afsnit 1.2.
- I 4.1.5 krav 7 er termen 'betroede adgange' ændret til 'privilegerede adgange'
- Kravene i 4.1.7 skal ikke længere medtages i anmelders revisionserklæring.
- I krav 5.2 punkt 9) er formulering om, at procedurer skal være underlagt revision ændret til, at de skal være dokumenterede.
- I 7.3 er beskrivelserne af evnen til at bære erstatningsansvar opdateret.
- Referencen til eIDAS-forordningen er opdateret til seneste udgave af forordningen.

Vejledning til National Standard for Identiteters Sikringsniveauer (NSIS)

Opdateret på baggrund af evaluering og erfaringsopsamling med revisorer og andre interessenter:

- Vejledning er udbygget vedr. kontrol af legitimation (3.1.2) ved verifikation af fysiske personer samt retningslinjer for validering af digitale kørekort.
- Vejledning er udbygget vedr. levering og aktivering (3.2.2), herunder fortolkning af kravene ved elektroniske udleveringsprocesser.
- Der er indført eksempler på, hvornår automatisk spærring kan være aktuel (3.2.3).
- Sikkerhed af autentifikationsmekanismer er udbygget (3.3.1).
- Sikkerhedstest af autentifikationsmekanismer er udbygget (3.3.1).
- Håndtering af underleverandører og deres ansvar er mere detaljeret beskrevet (4.1.1).
- Der er beskrevet eksempler på alternativer til ansvarsforsikringer (4.1.1 punkt 4).
- Bestemmelser vedr. oplysningspligt er udbygget (4.1.2).
- Vejledning til ISMS er udbygget (4.1.3).
- Krav til fysisk sikkerhed er udbygget (4.1.5 punkt 3).
- Beskrivelser af betroede medarbejdere og baggrundstjek er udbygget (4.1.5 punkt 5).
- Vejledning til nøglelængder og kryptografi er udbygget (4.1.6 punkt 7).
- Håndtering af medarbejderidentiteter (kapitel 5) er væsentligt udbygget, herunder vedrørende spærring og brug af autoritative kilder og procedurer for medarbejderes livscyklus.

- Vejledning vedrørende omveksling af eIDAS til NSIS-sikringsniveauer er indført i afsnit 6.1 og 6.2.
- Forhold vedr. sessionsstyring for brokere er udbygget (6.5).
- Logningskrav er udbygget (6.7).

I mange tilfælde refererer vejledningsteksterne nu til de tilsvarende områder i ISO 27001 Annex A, således at anmeldere lettere kan genfinde kontrolbeskrivelser og andet eksisterende materiale fra deres øvrige sikkerhedsarbejde.

Opdateret på baggrund af offentlig høring:

- Afsnit 3.1.2 punkt 6 er opdateret i forhold til validering af udenlandske pas.
- Afsnit 4.1.1 krav 3 har opdateret vejledning vedr. brug af anmeldte løsninger.
- Afsnit 4.1.1 krav 4 er opdateret i forhold til evne til at bære erstatningsansvar.
- Afsnit 4.1.3 krav 2 er opdateret med anbefaling om risikovurdering.
- Afsnit 4.1.5 krav 5 er opdateret i forhold til beskrivelsen af betroede medarbejdere og baggrundstjek.
- Afsnit 4.1.5 krav 7 er opdateret i forhold til beskrivelsen af privilegerede adgange.
- Afsnit 4.1.5 krav 7 har opdaterede henvisninger vedr. kryptografiske algoritmer.
- Afsnit 5.2 krav 9 har opdateret beskrivelse vedr. FullService IdP og deres aftaler med brugerorganisationer.
- Afsnit 6 krav 5 har opdaterede beskrivelser af forhold relevant for fastsættelse af sessionslængde.

Anmeldelses- og revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS)

Opdateret på baggrund af evaluering og erfaringsopsamling med revisorer og andre interessenter:

- Dokumenttitel ændret fra "Revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS)" til "Anmeldelses- og revisionsvejledning til National Standard for Identiteters Sikringsniveauer (NSIS)" for at tydeliggøre, at dokumentet ikke kun er rettet mod revisorer men også mod anmeldere.
- Struktur: Opdeling af kapitler.

- Eksemplet på udfyldelse af kontrolskema er uddybet og præciseret (2.1.1)
- Afsnit 1.3 Krav til revisionserklæringer er ændret til kapitel 3: Anmeldelser på niveau Betydelig og Høj.
- Præcisering af krav til dokumentation for tilsyn med underleverandører (3.4).
- Udvidelse af frist for indsendelse af Type 2-erklæringer fra 60 kalenderdage til 90 kalenderdage fra den dag, hvor 12-måneders perioden udløber (3.1).
- Nyt kapitel indført om anmeldelser på niveau Lav (kapitel 4).
- Nyt kapitel indført om anmeldelse af flere organisatoriske enheder (CVR-numre) (kapitel 5).
- Nyt kapitel indført om forhold der kan medføre afnotering (kapitel 6).
- Nyt kapitel indført om revision ved ophør af ID-tjeneste (kapitel 7).

Opdateret på baggrund af offentlig høring:

- Kapitel 2 er præciseret med, at det ikke er nødvendigt at vedlægge et kontrolskema i Excel-format, hvis det gives i et andet format og at Digitaliseringsstyrelsen vil udarbejde en skabelon for kontrolskemaet i Word.
- Afsnit 2.1.1 er præciseret med, hvilke revisionshandlinger revisor forventes at foretage + nyt eksempel.
- Kapitel 3 er ændret således at krav om eksplicit henvisning til dokumentation og eksplicit konklusion for hvert enkelt NSIS-krav udgår.
- I afsnit 3.2 er den forventede behandlingstid i NSIS Tilsynet ændret fra 30 til 60 kalenderdage.
- Afsnit 3.3 er udbygget med yderligere eksempler på signifikante ændringer.
- Afsnit 3.4.2 er præciseret i forhold til revisionshandlinger.
- Krav om redegørelse og handlingsplan for mindre væsentlige forhold, der er afdækket af revisionen, udgår af afsnit 3.2 og kapitel 4.
- Kapitel 4 er præciseret i forhold til intern revision.
- Det er beskrevet i kapitel 5, hvorledes ændringer i CVR-numre håndteres.
- Kapitel 6 er præciseret omkring proces ved overskridelse af tidsfrister.