Informationssäkerhetspolicy

Dnr 44-2024

Fastställd av direktionen 2024-05-27 § 16

Jämtlands
Gymnasieförbund

Innehållsförteckning

1 Inledning

Inom Jämtlands Gymnasieförbund används informationsteknik (IT) för att stödja, utveckla och effektivisera den administrativa såväl som den pedagogiska verksamheten. Att säkerställa hög tillgänglighet, relevant information och ändamålsenliga system är avgörande för förbundets resultat, liksom att förbundets informationstillgångar skyddas mot eventuella hot – interna eller externa, avsiktliga eller oavsiktliga.

Med informationstillgångar menas både information (data) som sådan och de resurser som används för att hantera informationen (IT-system, nätverk, servrar och arbetsstationer inklusive mobila enheter som surfplattor och mobiltelefoner).

1.1 Syfte

Syftet med informationssäkerhetspolicyn är att beskriva hur Jämtlands Gymnasieförbund arbetar för att säkerställa att all information hanteras på ett säkert och effektivt sätt. Genom att arbeta systematiskt med informationssäkerhet kan förbundet åstadkomma bättre kvalitet i verksamheten och ökad trovärdighet.

Policyn omfattar förbundets alla enheter och centrala funktioner och gäller för samtliga anställda, och förtroendevalda samt för elever, vårdnadshavare och övriga intressenter som använder förbundets informationstillgångar.

1.2 Utgångspunkter

Skyddet av information ska tillgodose de lagkrav som ställs på förbundet vad gäller myndighetsutövning och de åtaganden som förbundet i övrigt har gentemot samarbetspartners och övriga intressenter. Utgångspunkten är att var och en har ansvar för att skydda den information som man disponerar över utifrån givna riktlinjer och instruktioner. Arbetet med informationssäkerhet utgår från följande principer:

Principer för informationssäkerhet	
Tillgänglighet	Förbundets anställda, elever och förtroendevalda samt övriga intressenter ska ha tillgång till den information de behöver, när de behöver den och på förväntat sätt.
Riktighet	Vår information ska vara korrekt och tillförlitlig. Informationen ska skyddas mot oönskade förändringar och fel.
Konfidentialitet / sekretess	Vår information ska inte göras tillgänglig för eller avslöjas för obehöriga.
Spårbarhet	Aktiviteter i kritiska system ska kunna härledas i efterhand. Vi ska kunna visa vad som har hänt och vem som har gjort vad i våra informationssystem.

Förbundets arbete med informationssäkerhet ska omfatta såväl organisatoriska åtgärder som fysiska och logiska skyddsåtgärder (ansvarsfördelning, utbildning, riskanalys, behörighetsregler, säkrad, driftsmiljö, åtkomstskydd i datorer, säkerhetskopiering, etc.) Arbetet ska utföras på

ett strukturerat sätt i enlighet med denna policy och förbundets övriga fastställda riktlinjer och rutiner som är relevanta för arbetet med informationssäkerhet.

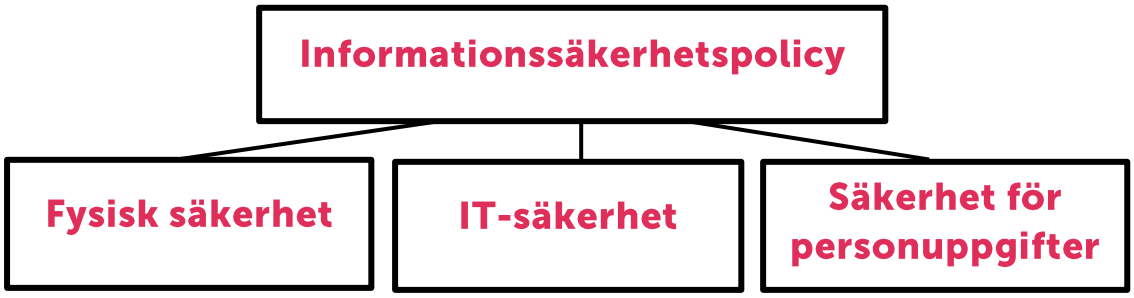
1.3 Målsättning

Det övergripande målet med IT-säkerhetsarbete är att minimera riskerna för störningar i förbundets olika verksamheter, på grund av fel i eller felaktig användning av ett eller flera IT-system, samt att verksamheternas information och enskildas integritet skyddas.

Förbundets arbete med informationssäkerhet ska resultera i kostnadseffektiva och behovsanpassade säkerhetsåtgärder. Åtgärder för att säkra informationen ska i så liten utsträckning som möjligt vara ett hinder för utvecklingen av olika tekniska lösningar. Samtidigt ska all verksamhetsutveckling som innebär att information hanteras med hjälp av digital teknik ske på ett sätt som inte äventyrar förbundets principer för informationssäkerhet.

1.4 Inriktning

Informationssäkerhetsarbetet i Jämtlands gymnasieförbund kan delas in tre huvudområden: fysisk säkerhet, IT-säkerhet samt säkerhet för personuppgifter. Denna övergripande informationssäkerhetspolicy kompletteras med specifika styrdokument och riktlinjer på verksamhetsnivå.



2 Ansvar

Ansvaret för arbetet med informationssäkerhet fördelas enligt följande:

Förbundsdirektion	Ansvarar för förbundets ledning och samordning. Direktionen fastställer informationssäkerhetspolicyn och är även personuppgiftsansvarig enligt Dataskyddsförordningens bestämmelser.
Förbundsdirektör	Ansvarar för verksamhetens organisation och verkställighet av beslut. Ansvarar för att hålla direktionen informerad om förbundets verksamhet. Fastställer riktlinjer och handlingsplaner för verksamheten och ansvarar för förbundets övergripande kvalitetsarbete. Beslutar om inköp av förbundsövergripande verksamhetssystem.

IT-chef	Ansvarar för förbundets IT-säkerhet (lagring, servrar, e-post, telefonsystem, intranät mm.) samt för att tillgängliggöra information om förbundets IT-säkerhetsarbete internt och externt. Beslutar om behörigheter i olika system och ansvarar även för att förbundet lever upp till gällande lagar och externa krav på förbundets informationssystem. Ansvarar även för strategisk planering av förbundets IT-resurser med avseende på teknisk utveckling, tillgänglighet och säkerhet. IT-chefen är sammankallande för IT-säkerhetsrådet.
Intendent	Ansvarar för fysisk säkerhet (inklusive inbrottslarm, passersystem, brandvarnare m.m.)
Dataskyddsombud	Utses av direktionen och har en rådgivande och övervakande roll i frågor som rör skyddet av personuppgifter. Ansvarar för registerförteckningen och förbundets kontakter med Integritetsskyddsmyndigheten (IMY).
Tekniker	Ansvarar för att säkerställa tillgänglighet och funktionalitet i förbundets IT-resurser och för att hantera felanmälningar.
IKT-pedagog	Ansvarar för utbildningsinsatser och kompetenshöjande åtgärder inom förbundets olika verksamhetssystem och tekniska hjälpmedel.
Systemansvariga	Har det operativa ansvaret för att beslutade åtgärder genomförs och för att giltig dokumentation runt IT-systemen finns.
Chefer	Ansvarar för att underställd personal är känner till innehållet informationssäkerhetspolicyn och för att riktlinjer och rutiner på IT-området efterlevs i verksamheten. Beslutar om inköp av digitala verktyg i den egna verksamheten.
Rektorer	Ansvarar för att kommunicera riktlinjer och rutiner på IT-området som gäller elever.
Samtlig personal	Ansvarar för att aktivt arbeta för en ökad IT-säkerhet. All personal är skyldiga att påtala brister i säkerheten till närmaste ansvarig och misstanke om säkerhetsincidenter eller personuppgiftsincidenter.
IT-säkerhetsråd	Fungerar som IT-chefens ledningsgrupp i frågor som rör förbundets IT-säkerhet. Ansvarar för det systematiska kvalitetsarbetet med avseende på IT-resurser, arbetssätt och informationssäkerhet. Ansvarar för att ta fram riktlinjer och rutiner för verksamheten. I IT-säkerhetsrådet ska ingå IT-chef, dataskyddsombud och intendent.
IT-strategigrupp	Ansvarar för det systematiska kvalitetsarbetet med avseende på funktionalitet, effektivitet och strategisk utveckling av förbundets IT-miljöer. IT-chefen är sammankallande.

3 Generella riktlinjer

3.1 Medvetenhet

Alla användare av förbundets IT-resurser ska göras medvetna om vilka informationstillgångar som finns inom organisationen och vilka risker som finns kopplade till dessa. Informationssäkerhetspolicyn och underliggande riktlinjer på IT-området ska göras kända i verksamheten.

3.2 Systematiskt kvalitetsarbete

Förbundets IT-resurser ska anpassas till verksamhetens behov. Utvecklingen av förbundets IT-miljöer ska ske på ett systematiskt sätt och ta hänsyn till samhällsutvecklingen, teknikutvecklingen och kostnader. Det systematiska kvalitetsarbetet ska inriktas på funktionalitet och säkerhet där båda aspekterna ska ges lika stort utrymme. Utveckling av teknik ska ske parallellt med utveckling av organisationens kompetens att använda tekniken på avsett vis.

3.3 Informationsklassning och riskbedömning

För att avgöra vilket skydd som behövs och hur olika typer av information får hanteras, ska känslig och/eller väsentlig information som hanteras inom förbundet klassificeras. Tillsammans med klassificeringen ska riskbedömningar avgöra vilka säkerhetsåtgärder som behövs för respektive informationstyp. Riskbedömningar ska genomföras löpande samt alltid vid större förändringar.

3.4 Åtkomst och behörighet

Förbundets IT-resurser ska skyddas mot obehörig åtkomst med brandväggar, antivirusprogram och olika typer av skalskydd som begränsar fysisk åtkomst till serverrum och andra IT-resurser.

Information i IT-system ska skyddas med antingen någon form av autentisering eller genom kryptering. Förbundet ska arbeta aktivt med behörigheter i IT-system och göra medvetna bedömningar av vilka användare som ska ha tillgång till systemen, för att minska mängden information som exponeras till olika användargrupper. Alla beslut och inställningar som rör användaråtkomst ska regleras centralt i IT-miljön.

Personal får inte ta del av eller bereda sig tillgång till information utifrån privata intressen.

3.5 Loggning och uppföljning

Uppföljning och kontroll, bland annat genom granskning av loggar, ska vara en naturlig del i förbundets informationssäkerhetsarbete. Det ska finnas möjligheter för att övervaka loggar kontinuerligt och ett ändamålsenligt system där man kan söka fram händelser och granska loggar på ett effektivt sätt.

3.6 Säkerhetsincidenter

Säkerhetsincidenter och personuppgiftsincidenter ska rapporteras och utredas enligt fastställda rutiner. Det ska finnas system för avvikelsehantering, det vill säga rapportering av

säkerhetsproblem och systematiskt arbete med åtgärder som ska förebygga eller minska effekten av framtida incidenter.

Den som upptäcker brister i informationssäkerheten måste uppmärksamma sin chef eller säkerhetsfunktionen på det. Alla medarbetare måste också rapportera händelser som kan göra att våra informationstillgångar utsätts för risker.

Förbundet ska ha en plan för hur verksamheten ska kunna upprätthållas och återställas i händelse av en allvarlig incident eller kris.

3.7 Externa system och molntjänster

I de fall förbundet använder system och tjänster från externa leverantör ska tjänsteavtal och i förekommande fall personuppgiftsbiträdesavtal upprättas som säkerställer att leverantören lever upp till lämplig säkerhet och följer gällande lagstiftning och överenskomna instruktioner.

3.8 Införande av nya system

Vid införande av nya system ska hänsyn tas till behov, kostnader och olika aspekter av informationssäkerhet och organisationens förmåga att tillhandahålla service och support. I möjligaste mån ska befintliga system användas. Nya system ska i första hand ersätta system som tas ur bruk eller fylla en funktion som inte kan tillgodoses i befintliga system.

IT-säkerhetsfrågorna ska beaktas redan vid upprättandet av kravspecifikation och anskaffning av informationssystem.

4 Revidering av dokumentet

Denna policy ska revideras vid behov i samband med förändringar i verksamhetens inriktning och omfattning.

Inom ramen för det systematiska kvalitetsarbetet ska en årlig revision av samtliga styrdokument och rutiner på informationssäkerhetsområdet genomföras.