

Program

Plan

• **Policy**

Riktlinjer

Borås Stads
**Policy för
informationssäkerhet
och dataskydd**

Borås Stads styrdokument

Planerande

PROGRAM – vägval, verksamheter och metoder i riktning för att nå målen i Borås
PLAN – aktiviteter, tidsram och ansvar

Normerande

POLICY – Borås Stads hållning
RIKTLINJER – rekommenderade sätt att agera

Fastställt av: Kommunfullmäktige
Datum: **2024-12-12**
För revidering ansvarar: Kommunstyrelsen
Dokumentet gäller för: Alla nämnder och bolag
Dnr: KS 2024-00396
Dokumentet gäller till och med: 2028

Globala målen

Detta styrdokument bidrar till följande globala mål:



Innehåll

1 Inledning	4
1.1 Informationssäkerhet och dataskydd	4
1.2 Mål och metod	4
2 Ansvar för informationssäkerhet och dataskydd	6
2.1 Grundprincip	6
2.2 Ansvar	6

1 Inledning

Borås Stads policy för informationssäkerhet och dataskydd styr kommunens inriktning och utgör ett ramverk för arbetet med informationssäkerhet och dataskydd i koncernens nämnder och bolag. Policyn riktar sig till samtliga medarbetare, förtroendevalda och övriga inom kommunens verksamheter som hanterar organisationens information. Policyn kompletteras med underliggande styrdokument som konkretiserar intentionerna i detta dokument.

Inom Borås Stads förvaltningar och bolag hanteras information som är viktig för verksamheten, samhället och invånarna. Felaktig informationshantering och brister i informationssäkerhet och dataskydd kan få stora konsekvenser för organisationens förmåga att bedriva sin verksamhet, äventyra samhällets motståndskraft vid kriser och incidenter, samt skada den enskildes integritet. Kommunens information ska därför skyddas från förlust av:

- **Konfidentialitet** – så att informationen inte röjs eller tillgängliggörs för obehöriga.
- **Riktighet** – så att informationen inte förändras på oönskat sätt, vare sig det sker obehörigen, av misstag eller på grund av en störning.
- **Tillgänglighet** – så att informationen är tillgänglig för behöriga när den behövs.

1.1 Informationssäkerhet och dataskydd

Borås Stads arbete med informationssäkerhet ska bedrivas riskbaserat, systematiskt, ändamålsenligt och effektivt genom ett ledningssystem för informationssäkerhet och dataskydd i enlighet med standarderna ISO/IEC 27001 och ISO/IEC 27701.

Med informationssäkerhet avses förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet vid hantering av information. Informationssäkerhet omfattar administrativ säkerhet och teknisk säkerhet, till exempel it-säkerhet och cybersäkerhet. Dataskydd definieras som skyddet av den personliga integriteten för individer genom att personuppgifter hanteras lagenligt och korrekt.

Genom denna policy åtar sig Borås Stad att dels ständigt förbättra organisationens ledningssystem för informationssäkerhet och dataskydd och dels uppfylla tillämpliga krav inom området.

1.2 Mål och metod

Borås Stads strategiska informationssäkerhetsmål är att

- kommunens information i alla lägen är kartlagd, klassad och har ett ändamålsenligt skydd
- informationssäkerhetsrisker som identifieras i organisationen hanteras effektivt
- organisationen har en god informationssäkerhetskultur där medarbetare och chefer har tillräcklig kompetens, tar ansvar, efterlever styrdokument och rapporterar brister
- kommunen har förmåga att bedriva sin verksamhet även vid incidenter eller störningar
- organisationen utvärderar effekten av sitt ledningssystem genom mätning och uppföljning samt interna revisioner.

För att nå målen ska respektive nämnd och bolag inom koncernen

- Säkerställa att resurser finns i den egna organisationen för ett effektivt och systematiskt arbete med informationssäkerhet och dataskydd, med fokus på ständiga förbättringar.
- identifiera och dokumentera tillämpliga krav på informationssäkerhet och dataskydd samt säkerställa att organisationen efterlever dessa.
- kartlägga hur organisationens information hanteras och lagras med utgångspunkt i verksamhetens processer.
- säkerställa att verksamhetens information skyddas på lämplig nivå utifrån klassningar, riskanalyser och organisationens riskacceptans.
- utse ägarskap för information och informationstillgångar i organisationen.
- kartlägga verksamhetens personuppgiftsbehandlingar och säkerställa ett gott dataskydd så att personuppgifter hanteras på ett sätt där individens rättigheter tillvaratas lagenligt och korrekt.
- ha ett kontinuitetsarbete så att verksamheten kan bedrivas även vid en allvarlig incident eller störning.
- kontinuerligt utbilda medarbetare inom informationssäkerhet och dataskydd.

De strategiska informationssäkerhetsmålen ska omsättas i kortsiktiga mål.

2 Ansvar för informationssäkerhet och dataskydd

2.1 Grundprincip

Ansvar för informationssäkerhet följer det ordinarie verksamhetsansvaret och sträcker sig på så sätt från den politiska ledningen, genom tjänstepersonsledningen och till varje enskild medarbetare. Den som är ansvarig för en viss verksamhet (förvaltning, avdelning, enhet, process, projekt och så vidare) är också formellt ansvarig för informationssäkerheten i verksamheten.

2.2 Ansvar

Kommunfullmäktige fastställer informationssäkerhetspolicy och uttrycker därigenom viljeinriktningen för kommunens arbete med informationssäkerhet och dataskydd.

Kommunstyrelsen verkställer Kommunfullmäktiges beslut och har övergripande ansvar för att leda, samordna och utveckla kommunens informationssäkerhetsarbete. Kommunstyrelsen ansvarar också för att ta fram styrdokument för stöd och reglering av koncernens informationssäkerhetsarbete samt att kommunens ledningssystem för informationssäkerhet och dataskydd är effektivt och ändamålsenligt. Kommunstyrelsen är personuppgiftsansvarig och utser dataskyddsombud för sina verksamheter.

Nämnder och kommunala bolag säkerställer att informationssäkerheten håller rätt och relevant nivå inom deras respektive verksamheter. Nämnderna och bolagen är personuppgiftsansvariga för sina verksamheter och utser dataskyddsombud. Respektive förvaltningschef/bolagschef ansvarar för att informationssäkerhetsarbetet bedrivs i linje med fastställd policy för informationssäkerhet och dataskydd.

Chefer är ansvariga för informationssäkerheten inom sin egen verksamhet.

Medarbetare och förtroendevalda hanterar kommunens informationstillgångar och har ett ansvar att följa kommunens informationssäkerhetspolicy och underliggande styrdokument för informationssäkerhet.



BORÅS
STAD

Postadress 501 80 Borås **Besöksadress** Stadshuset, Kungsgatan 55
Telefon 033-35 70 00 **e-post** boras.stad@boras.se **Webbplats** boras.se