Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren

Vedlegg til NSMs Rammeverk for håndtering av IKT-sikkerhetshendelser

Versjon 1
4. juni 2020

Innholdsfortegnelse

NSMs rammeverk

Meld. St. nr. 38 (2016-2017) IKT-sikkerhet - Et felles ansvar, stortingsmeldingen om IKT-sikkerhet, ble lagt frem våren 2017 og behandlet i Stortinget i vårsesjonen 2018. Styrking av vår nasjonale evne til å avdekke og håndtere digitale angrep er et av hovedområdene som omtales i stortingsmeldingen. Et sentralt tiltak for å bidra til en slik styrking er etableringen av et rammeverk for håndtering av IKT-sikkerhetshendelser. Dette rammeverket er utarbeidet av Nasjonal sikkerhetsmyndighet (NSM).

Hensikten med NSMs rammeverk for håndtering av IKT-sikkerhetshendelser[1] er å avklare og tydeliggjøre innsatsen mellom relevante aktører for å sette oss bedre i stand til å håndtere alvorlige IKT-sikkerhetshendelser som rammer på tvers av sektorer. På denne måten skal rammeverket bidra til mer effektiv håndtering av alvorlige IKT-sikkerhetshendelser, fra virksomhetsnivå til politisk nivå, gjennom god utnyttelse av samfunnets samlede ressurser. Det skal videre bidra til å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon om alle relevante IKT-sikkerhetshendelser.

Målgruppen for NSMs rammeverk er offentlige og private virksomheter som har betydning for kritisk infrastruktur og/eller kritiske samfunnsfunksjoner, sektorvise responsmiljøer, myndigheter som har en rolle knyttet til håndtering av IKT-sikkerhetshendelser og departementene.

Kunnskapsdepartementet har besluttet at rammeverket gjelder for underliggende virksomheter i høyere utdanning og forskning og har gitt Unit i oppgave å gjennomføre og følge opp rammeverket.

I samsvar med Nasjonal strategi for informasjonssikkerhet og handlingsplanen som følger strategien, legger rammeverk for håndtering av IKT-sikkerhetshendelser til grunn at de sektorvise responsmiljøene (SRM) skal ha en sentral rolle i hendelseshåndteringen.

Sektortilpasning av NSMs rammeverk

Arbeidet med gjennomføringen av rammeverket handler i stor grad om å koordinere og forbedre sektorens etablerte rutiner og kapasitet for hendelseshåndtering samt å sette dette inn i en større nasjonal sammenheng.

Dette dokumentet identifiserer sektorspesifikke myndigheter, etater og organer og deres rolle i hendelseshåndteringen i henhold til NSMs rammeverk.

[1] https://www.nsm.stat.no/publikasjoner/andre-publikasjoner/rammeverk-hendelseshandtering/

Institusjonene i UH-sektor underlagt rammeverket

Rammeverket gjelder for virksomheter underlagt Kunnskapsdepartementets avdeling for eierskap og styring

Arkitektur- og designhøgskolen i Oslo
Diku – Direktorat for internasjonalisering og kvalitetsutvikling i høyere utdanning
FEK - De nasjonale forskningsetiske komiteene
Høgskolen i Innlandet
Høgskolen i Molde - Vitenskapelig høgskole i logistikk
Høgskolen i Østfold
Høgskulen i Volda
Høgskulen på Vestlandet
Kunsthøgskolen i Oslo
NFR – Norges forskningsråd
Nokut - Nasjonalt organ for kvalitet i utdanninga
Nord Universitet
Norges Handelshøyskole
Norges idrettshøgskole
Norges miljø- og biovitenskapelige universitet
Norges musikkhøgskole
Norges teknisk-naturvitenskapelige universitet
NSD – Norsk senter for forskningsdata
NUPI – Norsk utenrikspolitisk institutt
OsloMet - storbyuniversitetet
Sámi allaskuvla - Samisk høgskole
Simula AS
Uninett AS
Unit - Direktoratet for IKT og fellestjenester i høyere utdanning og forskning
Universitetet i Agder
Universitetet i Bergen
Universitetet i Oslo
Universitetet i Stavanger
Universitetet i Sørøst-Norge
Universitetet i Tromsø - Norges arktiske universitet
Universitetssenteret på Svalbard

Sentrale aktører

NSMs rammeverk bygger på tre nivåer: virksomheter/systemeiere, sektorvise responsmiljøer (SRM) med fullmakt fra departement og NSM på nasjonalt sektorovergripende nivå.

Kunnskapsdepartementet (KD)

I tråd med Instruks for departementenes arbeid med samfunnssikkerhet, har ministeren for høyere utdanning og forskning det konstitusjonelle ansvaret for samfunnssikkerhet og beredskap i sektor for høyere utdanning og forskning. Dette ansvaret gjelder også for forebyggende IKT-sikkerhet og håndtering av IKT-sikkerhetshendelser i normalsituasjoner og i kriser. Ved kriser må KD innhente situasjonsrapporter fra egne operative virksomheter og være i stand til å identifisere og treffe beslutninger om nødvendige tiltak innen eget ansvarsområde for å håndtere den aktuelle situasjonen. KD skal påse at operative aktører har nødvendige fullmakter og vurdere behov for nasjonal og/eller internasjonal bistand til egen sektor. KD må videre kunne håndtere kommunikasjon med medier og befolkningen. Arbeidet må skje koordinert med andre departementer og Unit.

Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning

Kunnskapsdepartementet har i samråd med Unit bestemt at styringen av informasjonssikkerhet og personvern på sektornivå skal baseres på standarden ISO/IEC 27014:2013 – Governance of information security som er operasjonalisert gjennom innføringen av Kunnskapsdepartementets styringsmodell for informasjonssikkerhet 7. januar 2019. Styringsmodellen er tilpasset sektornivået i høyere utdanning og forskning. Departementet har gitt Unit ansvaret for den løpende sektorstyringen.

Unit skal i samråd med departementet sørge for gjennomføringen av rammeverk for håndtering av IKT-sikkerhetshendelser. Units ansvar er å sørge for at alle ansvarsområdene og oppgavene som ikke ligger til departementsnivået i rammeverket ivaretas. Dette innebærer blant annet å sørge for at Uninett CERT ivaretar oppgaven med å være et sektorvist responsmiljø slik dette er beskrevet i rammeverket og å utarbeide en arbeidsdeling og løpende samarbeid mellom Unit og Uninett i håndteringen av IKT-sikkerhetshendelser.

Units beredskapsorganisasjon skal støtte Uninett CERT og Kunnskapsdepartementets kriseledelse ved alvorlige hendelser.

Units rolle i rammeverket er som bindeledd mellom SRM-nivået og departementsnivået slik dette er beskrevet i NSMs rammeverk (se også Aktørkart).

Sektorvist responsmiljø (SRM) – Uninett CERT

Departementene skal påse at det er etablert sektorvise responsmiljø (SRM) med operativt ansvar for å dekke virksomheter innen hele eller deler av departementets myndighetsområde. Dette ansvaret har Kunnskapsdepartementet delegert til Unit.

Uninett CERT er utpekt av Unit på vegne av Kunnskapsdepartementet som sektorvist responsmiljø for høyere utdanning og forskning som definert i Nasjonal sikkerhetsmyndighets rammeverk for håndtering av IKT-sikkerhetshendelser, og skal gjennomføre oppgavene som SRM slik de er beskrevet i rammeverket.

Uninett CERT har i rollen som SRM som formål å forebygge, oppdage og håndtere sikkerhetshendelser for å beskytte sektorens informasjonsverdier, produksjons- og kommunikasjonsevne, materielle verdier og omdømme.

Uninett CERT skal både beskytte sektoren gjennom sentrale sikringstiltak i Uninetts nett og tjenester, og bistå virksomhetene i å utøve sitt eget ansvar for informasjonssikkerheten lokalt. Uninett CERT skal også koordinere sikkerhetsarbeidet i sektoren, samt samhandle med responsmiljøer fra andre sektorer og sikkerhetsområder.

Uninett CERT har fullmakt til å gjøre de tiltak de finner nødvendig i forbindelse med håndtering av IKT-sikkerhetshendelser i sektor for høyere utdanning og forskning. Dette inkluderer å begrense eller blokkere nettilkoblingen til enkeltressurser innad i forskningsnettet eller mellom forskningsnettet og omverdenen. I ytterste instans gjelder dette også en tilknyttet institusjons fullstendige nettforbindelse. Uninett CERT skal varsle Units beredskapsorganisasjon ved alvorlige hendelser.

Uninett CERT kan pålegge tilknyttede institusjoner tiltak for å stanse hendelser og begrense skadeomfang. Ved alvorlige hendelser kan Uninett CERT selvstendig iverksette egne tiltak som påvirker institusjonenes nettilknytning dersom lokale tiltak ikke kan skje tilstrekkelig raskt eller med tilstrekkelig virkning. Uninett CERT skal rapportere all bruk av slike tiltak til Unit.

Responsmiljøene NTNU SOC (Sikkerhetsoperasjonssenter) og Universitetet i Oslos IT-sikkerhetsgruppe UiO-CERT kan ved avtale bidra med kapasitet inn i Uninett CERT. Samarbeidet kan utvides med flere aktører.

Uninett CERT er ansvarlig for å vedlikeholde sektorens sambandskatalog.[2]

Uninett CERTs kontaktinformasjon https://www.uninett.no/cert
Uninett CERTs Policy and Service Level Statement
RFC 2350: Expectations for Computer Security Incident Response at Uninett CERT
NTNU SOC https://innsida.ntnu.no/wiki/-/wiki/Norsk/NTNU+SOC+-+Digital+sikkerhet
UIO-CERT https://www.uio.no/tjenester/it/sikkerhet/cert/

Virksomhetenes responsmiljøer - Incident Responce Team (IRT)
Unit har ansvar for å påse at virksomhetene har etablert egne responsmiljøer for håndtering av IKT-sikkerhetshendelser (IRT – Incident Response Team).

Uninett CERT delegeres det faglige ansvaret for å videreutvikle IRT-rollen og bidra til å gjøre institusjonene i stand til å ivareta denne. De har også ansvar for å tilby nødvendig opplæring. Det er en forutsetning at responsmiljøene etablerer en TLP-avtale[3] med Uninett AS og at de utveksler krypteringsnøkler slik at konfidensiell informasjon kan deles.

Oppdatert liste over virksomheter som har eget IRT (Incident Response Team) finnes på Uninett CERT sine informasjonssider https://www.uninett.no/cert-team-list

Kunnskapsdepartementet har besluttet at virksomhetene som omfattes av rammeverket skal ivareta det ansvaret og gjennomføre de oppgaver slik disse er beskrevet for virksomhetsnivået i NSMs rammeverk.

---

[2] Sambandskatalogen skal inneholde kontaktinformasjon til bruk ved håndtering av IKT-sikkerhetshendelser slik at det er enkelt å komme i kontakt med relevante samarbeidsparter både gjennom åpne (ugraderte) kanaler og gjennom kommunikasjonskanaler som er sikkerhetsgradert i henhold til Sikkerhetsloven.
[3] Trafikklysprotokoll (TLP) – Kontrollert deling av sensitiv informasjon
https://www.uninett.no/trafikklysprotokoll-tlp

Varsling

Figur 1 viser hvilke aktører som kan bli involvert ved en IKT-sikkerhetshendelse hos en virksomhet i sektor for høyere utdanning og forskning. Unit har ansvar for å vedlikeholde aktørkartet.

Virksomheten skal varsle sitt SRM, Uninett CERT ved sikkerhetshendelser som enten er alvorlige, går ut over virksomhetens myndighetsområde eller har klar relevans for sektoren eller enda videre

Uninett CERT skal varsle Units beredskapsorganisasjon ifølge Units varslingsliste ved alvorlige hendelser, potensielle kriser eller andre forhold som har en betydelig påvirkning på sektoren som helhet.

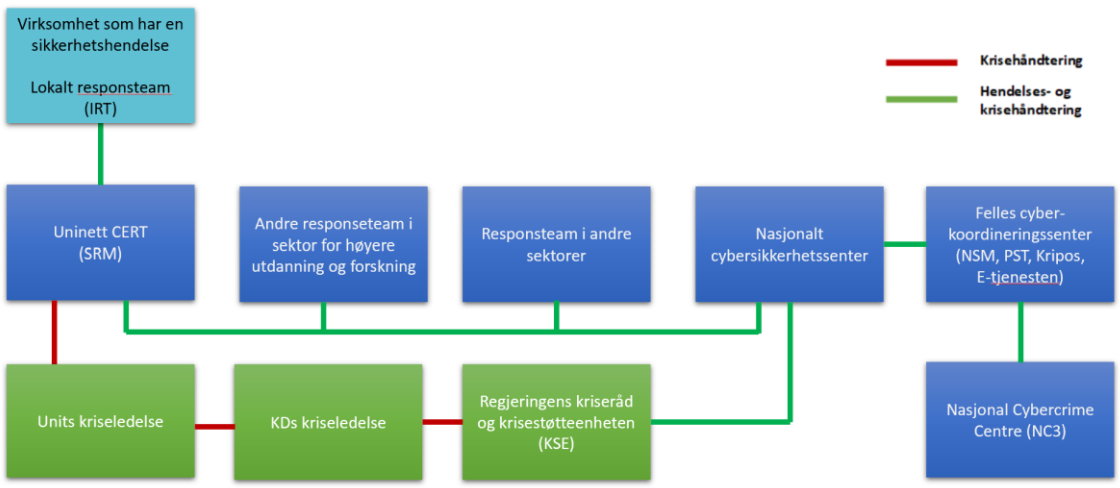
Unit skal varsle Kunnskapsdepartementets kriseledelse ved alvorlige hendelser eller kriser, etter departementets rutiner for krisehåndtering. Units kriseledelse bistår med informasjonshåndtering og annen støtte. De kan søke bistand fra KDs kriseledelse som igjen kan eskalere hendelsen til Regjeringens krisestøtteenhet (KSE).

Etter regjeringens rutiner for krisehåndtering skal Kunnskapsdepartementets kriseledelse om situasjonen krever det inngå i Regjeringens kriseråd og ellers yte påkrevd bistand koordinert gjennom Krisestøtteenheten (KSE).

Uninett CERT skal varsle NCSC (tidligere NorCERT) ved alvorlige hendelser, potensielle kriser eller forhold av sektoroverspennede natur.

NCSC (Nasjonalt cybersikkerhetssenter) skal om nødvendig eskalere situasjoner til Regjeringens kriseråd eller sørge for koordinering mellom SRMer og gjennom FCKS (Felles cyberkoordineringssenter) med Kripos eller andre enheter under NC3 (National Cybercrime Centre).
Uninett CERT vil samarbeide med responsteam i og utenfor sektoren hvis det er nødvendig.

Uninett CERT skal koordinere håndtering av alvorlige hendelser i sektoren med involverte aktører nasjonalt og internasjonalt.



FIGUR 1. AKTØRER, BESLUTNINGS- OG RAPPORTERINGSVEIER

UNIT

DIREKTORATET FOR IKT OG FELLESTJENESTER
I HØYERE UTDANNING OG FORSKNING