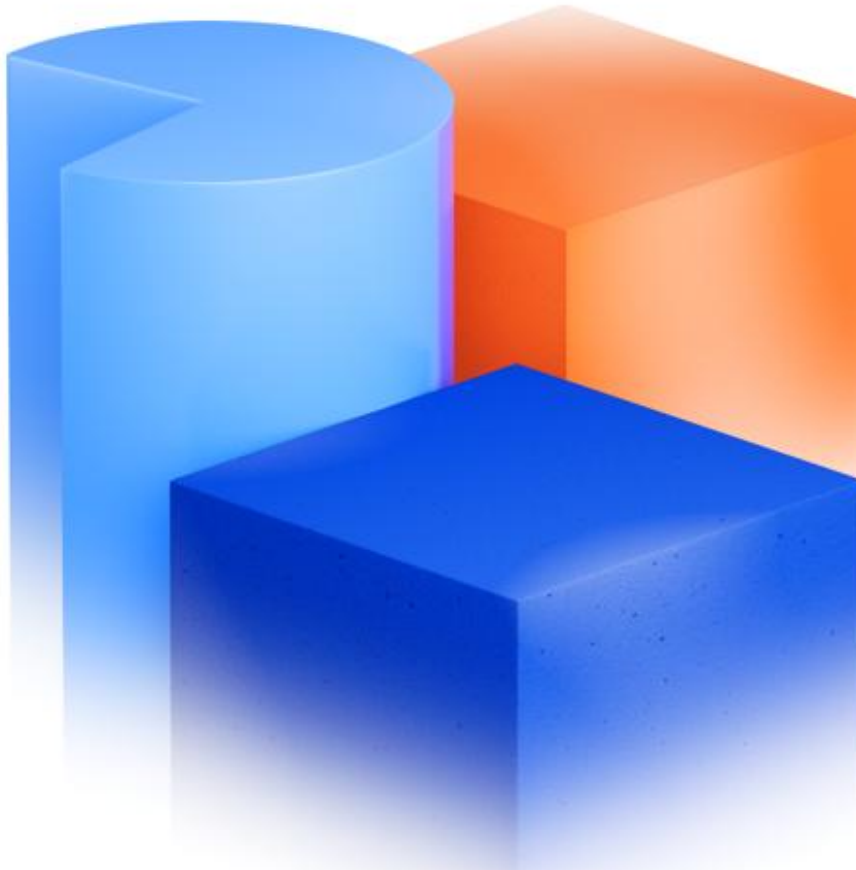
[Infoga bild här] [Infoga bild här]

# Informationssäkerhetspolicy

261101



POLICY

Fastställd av GD: 12 oktober 2026
Träder i kraft: 1 november 2026
Upphör att gälla: 1 november 2029

Ansvarig: Terése Kalinski
Dnr: SCB2026/747
Version: 1

# Informationssäkerhetspolicy

SCB:s verksamhet, från det att företag, organisationer och individer tillfrågas om uppgifter till dess att resultaten redovisas på SCB:s webbplats eller levereras som ett resultat av ett uppdrag, innebär en omfattande hantering av information. När SCB samverkar med andra svenska och utländska myndigheter och organisationer ställs också krav på en god informationssäkerhet.

Det är därför av största vikt att vi hanterar informationssäkerhetsfrågor på ett förtroendeingivande och metodiskt sätt. Den information som SCB förfogar över och hanterar är en viktig strategisk tillgång som måste skyddas.

Med information avses alla slags uppgifter som används i verksamheten oavsett om uppgiften är muntlig eller skriftlig och oberoende av hur den bearbetas, lagras eller transporteras.

**Generella krav**

- Huvuddelen av säkerhetsarbetet ska ske hos avdelningar, enheter och sektioner, d v s hos dem som närmast hanterar informationen.
- Säkerhetsarbetet ska utföras systematiskt och utgå från myndighetens regelverk för informationssäkerhet.
- All information och alla informationssystem ska ha ett tydligt ägarskap och utpekat ansvar inom myndigheten.
- Informationssäkerhet ska integreras i förvaltning, projekt- och utvecklingsarbete och ingå som en naturlig del i det dagliga arbetet.
- All personal ska ha kunskap om och tillämpa gällande riktlinjer för informationssäkerheten gällande de egna arbetsuppgifterna. Den närmaste chefen ska ge stöd och vägledning i detta.
- Personalen ska regelbundet utbildas i säkerhet.
- Förväntningar, utbildningar och krav avseende informationssäkerhet gäller både egna anställda såväl företag och personal som anlitas för särskilda uppdrag.
- Kravställan och uppföljning av säkerhet ska ske vid upphandlingar och annan extern samverkan.
- Tilldelning och borttagande av behörigheter ska ske i enlighet med fastställda riktlinjer. Användare ska endast ha de behörigheter som krävs för arbetsuppgifterna.
- All personal ska informeras om att deras aktiviteter i informationssystemen kan övervakas och följas upp.
- Informationssäkerhetsarbetet ska bedrivas riskbaserat.
- Risk- och sårbarhetsanalyser ska genomföras inom myndigheten, varefter det ska vidtas nödvändiga åtgärder för att se till att information har rätt skydd.

- Det ska finnas kontinuitetsplaner för särskilda händelser och kriser för prioriterade verksamheter.
- Det ska finnas rutiner för hantering och uppföljning av säkerhetsincidenter.
- Efterlevnad av riktlinjer och krav ska granskas genom återkommande uppföljningar och kontroller.

**Myndighetens ledningssystem för informationssäkerhet (SCB LIS)**

Informationssäkerhetsarbetet på myndigheten ska styras utifrån krav som utgår från SCB LIS. Myndighetens säkerhetsorganisation förvaltar SCB LIS. Dessa ska regelbundet följas upp och uppdateras vid behov.

SCB LIS består av följande:

- Informationssäkerhetspolicy.
- Riktlinjer.
- Instruktioner.
- Utbildningsmaterial.
- Checklistor.
- Mallar.