Stockholms stad

**PM Rotel I (Dnr KS 2025/1384)**

# Anmälan om svar på remiss av Förslag till nya föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning enligt ny cybersäkerhetslag

Remiss från Myndigheten för samhällsskydd och beredskap (MSB)

## Förslag till beslut

Borgarrådsberedningen föreslår att kommunstyrelsen beslutar följande.

Anmälan om svar på remiss godkänns.

**Föredragande borgarrådet Karin Wanngård**

## Sammanfattning av ärendet

Myndigheten för samhällsskydd och beredskap (MSB) har remitterat Förslag till nya föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning enligt den kommande cybersäkerhetslagen samt tillhörande konsekvensutredning till bland annat Stockholms stad för yttrande.

På grund av kort remisstid har staden svarat med stadsledningskontorets tjänsteutlåtande.

## Beredning

Ärendet har remitterats till stadsledningskontoret.

*Stadsledningskontoret* tillstyrker förslagen i huvudsak men anser att vissa delar behöver förtydligas för att säkerställa en ändamålsenlig och proportionerlig tillämpning i kommunal verksamhet.

## Föredragande borgarrådets synpunkter

Jag föreslår att borgarrådsberedningen föreslår att kommunstyrelsen godkänner anmälan om svar på remissen.

Stockholm den 14 januari 2026

Karin Wanngård

Bilagor

1. Remiss - Förslag till nya föreskrifter om säkerhetsåtgärder och utbildning enligt ny cybersäkerhetslag, dnr KS 2025/1384-1.1
2. Remiss - Konsekvensutredning gällande förslag till nya föreskrifter om säkerhetsåtgärder och utbildning enligt ny cybersäkerhetslag, dnr KS 2025/1384-1.2

**Borgarrådsberedningen** tillstyrker föredragande borgarrådets förslag.

## Ärendet

Myndigheten för samhällsskydd och beredskap (MSB) har remitterat Förslag till nya föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning enligt den kommande cybersäkerhetslagen samt tillhörande konsekvensutredning till bland annat Stockholms stad för yttrande.

Enligt artikel 21 i NIS2-direktivet ska medlemsstaterna säkerställa att verksamhetsutövare vidtar tekniska, driftsrelaterade och organisatoriska åtgärder som är lämpliga och proportionella. I Sverige genomförs direktivet genom den föreslagna cybersäkerhetslagen, som utgör grunden för MSB:s föreskrifter om säkerhetsåtgärder och utbildning.

MSB:s förslag till föreskrifter syftar till att bidra till att säkerställa en hög och enhetlig nivå av cybersäkerhet i Sverige. Förslaget förtydligar hur verksamhetsutövare ska uppfylla lagens krav på säkerhetsåtgärder och utbildning, och stödjer ett riskbaserat och proportionerligt genomförande av NIS2-direktivets bestämmelser. Föreskrifterna preciserar vilka organisatoriska, tekniska, driftsrelaterade och fysiska säkerhetsåtgärder som minst ska vidtas samt vilka krav som gäller för utbildning av verksamhetsutövarens ledning.

## Remissammanställning

Ärendet har remitterats till stadsledningskontoret.

### Stadsledningskontoret

**Stadsledningskontorets** tjänsteutlåtande daterat den 19 november 2025 har i huvudsak följande lydelse.

## Sammanfattning av synpunkter

*Stadsledningskontoret tillstyrker* i huvudsak MSB:s förslag till föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning enligt den kommande cybersäkerhetslagen. Föreskrifterna bedöms ge en tydlig och strukturerad grund för hur verksamhetsutövare uppfyller lagens krav samt bidrar till en hög och enhetlig nivå av cybersäkerhet.

*Stadsledningskontoret anser* dock att vissa delar behöver förtydligas för att säkerställa en ändamålsenlig och proportionerlig tillämpning i kommunal verksamhet. Kraven i föreskriften är detaljerade, vilket riskerar att begränsa proportionalitetsprincipens praktiska betydelse och göra föreskrifterna mer styrande än vad som avsetts.

Vidare *efterfrågar stadsledningskontoret* en mer konkret redovisning i konsekvensutredningen av de förväntade investeringskostnaderna samt tydligare

vägledning kring eventuella behov av systemuppgraderingar och tidsramar för genomförandet.

*Stadsledningskontoret bedömer* att de allmänna råden är väl utformade och ger god vägledning för hur föreskrifterna kan tillämpas i praktiken även om antalet allmänna råd skulle kunna utökas.

## Ställningstaganden

### 1 kap. Inledande bestämmelser

Kapitlet *lämnas utan synpunkt.*

### 2 kap. Organisatoriska säkerhetsåtgärder

**Ledningens ansvar för säkerhetsåtgärder**

*Stadsledningskontoret tillstyrker* kraven på ledningens ansvar för cybersäkerhetsarbetet och instämmer i vikten av att utbilda ledningspersoner i säkerhetsåtgärder och riskhantering enligt 6 § och 9 §. En hög kompetensnivå i ledningen bedöms vara avgörande för styrning, förankring och resurstilldelning. Vad gäller ledningens ansvar för säkerhetsåtgärder enligt 6 § *föreslår stadsledningskontoret* att ett allmänt råd vore lämpligt för att ge exempel på hur de angivna punkterna kan hanteras i praktiken.

*Stadsledningskontoret avstyrker* den föreslagna utformningen av 7 §. Bestämmelsen är alltför detaljerad och riskerar att låsa fast organisationer vid en viss struktur. Det bör vara upp till verksamhetsutövaren att bedöma hur funktionerna för samordning, informationsägarskap och systemägarskap organiseras och fördelas, utifrån verksamhetens storlek, komplexitet och befintliga ledningsstruktur. Begreppet ”samordnare” kan uppfattas som att en specifik person ska utses, medan avsikten snarare bör vara att säkerställa att en samordnande funktion finns. Stadsledningskontoret föreslår därför att paragrafen formuleras på en mer övergripande nivå och att exemplen på roller och deras mandat i stället förs till de allmänna råden.

*Stadsledningskontoret avstyrker* den föreslagna detaljnivån i bestämmelsen om vad ledningen ”minst” ska informera sig om enligt 8 §. Den uttömmande punktlistan riskerar att bli styrande på processnivå, tränga undan den riskbaserade ansatsen och försvåra en effektiv integrering i stadens ordinarie styrning och ledning. Det bör vara upp till verksamhetsutövaren att, utifrån sin riskbild och organisatoriska struktur, bedöma vad ledningen behöver informeras om och hur uppföljningen ska genomföras. De angivna punkterna bör i stället utgöra allmänna råd.

**Personalsäkerhet**

*Stadsledningskontoret tillstyrker* bestämmelserna i 10–11 §§ om personalsäkerhet och ser positivt på att även inhyrd personal omfattas. Det tydliggör att alla som hanterar verksamhetens information ska ges förutsättningar att arbeta säkert. Dock bedömer stadsledningskontoret att krav på inhyrd personals kompetens kan föranleda ökade kostnader i de fall där kompetensutvecklingsbehov inte tillgodoses löpande av leverantören.

**Informationsklassning**
*Stadsledningskontoret tillstyrker* bestämmelsen om informationsklassning enligt 13 §, men önskar ett förtydligande av hur begreppet *autenticitet* ska tolkas. Det framgår inte om autenticitet avses ingå som en del av riktighet eller om det ska bedömas som en separat parameter vid klassning. Ett klargörande är viktigt för att säkerställa en enhetlig tillämpning och jämförbarhet mellan verksamhetsutövare.

**Riskhantering**
*Stadsledningskontoret tillstyrker* kravet i 16 § på att arbetet med säkerhetsåtgärder ska följas upp regelbundet, men anser att kravet på uppföljning minst var tredje månad är alltför långtgående för samtliga system. En sådan uppföljningsfrekvens är rimlig för sektorskritiska system men blir administrativt betungande för mindre kritiska system och tar resurser från mer prioriterad riskhantering.
*Stadsledningskontoret föreslår* därför att uppföljningsfrekvensen görs riskbaserad och kopplas till systemens kritikalitet för att säkerställa en mer proportionerlig tillämpning.

**Krishantering**
*Stadsledningskontoret föreslår* att bestämmelsen i 21 § kompletteras, antingen genom ett tillägg eller ett allmänt råd, som tydliggör att krishantering vid cyberhändelser bör integreras i verksamhetsutövarens ordinarie krishanteringsprocess. En sådan precisering skulle bidra till en samlad hantering av kriser och motverka att parallella strukturer etableras.

Övriga paragrafer i kapitlet *lämnas utan synpunkt.*

## 3 kap. Tekniska och driftrelaterade säkerhetsåtgärder
*Stadsledningskontoret vill framhålla* att flera av bestämmelserna i kapitel 3 är omfattande och kan vara resurs- och kostnadsdrivande att genomföra, särskilt för verksamhetsutövare med stora och komplexa digitala miljöer. För att möjliggöra ett effektivt och proportionerligt införande bör samtliga krav tillämpas utifrån en riskbaserad ansats och med beaktande av systemens kritikalitet. Som exempel kan nämnas bestämmelserna om säkerhetsloggning, där det är rimligt att ställa höga krav på system med högt skyddsbehov, men mindre ändamålsenligt att tillämpa samma nivå för samtliga system. Den lägsta nivån bör vara hög, men samtidigt genomförbar och möjlig att tillämpa i praktiken.

*Stadsledningskontoret föreslår* att MSB ser över kapitlet i sin helhet och bedömer om bestämmelserna kan utformas så att de tydligare möjliggör en riskbaserad och proportionerlig tillämpning.

**Förvärv, utveckling och underhåll av system**
*Stadsledningskontoret tillstyrker* bestämmelsen i 2 §, men konstaterar att marknaden för certifierade system enligt EU:s cybersäkerhetsförordning ännu är outvecklad. Det bör därför framgå i föreskriften, eller de allmänna råden, att kravet tillämpas successivt i takt med att sådana certifieringar blir tillgängliga.

*Stadsledningskontoret tillstyrker* bestämmelsen om krav vid utkontraktering, men anser att paragrafen till del reglerar sådant som redan omfattas av andra bestämmelser i föreskriften.
Enligt 2 kap. 13 § ska informationsklassning genomföras innan information behandlas i system, vilket även inkluderar behandling hos leverantör. Kravet i denna paragraf blir därmed delvis överflödigt och riskerar att leda till dubbelreglering. *Stadsledningskontoret föreslår* att punkt 1 tas bort, eller alternativt omarbetas till ett allmänt råd. Vidare konstaterar stadsledningskontoret att kraven i föreskriften kommer att innebära ett betydande arbete med att säkerställa efterlevnaden i befintliga avtal för verksamhetsutövare med många leverantörsavtal.

*Stadsledningskontoret tillstyrker* bestämmelsen i 4 § men föreslår ett allmänt råd som förtydligar att kraven ska tillämpas proportionerligt och riskbaserat, så att mindre förändringar i system inte medför onödigt administrativt arbete.

**Behörighetshantering och autentisering**
*Stadsledningskontoret tillstyrker* kravet på regelbunden granskning av behörigheter enligt 16 §, men *föreslår* att frekvensen bör kunna anpassas utifrån systemens kritikalitet och risknivå för att undvika oproportionerlig administrativ belastning.

*Stadsledningskontoret tillstyrker* kravet på multifaktorsautentisering enligt 19 § för extern åtkomst och systemadministration, och konstaterar att det ligger i linje med stadens säkerhetsstrategi. *Stadsledningskontoret föreslår* att MSB kompletterar föreskriften eller de allmänna råden med vägledning om vilka kompensationsåtgärder som kan accepteras när multifaktorsautentisering inte kan införas av tekniska skäl, samt hur dessa bör dokumenteras och följas upp.

**Säkerhetsloggning och logganalys**
*Stadsledningskontoret tillstyrker* kravet i 23 § men efterfrågar förtydligande av vilka förväntningar som finns på att verksamhetsutövaren ska kunna upptäcka och reagera på hot i realtid. I sin nuvarande form riskerar bestämmelsen att vara missvisande. I sin nuvarande form riskerar bestämmelsen att vara missvisande.
*Stadsledningskontoret föreslår* därför att paragrafen omformuleras så att loggningen uttryckligen ska möjliggöra upptäckt av försök till, eller tecken på, obehörig åtkomst. En sådan formulering skulle bättre överensstämma med etablerad praxis för säkerhetsloggning, exempelvis enligt ISO 27002, och bidra till en mer ändamålsenlig tillämpning.

## 4 kap. Fysiska säkerhetsåtgärder
Kapitlet *lämnas utan synpunkt.*

## 5 kap. Sektorsspecifika säkerhetsåtgärder
**Offentlig förvaltning**
*Stadsledningskontoret tillstyrker* kravet på att verksamhetsutövare ska identifiera och hantera behovet av kriskommunikation enligt 1 §. För offentlig förvaltning anges

Rakel och SGSI som system för kriskommunikation. *Stadsledningskontoret konstaterar* att hanteringen av frågan kan vara komplex med hänsyn till kommuners olika förutsättningar och tillgång till dessa system. Formuleringen i förslaget – att verksamhetsutövaren ska ”identifiera och hantera behovet” – indikerar att kravet inte är absolut. *Stadsledningskontoret föreslår* att detta förtydligas ytterligare i föreskrifterna för att undvika tveksamhet vid tolkning och tillämpning.

## 6 kap. Undantag

Kapitlet *lämnas utan synpunkt.*

## Konsekvensutredning rörande föreskrifter om säkerhetsåtgärder och utbildning

*Stadsledningskontoret tillstyrker* bedömningen att kostnaderna för införande av säkerhetsåtgärder kommer att variera beroende på verksamhetens art, omfattning och cybersäkerhetsmognad, och att det är svårt att tydligt separera kostnader som uppstår till följd av cybersäkerhetslagen från övrigt cybersäkerhetsarbete.

*Stadsledningskontoret efterfrågar* samtidigt en mer konkret bedömning av de investeringar som kan förväntas behövas, exempelvis för säkerhetssystem, infrastruktur, segmentering och redundans. Vidare önskas en tydligare uppskattning av möjliga återkommande driftskostnader, såsom licenser för säkerhetsverktyg och extern support.

*Stadsledningskontoret föreslår* även att konsekvensutredningen förtydligar om befintliga system behöver uppgraderas samt inom vilken tidsram sådana åtgärder i så fall bör genomföras.