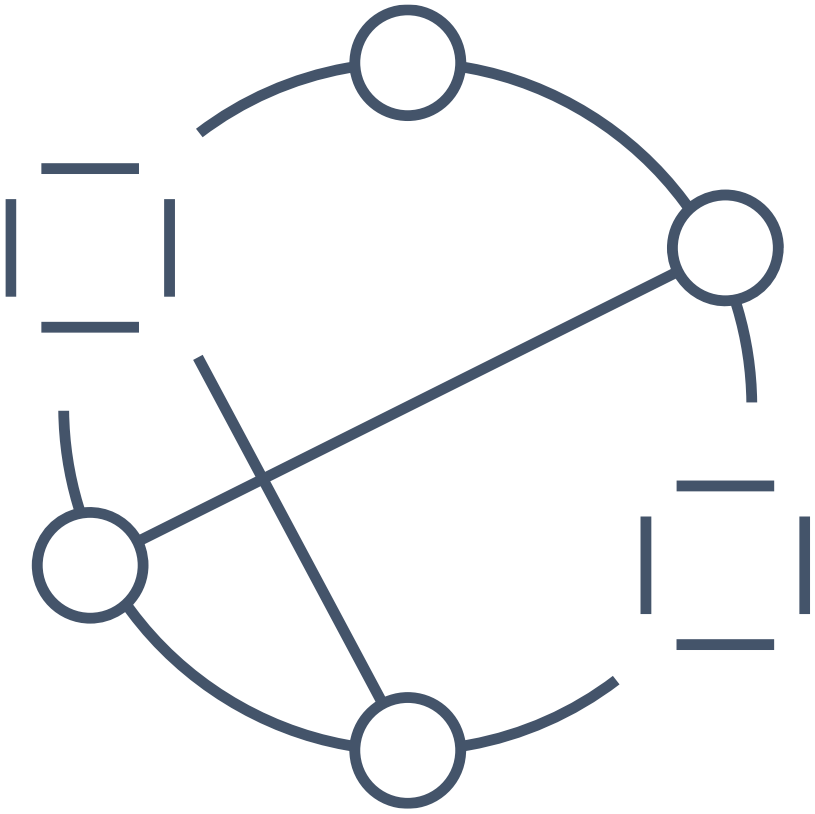
Bilag 2:

Service Beskrivelse - Dubex Incident Response Rammeaftale – Dansk Fjernvarme

Identifikation, isolering, og genopretning ved sikkerhedshændelser



Indholdsfortegnelse

1. Indhold, baggrund og formål

1.1 Indhold

Servicebeskrivelsen specificerer indholdet og særlige betingelser for den branchespecifikke Incident Response Service aftale igennem Dansk Fjernvarme.

1.2 Kundens værdi

Cyberangreb bliver hyppigere, mere avancerede og udgør en større trussel mod alle typer virksomheder. Derfor har du brug for en pålidelig sikkerhedspartner, der kan hjælpe dig med at identificere, isolere og genoprette.

Nærværende aftale giver dig adgang til Dubex Incident Response Teamet, hvori højtkvalificerede eksperter med de nødvendige værktøjer og mange års erfaringer står klar til at hjælpe.

Med Dubex Incident Response aftale får du som kunde:

- Mulighed for at forbedre din parathed, og reducere din risikoeksponering ved at følge *best practice* og anbefalinger fra Dubex Incident Response Team (herefter Dubex IRT).
- Vejledning og assistance fra Dubex Incident Response Team, som kan stoppe angrebet, begrænse skaden og undersøge årsagen.
- Adgang til Dubex' specialiserede viden og ekspertise indenfor incident response.
- Løbende evaluering og opdatering af proces og procedurer.

Din kvalitetssikring:

Dubex Incident Response Service er ISO/IEC 27001:2022 og ISAE3000/3402 certificeret. Desuden er Dubex Incident Response services inspireret af *best practice* fra henholdsvis NIST/FIRST/SIM3. Dette for at sikre en høj modenhed i vores service inklusiv veldokumenterede processer og procedurer som er med til at sikre et effektivt Incident Response beredskab.

1.3 Incident Response Team og omfang

Dubex Incident Response Team består af højt certificerede sikkerhedskonsulenter med mange års erfaring og ekspertise inden for incident response, herunder digital efterforskning, malwareanalyse med videre. Hver konsulent har den nødvendige viden, og værktøjer til at håndtere cyberangreb effektivt.

Dubex Incident Response konsulenter er uddannet i henhold til deres roller og ansvar, hvilket sikrer korrekt håndtering af bevisdata i forbindelse med cyberangreb. Dette omfatter korrekt håndtering af digitale spor samt sikring af bevismateriale for at lette en korrekt overdragelse til lokale eller internationale myndigheder, hvis det er nødvendigt.

I tilfælde af et cyberangreb, skal du aktivere og kontakte Dubex Cyber Defence Center som beskrevet i kundens Incident Proces Manual. Dubex Incident Manager samarbejder tæt sammen med jeres organisation for at kvalificere og kategorisere hændelsen. Dubex sikrer formel klassificering af incidents, hvilket giver effektiv håndtering af potentielle cyberangreb.

Dubex rådgiver også om, hvordan din organisations it-sikkerhed kan forbedres for at undgå lignende cyberangreb i fremtiden. Dette leveres som en betalt service baseret på medgået tid.

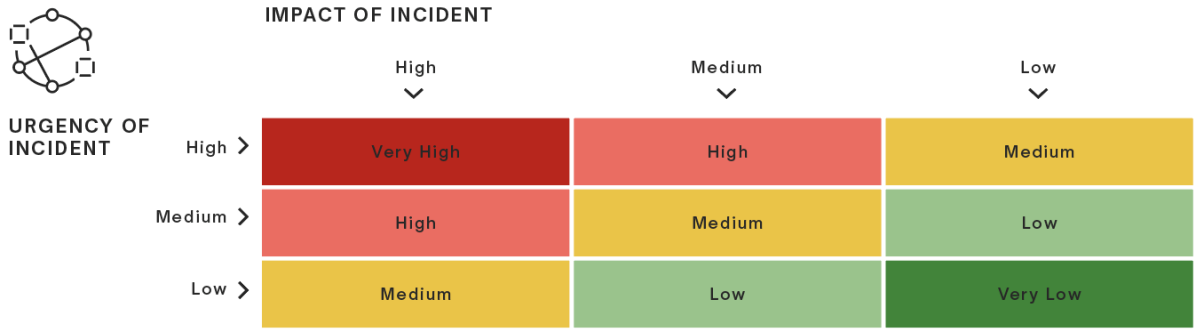
Dubex IRT består af følgende roller:

Incident Manager	Lead analyst	Incident Analyst
Vores Incident Managers sikrer et klart omfang for incident aktiviteter der skal udføres. Dette sker altid med din accept. Koordinerer statusmøder med briefing om status og incident aktiviteter Daglig gennemgang af tidsforbrug på incidents på tværs af alle aktive ressourcer og sikrer kundens accept af de påkrævede timer. Incident rapportering til kunden.	Triage undersøgelse. Prioritering af opgaver i forbindelse med incident efterforskning, inddæmning, samt hjælp til genopretning. Tidslinje og incident dokumentation. Artefakt dokumentation.	Incident efterforskning, inddæmning, samt hjælp til genopretningsopgaver tildelt af ledende analytiker.

1.4 Prioritering af hændelser

Prioritering af Incident Response aktiviteter i relation til cyberangreb henviser til, hvor hurtigt og alvorligt en situation kræver en reaktion for at mildne dens indvirkning på jeres organisation. Cyberangreb kan variere meget i indvirkning samt hastende karakter, og det afhænger af flere faktorer; herunder typen af angreb, dets potentielle konsekvenser for din virksomhed, målets sårbarhed og angriberens motivationer.

Dubex IRT vil under et incident afstemme forventningerne til hændelsens prioritering. Nedenstående grafik beskriver prioriteringen af hændelser:



Prioritering af hændelsesmatrix

1.5 Statusmøder

Som en del af Dubex Incident Response Service-aftalen afholder vi årlige statusmøder for at holde dig opdateret med de nyeste sikkerhedstendenser. De årlige statusmøder afholdes online mellem parterne, med en varighed på ca. en time. Her gennemgår vi bl.a. din Incident Procedure Manual igen for at tilse, at den stadig stemmer overens med de fælles krav og behov for et effektivt samarbejde før og under incidents.

Hver 6. måned giver vi dig også ny viden baseret på nye og aktuelle trusler. Dette sker via Dansk Fjernvarmes fælles sektorspecifikke onlinemøder.

1.6 Forensics

Dubex IRT tilbyder ekspertise inden for digital efterforskning og analyse samt bevissikring. Vores mål er at hjælpe dig med at identificere præcis, hvad der er sket med de berørte systemer. Vi reagerer hurtigt og effektivt for at lokalisere, isolere og afhjælpe sikkerhedsproblemer.
Vores specialister undersøger bagdøre, analyserer logfiler og gennemgår alt, der kan indikere, hvad der har forårsaget angrebet. Dette arbejde er afgørende for at forhindre lignende hændelser i fremtiden.

1.7 Rådgivning på management niveau

Vores Incident Management funktion sikrer, at du som kunde har adgang til ledelsessparring. Vi gennemfører ”War Rooms”, Incident koordinations møder, for at holde dig involveret og opdateret om prioritering af hændelser, fremskridt og opgaver relateret til inddæmning og genopretning. Fælles War Room-møder er vigtige for at sikre, at ledelsen får den rette sparring og indblik ift. kritiske beslutninger og prioriteringer under incidents.

1.8 Værktøjer inkluderet

Vores eksperter benytter en omfattende portefølje af Incident Response og Forensics softwareværktøjer til afhjælpning af hændelser og digital analyse. Vi gør altid brug af branchens bedste værktøjer til at sikre et effektivt arbejde med at begrænse og undersøge hændelser i jeres organisation. Alle Dubex standardværktøjer er inkluderet i vores service.

1.9 Debriefing efter et incident

Efter et incident kan vores Incident Response team efter ønske lave en incidentrapport der præcist identificerer, hvad der skete i dit miljø. Vi rådgiver også om, hvordan du kan forbedre it-sikkerheden generelt, så du kan undgå lignende sikkerhedsbrud i fremtiden.

Før debriefingen begynder vil vi tilpasse rapportens detaljeringsniveau og forventet tidsforbrug i overensstemmelse med dig.

2. Dubex Incident Response Service RACI Matrix

Nedenstående tabel beskriver parternes opgaver, roller og ansvar i overensstemmelse med de aftalte beslutningsprocesser i henhold til aftalen.

- **R =** Ansvarlig - Hvem udfører opgaven;
- **A =** Ansvarlig - Hvem har myndighed til at godkende eller afvise opgaven;
- **C =** Konsulteret - Hvem har vigtig viden og giver information;
- **I =** Informeret - Hvem skal informeres om status og resultater.

Ansvar – Dubex Incident Response Team	Dubex	Kunde
Adgang til Dubex Incident Response Service	RAC	I
Afholdelse af statusmøder	RA	CI
Udarbejdelse og vedligeholdelse af Incident Proces Manual	CI	RA
Kategorisering af hændelser	RC	IA
Håndtering af hændelser	RC	IA
Debriefing efter en hændelse	RA	CI
Forensics	RA	CI
Vedligeholdelse af tilgængeligheden af ITSM-webportalen (IT Service Management), hvor du kan få adgang til sagsproceduren.	RAC	I

2.1 Brugsret til software og dokumentation

Som kunde erhverver du alene brugsret til den leverede software og dokumentation. Det betyder, at du modtager en tidsbegrænset, ikke-eksklusiv og ikke-overdragelig licens til at gøre brug af disse softwareværktøjer og dokumentation i aftalens løbetid.

2.2 Indhold af Dubex Incident Response Service

Tabellen nedenfor beskriver indholdet af Dubex Incident Response Service.

Indhold	Dubex Incident Response Service
Adgang til tjeneste	Du har adgang til Dubex Incident Response-tjenester 24/7/365.
Håndbog i kvalificeret beredskab	Der defineres en kvalificeret Incident Procedure Manual for at optimere effektiviteten, når kunden aktiverer Dubex IRT
Håndtering af hændelser	Dubex håndterer hændelser. Dette leveres som en betalt service baseret på medgået tid (T&M).
Værktøjer inkluderet	Alle Dubex standardværktøjer er inkluderet i vores service.
Status møder	Årlig
Sektorspecifik orientering	En online sektorspecifik trusselsintelligensopdatering leveres hver 6. måned
Rapport om reaktion på hændelser	Hvis du aktiverer beredskabet, kan parterne aftale at levere en hændelsesrapport efter brug af tjenesten, som skal indeholde anbefalinger mv. Rapportering leveres som en betalt service baseret på medgået tid (T&M).
Forensics analyse	Adgang til Forensics eksperter i forbindelse med efterfølgende dataindsamling og digital analyse efter behov. Forensics leveres som en betalt service baseret på medgået tid(T&M).

2.3 Økonomi

Dubex Incident Response-servicegebyret betales forud på årsbasis som angivet i leveranceaftalen. Timer brugt i forbindelse med Dubex Incident Response Service-aftalen faktureres i overensstemmelse med bilag 1; Dubex generelle vilkår og betingelser. Timeprisen fremgår af leveranceaftalen.

3. Serviceniveauaftale

3.1 Tilgængelighed

Dubex er forpligtet til at overholde følgende krav:

Tilgængelighed	Kommentar
24/7/365	Når aftalen er underskrevet, stilles beredskabstjenesten til rådighed 24/7/365.

3.2 Svartider

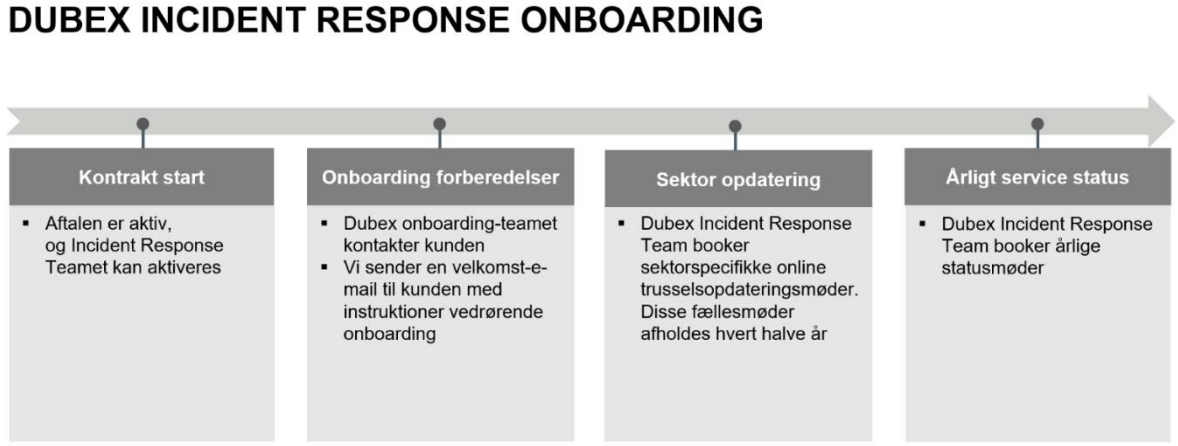
Dubex er forpligtet til at overholde svar tiderne med følgende krav:

Hændelser eskaleret i overensstemmelse med Incident Proces Manualen		
Beskrivelse	**Svartid**	**SLA**
Dubex Incident Response service opstart	<4 timer	100%
Dubex Incident Response konsulent(er) tilstede på lokationen i henhold til proces- og proceduremanualen	<4 timer <8 timer <24 timer	90%
Dubex Incident Response konsulent(er) på stedet i henhold til den fastlagte procedure	<8 timer	97,5%
Dubex Incident Response konsulent(er) på stedet i henhold til den fastlagte procedure	<24 timer	100%
Incident Response og kriminalteknisk rapportering efter hændelsens afslutning	10 Dubex hverdage	90 %

4. Onboarding

Når du underskriver serviceaftalen, modtager du en velkomstmail med instruktioner om, hvordan du aktiverer Dubex Incident Response Team.
Denne e-mail indeholder også en vejledning til, hvordan du udfylder vores fælles Incident Procedure Manual (IPM). Manualen fungerer som en ressource, hvis din organisation står over for en sikkerhedshændelse, der kræver hurtig assistance.

IPM vil blive evalueret på de årlige servicestatusmøder.



4.1 Onboarding ansvar - RACI Matrix

Tabellen nedenfor beskriver parternes opgaver, roller og ansvar i overensstemmelse med de aftalte onboarding-processer i henhold til nærværende aftale.

- **R =** Ansvarlig – Hvem udfører og fuldfører opgaven.
- **A =** Ansvarlig – Hvem har bemyndigelse til at godkende eller afvise opgaven.
- **C =** Konsulteret - Hvem har vigtig viden og giver information.
- **I =** Informeret - Hvem skal informeres om status og resultater.

Ansvar – onboarding af Dubex Incident Response Team	Dubex	kunde
Planlægning af onboarding-fasen	RA	CI
Udarbejdelse af Incident Procedure Manual	CI	RA
Opret og aktiver dine brugere i Dubex ITSM-systemet	RA	CI
Planlægning af statusmøder	RA	IC

4.2 Offboarding

Når serviceaftalen er udløbet, og aftalen opsiges, vil din organisation blive fjernet. Offboardingen forventes at vare 1-2 uger.

Dubex fjerner dine oplysninger fra alle Dubex systemer. Du er ansvarlig for at fjerne installeret software og slette dokumentation vedrørende levering af Dubex Incident Response Service.

4.3 Offboarding ansvar - RACI Matrix

Tabellen nedenfor beskriver parternes opgaver, roller og ansvar i overensstemmelse med de aftalte offboarding-processer i henhold til nærværende aftale.

- **R =** Ansvarlig – Hvem udfører og fuldfører opgaven.
- **A =** Ansvarlig – Hvem har bemyndigelse til at godkende eller afvise opgaven.
- **C =** Konsulteret - Hvem har vigtig viden og giver information.
- **I =** Informeret - Hvem skal informeres om status og resultater.

Ansvar – Dubex Incident Response Service offboarding	Dubex	Kunde
Sletning af brugere i ITSM-portalen	RAC	I
Sletning af Incident Procedure Manual i Dubex systemer	RAC	I
Af installation af Dubex og 3. parts software på dine systemer	IC	RA
Sletning af eventuelt indsamlet incident data i Dubex systemer	RAC	I