NorgesGruppen

Standard kontraktkrav til informasjonssikkerhet og risikostyring

Versjonskontroll:

Versjon	Dato	Endret	Godkjent av
1.0	05.04.2022	1. utkast	Paul Svenning
1.1	02/11/2022	Lagt til engelsk versjon av kravene	Paul Svenning

Følgende overordnede krav skal være med i alle tjenesteavtaler som NGD inngår med leverandører. Kravene skal være en del av bilag 1 dersom man benytter SSA rammeverket. Dersom man benytter annet avtaleformat, må alle punkter sjekkes ut i avtaleutkastet og de må verifiseres å være ivaretatt før signering av avtale.

Krav	**Engelsk versjon**	**Kommentar**
a) Leverandøren skal ha et styringssystem for informasjonssikkerhet (ISMS), basert på anerkjente standardarder som ISO 27001, NIST CSF, CIS eller NSM Grunnprinsipper for IT-sikkerhet. Styringssystemet skal på en effektivt og god måte ivaretar Kundens informasjon og renomme.	a) The Supplier shall have an Information Security Managements System (ISMS) based on recognized standards as ISO 27001, NIST, CSF, CIS or NSM basic principles for IT security. The information Security system shall be efficient and in an good way	Dette kravet er nødvendig for: i. Å sikre etterlevelse av GDPR, som krever at bedrifter som behandler personopplysninger skal ha et styringssystem for informasjonssikkerhet. ii. Å sikre at våre leverandører har et bevists forhold til informasjonssikkerhet og ikke utgjør en risiko for konsernets informasjonssikkerhet

	safeguard the Customer's information and reputation.	iii. Å sikre etterlevelse av NG sine krav til informasjonssikkerhet iv. Å sikre sikkerheten i forsyningskjeden Dette er et krav som ikke kan fravikes.
b) Leverandøren skal til enhver tid ha ett oppdatert register over informasjon og utstyr tilhørende Kunden som disponeres av Leverandøren.	b) The Supplier shall at all times have an up-to date register of information and assets belonging to the Customer that is controlled by the Supplier. .	Dette kravet er nødvendig for: i. Bedre forstå konsekvensene for NorgesGruppen hvis leverandøren blir utsatt for en sikkerhetshendelse ii. Bevisstgjøre og ansvarliggjøre leverandøren i forhold til forvaltning av NG informasjon og utstyr. iii. Å sikre etterlevelse av GDPR, hvis leverandøren behandler personopplysninger på vegne av NG. Kan frafalles, hvis leverandøren ikke i. Disponerer utstyr (f.eks PC'er) tilhørende NorgesGruppen ii. Ikke prosesserer forretningsdata tilhørende NorgesGruppen iii. Ikke prosesser persondata på vegne av NorgesGruppen iv. Hvis det allerede dekkes inn av DPA (databehandleravtale)
c) Leverandøren skal ha et system for tilgangs- og identitetskontroll som forhindrer uautorisert tilgang til systemer og informasjon.	c) The Supplier shall have a system for access- and identity control to prevent unauthorized access to systems and information.	Dette kravet nødvendig for: i. Å sikre etterlevelse av GDPR, hvis leverandøren behandler personopplysninger på vegne av NG. ii. Redusere risikoen for at informasjon tilhørende NG kommer på avveie. iii. Redusere risikoen for at NG blir rammet av et cyberangrep via leverandørkjeden.

		Dette er et krav som ikke kan fravikes
d) Leverandøren skal ha en prosess for å garantere at all programvare og maskinvare som benyttes enten tilhører en aktivt forvaltet vedlikeholdsavtale eller har lokale rutiner for å sikre at programvare/maskinvare uten vedlikeholdsavtale holdes oppdatert i henhold til programvare-/maskinvareleverandørs anbefalinger.	d) The Supplier shall have a process to ensure that all software and hardware that are used, either belong to an actively managed maintenance agreement or have local routines to ensure that software / hardware without a maintenance agreement is kept up-to-date in accordance the software-/hardware vendor's recommendations.	Dette kravet nødvendig for: i. Å sikre etterlevelse av GDPR, hvis leverandøren behandler personopplysninger på vegne av NG. ii. Redusere risikoen for at NG blir rammet av et cyberangrep via leverandørkjeden. Dette er et krav som ikke kan fravikes
e) Leverandøren skal sørge for at informasjonssikkerhetskrav i kontrakten er gjort kjent for og er gjort gjeldende for underleverandører av varer og tjenester som omfattes av avtalen.	e) The Supplier shall ensure that security requirements in the Contract are communicated to and made applicable for subcontractors of the services provided to the Customer.	Dette kravet nødvendig for: i. Å sikre etterlevelse av GDPR, hvis leverandøren behandler personopplysninger på vegne av NG. ii. Redusere risikoen for at NG blir rammet av et cyberangrep via leverandørkjeden. Dette er et krav som ikke kan fravikes
f) Leverandøren skal ha klare rutiner for håndtering av sikkerhetshendelser og utbedring av offentlig rapporterte sårbarheter som påvirker leverandørens IT- og OT-systemer	f) The Supplier must have clear routines for handling security incidents and improvement of publicly reported weaknesses that affect the Suppliers IT- and OT systems.	Dette kravet nødvendig for: i. Å sikre etterlevelse av GDPR, hvis leverandøren behandler personopplysninger på vegne av NG. ii. Redusere risikoen for at leverandøren ikke klarer å levere varer og tjenester som kontraktfestet.

		iii. Redusere risikoen for at NG blir rammet av et cyberangrep via leverandørkjeden. Med offentlige rapporterte sårbarheter så menes offentliggjorte sårbarheter i programvare eller maskinvare som er levert til NG av leverandøren, eller i programvare og maskinvare som leverandøren benytter for å levere tjenester og varer til NG. Dette er et krav som ikke kan fravikes
g) Leverandøren skal ha etablerte og effektive sikkerhetskontroller egnet til å avdekke og forhindre skadevare, sikkerhetshendelser og handlinger som negativt kan påvirke Kunden.	g) The Supplier must have established and effective security controls that are capable of detecting and preventing damage, securityincidents and actions that could adversely affect the Customer.	Dette kravet nødvendig for: i. Å sikre etterlevelse av GDPR, hvis leverandøren behandler personopplysninger på vegne av NG. ii. Redusere risikoen for at NG blir rammet av et cyberangrep via leverandørkjeden. Dette er et krav som ikke kan fravikes
h) Leverandøren skal ha rutiner for effektiv varsling av Kunden om sikkerhetshendelser som påvirker, eller indirekte kan påvirke, kunden.	h) The Supplier must have routines for effective notification of the Customer regarding security incidents that affect, or indirectly potentially affect the Customer. Notification to the Customer must be made without undue delay.	Dette kravet nødvendig for: i. Å sikre etterlevelse av GDPR, hvis leverandøren behandler personopplysninger på vegne av NG. ii. Å sikre at NG blir raskt informert om sikkerhetshendelser som potensielt kan ha negative konsekvenser for NG. iii. Å sikre at NG raskt kan iverksette egne risikoreduserende tiltak ved

		sikkerhetshendelser som kan ha negative konsekvenser for NG. Dette er et krav som ikke kan fravikes
i) Leverandøren skal ha oppdaterte planer som sikrer forretningskontinuitet ved katastrofale informasjonssikkerhetshendelser som påvirker leveranse av varer og/eller tjenester til Kunden.	i) The Supplier shall have updated plans that secure the business continuity in case of catastrophic information security incidents that affect the delivery of goods and/or services to the Customer.	Dette kravet eksisterer for å sikre NG sin egen forretningskontinuitet hvis en kritisk eller katastrofal hendelse rammer en eller flere av våre underleverandører. Kan frafalles hvis: i. Leverandøren ikke negativt kan påvirke NG sin forretningskontinuitet. F.eks ved stopp i vareflyt, leveranse av tjenester eller cyberangrep mot NG via leverandørkjeden.
j) Leverandørens personell som jobber med taushetsbelagt informasjon relatert til Kunden skal ha signert en taushetserklæring.	j) All Supplier's personnel working with confidential information related to the Customer must have signed a Non-Disclosure Agreement.	Dette kravet nødvendig for: i. Økt bevissthet hos ressurser som behandler informasjon på vegne av NG ii. Redusert risiko for at informasjon tilhørende NG blir lekket eller kommer på avveie. iii. Sanksjonsmuligheter hvis taushetsbelagt informasjon skulle komme på avveie Dette er et krav som ikke kan fravikes
k) Leverandøren skal som minimum gjennomføre årlige sikkerhetsrevisjoner av eget styringssystem	k) The Supplier shall as a minimum conduct annual security audits of its own information security	Dette kravet eksisterer for å sikre at leverandøren holder sitt eget styringssystem for informasjonssikkerhet oppdatert, noe som blant

for informasjonssikkerhet (ISMS). Revisjon skal dokumentere funn og tiltak for avdekkede avvik.	management system (ISMS). The audit shall document findings and actions for uncovered deviations..	annet reduserer risikoen for at de rammes av en cyberhendelse som kan påvirke NG negativt. Kan frafalles hvis: ii. Leverandøren ikke negativt kan påvirke NG sin forretningskontinuitet. F.eks ved stopp i vareflyt, leveranse at tjenester eller cyber angrep mot NG via leverandørkjeden. iii. Leverandøren ikke behandler personopplysninger på vegne av NG iv. Leverandøren ikke behandler sensitive forretningsdata.
l) Kunden har rett til å gjennomføre en sikkerhetsrevisjon av leverandørens styringssystem for informasjonssikkerhet (ISMS). Sikkerhetsrevisjonen kan gjennomføres en gang per år, eller i etterkant av alvorlige sikkerhetshendelser. Alternativt så kan revisjonen gjennomføres av uavhengig 3dje part valgt av kunden i samråd med leverandøren. i. Avvik som utgjør en risiko for kunden, skal forelegges kunden med en tilhørende tiltaksplan.	l) The Customer has the right to carry out a security audit of the Supplier's Information Security Management System (ISMS) The security audit can be carried out once a year or in the aftermath of serious security incidents. The audit can be carried out by a independent third part chosen by the Supplier, and in this case the audit report shall be presented to the Customer. i. Non-conformities that represent a risk for the Customer shall be presented to the customer with a plan for mitigating actions.	Dette kravet nødvendig for: i. Sikre at leverandøren overholder sikkerhetskravene som er definert i kontrakten ii. Sikre at leverandøren ikke utgjør en uakseptabel sikkerhetsrisiko for NG iii. Redusere risikoen for at en cyberhendelse i leverandørkjeden har en negativ påvirkning for NG iv. Sikre kontinuerlig forbedring av leverandørens og kundens ISMS Kan frafalles hvis: i. Leverandøren ikke negativt kan påvirke NG sin forretningskontinuitet. F.eks ved stopp i vareflyt, leveranse at tjenester eller cyberangrep mot NG via leverandørkjeden. ii. Leverandøren ikke behandler personopplysninger på vegne av NG

		iii. Leverandøren ikke behandler sensitive forretningsdata. iv. Leverandøren er ISO27001 sertifisert for de områdene som inngår i leveransen til NG.
m) Leverandøren skal ha en fungerende og etablert prosess for risikostyring. Prosessen skal håndtere risikoer relatert til informasjonssikkerhet og være basert på et anerkjent rammeverk for risikostyring som for eksempel ISO 27005, ISO 31000, ISF IRAM eller tilsvarende.	m) The Supplier shall have a functioning and established risk management process. The process should address risks related to information security and be based on a recognized risk management framework such as ISO 27005, ISO 31000, ISF IRAM or equivalent.	Dette kravet eksisterer for å sikre at leverandøren holder sitt eget styringssystem for informasjonssikkerhet levende, noe som blant annet reduserer risikoen for at de rammes av en cyberhendelse som kan påvirke NG negativt. Kan frafalles hvis: i. Leverandøren ikke negativt kan påvirke NG sin forretningskontinuitet. F.eks ved stopp i vareflyt, leveranse at tjenester eller cyber angrep mot NG via leverandørkjeden. ii. Leverandøren ikke behandler personopplysninger på vegne av NG iii. Leverandøren ikke behandler sensitive forretningsdata.
n) Leverandøren skal som minimum gjennomføre en årlig risikoanalyse som belyser alle aspekter av Leverandørens ansvar under kontrakten. Risikoanalysen skal dokumenteres, oversendes Kunden og gjennomgås med Kunden.	n) The Supplier shall, as a minimum, carry out an annual risk analysis which highlights all aspects of the Supplier's liability under the contract. The risk analysis must be documented, sent to the Customer and reviewed with the Customer.	Dette kravet eksisterer for å sikre at leverandøren holder sitt eget styringssystem for informasjonssikkerhet levende, noe som blant annet reduserer risikoen for at de rammes av en cyberhendelse som kan påvirke NG negativt. Kan frafalles hvis: i. Leverandøren ikke negativt kan påvirke NG sin forretningskontinuitet. F.eks ved stopp i vareflyt, leveranse at tjenester eller cyberangrep mot NG via leverandørkjeden.

		ii. Leverandøren ikke behandler personopplysninger på vegne av NG iii. Leverandøren ikke behandler sensitive forretningsdata.