DIREKTIV FÖR IT OCH DIGITALISERING SAMT INFORMATIONS- OCH CYBERSÄKERHET

Syftet med Lisebergs *direktiv för IT och digitalisering samt informations- och cybersäkerhet* är att ange hur verksamhetsutveckling ska stödjas genom digitalisering och dess grundläggande möjliggörare, IT. Med digitalisering avses i detta direktiv utveckling av verksamhet, arbetssätt och tjänster med stöd av digital teknik. Informationen ska behandlas på ett säkert sätt, och detta direktiv skapar förutsättningar för ett systematiskt och långsiktigt informations- och cybersäkerhetsarbete.

Lisebergs *direktiv för IT och digitalisering samt informations- och cybersäkerhet* baseras på Göteborgs Stads *riktlinje för styrning, samordning och finansiering för digital utveckling och förvaltning* samt Göteborgs Stads *riktlinje för informations- och cybersäkerhet*.

Begrepp och definitioner
För att skapa en enhetlig förståelse i organisationen används följande begrepp i detta direktiv och tillhörande anvisningar:

- **IT-resurs**: Datorer, mobila enheter, nätverk, servrar, system, programvaror och kringutrustning som används i verksamheten.
- **Digital lösning**: Digital tjänst, system, applikation eller arbetsprocess som stöds av digital teknik.
- **IT-tjänst**: En av Liseberg tillhandahållen funktion eller lösning som stödjer verksamheten.
- **Informationstillgång**: Information och de resurser som hanterar informationen. Begreppet omfattar digital, fysisk och muntlig information.
- **Informationssäkerhet**: Skydd av information avseende konfidentialitet, riktighet och tillgänglighet.
- **IT-säkerhet**: Den tekniska delen av informationssäkerheten i IT-system och IT-miljöer.
- **Cybersäkerhet**: Den del av IT-säkerheten som avser att förebygga, upptäcka och hantera digitala hot som intrång, skadlig kod och sårbarheter.

Antagen den XX månad 202x av styrelsen för Liseberg

Principer för IT och digitalisering:

- Vid behov av nya IT-tjänster ska valet av lösning i första hand utgå från verksamhetsbehovet. Behovet ska tillgodoses genom att befintliga IT-tjänster antingen återanvänds, anskaffas från extern part eller utvecklas av Liseberg.
- Vid införande av nya digitala förmågor, exempelvis digitala tjänster, processer eller arbetssätt, ska långsiktighet och helhet balanseras mot ekonomi.
- Övergripande prioritering av IT- och digitaliseringsarbetet ska ske i Ledningsgrupp Digitalisering för att säkra finansiering, skapa en samordnad färdplan samt synliggöra beroenden till andra initiativ och IT-tjänster i Lisebergs digitala ekosystem, det vill säga samverkan och beroenden mellan Lisebergs digitala lösningar och IT-tjänster.
- Liseberg ska följa utvecklingen av nya lagar och säkerställa efterlevnad av tillämpliga lagar och regler inom området, såsom AI-förordningen (AI Act), dataskyddsförordningen (GDPR) och cybersäkerhetslagen (CSL).
- För varje IT-tjänst ska det finnas en förvaltningsorganisation med representanter från både IT-avdelningen och verksamheten, med ansvar för förvaltning och vidareutveckling.
- Liseberg ska, när det är möjligt, använda befintliga teknologier och plattformar för att effektivisera kompetensförsörjning och möjliggöra kostnadsoptimering.
- Liseberg bör använda Göteborgs Stads kommungemensamma tjänster i den mån det är möjligt och där det passar verksamhetsbehovet.
- Digitalisering är inte ett mål i sig utan bör genomföras med definierad nytta och leda till värde.

Principer för informations- och cybersäkerhet:

- Liseberg ska bedriva ett systematiskt informationssäkerhetsarbete för att skydda information utifrån dess behov.
- Liseberg ska arbeta riskbaserat med cybersäkerhet för att skydda IT-miljöer och digitala lösningar mot hot, sårbarheter och obehörig åtkomst.
- Informationssäkerhet innebär skydd av informationstillgångar avseende:
    - *Konfidentialitet*, att information inte tillgängliggörs eller avslöjas för obehöriga.
    - *Riktighet*, inklusive autenticitet, att information skyddas mot oönskad förändring, att information är korrekt, inte manipulerad, förstörd eller förfalskad samt kommer från pålitlig källa.
    - *Tillgänglighet*, att information är tillgänglig och användbar när det behövs.
- Informationssäkerhetsincidenter, det vill säga händelser som kan påverka konfidentialitet, riktighet eller tillgänglighet, ska anmälas och hanteras skyndsamt.
- Lisebergs styrelse har det yttersta ansvaret för informationssäkerheten, inklusive hantering av identifierade risker, och ska hållas uppdaterad om arbetet samt väsentliga händelser inom området, exempelvis större incidenter och väsentliga riskförändringar.

Antagen den XX månad 202x av styrelsen för Liseberg

- IT-avdelningen ska agera i rollen som incidenthanterare och informationssäkerhetssamordnare, det vill säga samordna och stödja informationssäkerhetsarbetet.
- Kontinuitet och återställningsförmåga. Liseberg ska säkerställa att verksamhetens kritiska processer kan upprätthållas även vid störningar i IT-miljön. Informations och cybersäkerhetsarbetet ska därför omfatta etablerade kontinuitetsplaner och reservrutiner i verksamheten, samt förmåga att säkerhetskopiera och återställa information på ett kontrollerat sätt vid incidenter eller avbrott.

Relaterade styrdokument
Se Lisebergs *säkerhetsdirektiv* för mer information om relationen mellan informationssäkerhet och Lisebergs säkerhetsarbete.

Se Lisebergs direktiv för *hantering av personuppgifter och dataskydd* för vägledning om inom vilka geografiska områden Liseberg bör behandla personuppgifter. Direktivet preciserar exempelvis att Liseberg vid upphandling av digitala lösningar eller tjänster ska ansvara för kundrelationen samt hantering av personuppgifter. Det beskriver också att digitala lösningar bör utformas så att de inte exkluderar någon målgrupp.

Se Lisebergs *hållbarhetsdirektiv* för mer information om hur Liseberg ska arbeta resurseffektivt med fokus på att minska miljö- och klimatpåverkan, vilket berör val av hårdvara och mjukvara.

Antagen den XX månad 202x av styrelsen för Liseberg