



UMEÅ UNIVERSITET

POLICY - IT-STRATEGI VID UMEÅ UNIVERSITET

Typ av dokument:	Policy
Datum:	2025-10-24
Dnr:	FS 1.1-2035-25
Beslutad av:	Universitetsdirektör
Giltighetstid:	2025-12-01 - tills vidare
Område:	Lokaler, it, miljö och säkerhet
Ansvarig förvaltningsenhet:	Enheten för IT-stöd och systemutveckling
Ersätter dokument:	Denna IT-strategi ersätter Umeå universitets IT-strategi beslutad 2009-11-05, Dnr 100-802-09



Innehåll

1.	Beskrivning	1
1.1	Interna styrdokument som påverkar	1
2.	Bakgrund.....	2
2.1	Nuläge.....	2
2.2	Mål.....	2
3.	Övergripande strategi	3
3.1	Upphandling och licenser.....	6
3.2	Användarstöd	6
3.3	Identitets och behörighetshantering	7
3.4	Användande av publika molntjänster	7
3.5	Användande av AI-tjänster	8
3.6	Användande av lokala IT-tjänster	8
3.7	Sammanhållen IT-arkitektur	9
4.	IT-strategi som stöd till forskning	9
5.	IT-strategi som stöd till utbildning.....	10
6.	IT-strategi som stöd till administration	11
7.	Strategi för cybersäkerhet.....	12
7.1	Informationshantering.....	12
7.2	Skydd av informationstillgångar	12
7.3	Loggning/övervakning	13
7.4	Security Operations Center (SOC)	13
7.5	Incidenthantering.....	13
7.6	Backup och restore	14
7.7	Kontinuitetshantering	14
8.	Framtida utveckling och innovation.....	15
9.	Kompetensförsörjning och omvärldsbevakning.....	15



1. Beskrivning

I dagens digitaliserade samhälle är en robust IT-strategi avgörande för att Umeå universitet ska kunna uppnå sina mål och visioner. En väl genomarbetad IT-strategi möjliggör inte bara en effektiv och säker hantering av information, utan stödjer också universitetets kärnverksamhet forskning, utbildning och administration. Denna IT-strategi syftar därför till att skapa en hållbar, säker och tillgänglig IT-miljö som främjar forskningens och utbildningens kvalitet såväl i dag som i framtiden.

IT-strategin beskriver hur universitetsgemensamma IT-miljöer, -system, och IT-säkerhetsarbete, med hänsyn till gällande lagstiftning och föreskrifter, ska stötta universitetets verksamheter på ett tryggt, säkert, effektivt och ändamålsenligt sätt. Allt för att hjälpa medarbetare och studenter i sin vardag.

IT-system, -tjänster och stöd ska, i den mån det är möjligt, förenkla och underlätta arbetsprocesserna.

Utöver detta beskriver IT-strategin övergripande universitetets långsiktiga mål med hur inköp, utveckling och förvaltning av IT-system ska gå till, hur universitetet ser på användandet av såväl publika molntjänster, lokala IT-system, IT-säkerhetsfrågor och mycket annat. Detta strategidokument ska ge en tydlig inblick i vilka satsningar på övergripande nivå som kommer att behöva genomföras inom IT de närmaste åren.

Mål och strategier inom IT ska revideras vartannat år för att kontinuerligt ta hänsyn till de förändringar som sker.

1.1 Interna styrdokument som påverkar

I arbetet med framtagandet av strategier inom IT har följande dokument beaktats:

- Vision för Umeå universitet Dnr: FS 1.1-96-19
- Umeå universitets digitaliseringsstrategi Dnr: FS 1.1-1891-23
- Umeå universitets policy för e-lärande, 2016-04-05 Dnr: FS 1.1-377-14
- Informationssäkerhetspolicy för Umeå universitet, 2018-06-13 Dnr: FS 1.1.2-1833-14
- Anvisning anskaffning av system eller molntjänst vid Umeå universitet Dnr: FS 1.1-1257-23

Särskild vikt har lagts på den digitaliseringsstrategi som framtagits vid universitetet då den pekar ut de viktiga områden som behöver beaktas under den digitaliseringsprocess som pågår och där IT spelar en mycket viktig roll.

Digitaliseringsstrategin pekar på fem viktiga områden: ledning, infrastruktur, kompetens, trygghet och innovation. Denna IT-strategi tar allt detta i beaktande med tonvikt på att skapa förutsättningar för trygghet, infrastruktur och även innovation.



2. Bakgrund

2.1 Nuläge

Användarna och verksamheten vid Umeå universitet

Universitetets IT-stöd ska vara robust och tillförlitligt och stödja kärnverksamheten vid Umeå universitet att nå sina mål inom forskning och utbildning. För att det ska uppnås krävs såväl att IT-tjänsterna förvaltas väl samt har ett framåtsyftande fokus som hela tiden speglar universitetets uppdrag. Med universitetsgemensam IT avses de system eller funktioner som erbjuds till hela universitetet och som företrädesvis finansieras via anslag.

Digitaliseringen har de senaste åren tagit fart ordentligt, och inte minst den tidigare nedstängningen av undervisning på campus i fotspåren av covid-19 har påskyndat denna process ytterligare. Som digitaliseringsstrategin pekar på så är trygghet för användarna en viktig fråga. När digitaliseringsgraden ökar, växer även de digitala hoten mot universitetet. Hoten kan handla om obehörig åtkomst, identitetsstöld, dataintrång och sabotage, informationsstöld samt överbelastningsattacker av olika slag. Om hoten realiseras kan det få långtgående negativa effekter för universitetet. Regeringen har uppmärksammat dessa reella hot och ställer i regleringsbrevet till universitet och högskolor krav på skärpt hantering av rapportering, analys, åtgärder med mera kopplat till cybersäkerhet.

Alla som verkar vid Umeå universitet ska känna sig trygga med de IT-tjänster som universitetet tillhandahåller. En viktig del i denna trygghet är att IT- och informationssäkerheten är väl utvecklad och utformad. Stöd ska tillhandahållas för att verksamheten ska kunna följa regler och lagar utan att det upplevs som ett hinder i arbetet. Detta innebär allt från stöd som underlättar det grundläggande administrativa arbetet i vardagen till funktioner som säker hantering och lagring av känslig information.

Sektorn och samhället

Universitetet verkar i en konkurrensutsatt omgivning och omvärlden ska uppfatta att IT-stödet och den digitala arbetsplatsen vid Umeå universitet är väl anpassat till uppdraget, är enhetlig och logiskt samt att det genomförs kostnadseffektivt i förhållande till nyttan. Utöver detta tillkommer även andra faktorer att beakta som till exempel vilka sektorsgemensamma tjänster som finns tillgängliga, vad andra lärosäten i sektorn gör, vilka leverantörer som är aktiva och som kan leverera bra produkter på lång sikt med mera.

2.2 Mål

Den IT-miljö som erbjuds vid Umeå universitet ska:

- a) **Främja** att kärnverksamheten vid Umeå universitet når sina mål inom forskning och utbildning. Det innebär exempelvis att säkerställa att universitetets gemensamma IT-miljö tillhandahåller relevant stöd för att lösa de flestas behov samt ger stöd för effektiviseringar av administrativa processer. Det innebär också att erbjuda möjligheter att samarbeta såväl inom som utanför universitetet på ett smidigt och säkert sätt.
- b) **Underlätta** för verksamheten att följa de lagar och regler som gäller, och samtidigt minimera den eventuellt negativa inverkan det får på användarvänligheten.



- c) Säkerställa** att universitetet tillhandahåller en hög nivå av IT- och informationssäkerhet och skapar en robust säkerhetsmiljö i flera lager som kan motstå attacker och anpassa sig till nya hot.

En tät strategisk verksamhetsdialog är nödvändig för att IT ska kunna vara med tidigt och identifiera nya behov för att kunna erbjuda adekvat IT stöd samt även genomföra anpassningar som går i linje med för var tid aktuellt verksamhetsbehov.

3. Övergripande strategi

Universitetets IT-strategi ska vara flexibel för att hantera nya möjligheter och hot, och samtidigt verka för användarnas behov av användbara system med hög IT-säkerhet. Strategin pekar ut riktningen och gör det enklare att göra rätt saker och samtidigt göra saker rätt.

Framåt tillsammans

För att kunna möta dessa utmaningar och uppnå alla mål är det viktigt att Umeå universitet erkänner de begränsningar som finns i att arbeta isolerat. Att söka samarbeten inom sektorn och att använda nationella system där det är möjligt måste vara första alternativet vid såväl framtagande av nya IT-tjänster som förvaltande av befintliga IT-tjänster. Som andra alternativ gäller att använda plattformar från starka externa leverantörer, framför allt från leverantörer som används av andra lärosäten. Om det inte går att hitta en lösning med hjälp av något av dessa ska universitetet i sista hand ta fram egna lösningar. När egna lösningar tas fram ska även målet vara att dessa ska gå att erbjuda till andra i sektorn.

Innan någon ny IT-tjänst införs ska det genomföras en utredning samt säkerställas att det är i linje med universitetets arkitekturprinciper för IT-system. Det sammanvägda resultatet av utredningen ska ligga till grund för beslutet av vald lösning. Genom att välja denna approach till IT-tjänster kan universitetet fokusera på att utveckla det som verkligen är nödvändigt och på så sätt få resurser att erbjuda skräddarsydda IT-tjänster där de verkligen krävs.

IT-tjänster som används inom Umeå universitet ska komplettera varandra i sina användningsområden och inte konkurrera med varandra. De enskilda systemen ska bidra till en helhet som stödjer verksamhetens olika processer.

Endast IT-tjänster som gör dokumenterad nytta ska införas och föråldrade system ska avvecklas. Universitetsgemensamma system skall användas i första hand. Lokala system ute på institutioner och enheter sätts upp endast då speciella skäl föreligger. Notera att samma krav på bland annat cybersäkerhet gäller även för dessa, och att det fulla ansvaret för systemet ligger hos prefekt eller enhetschef. Extra kostnader som kan uppstå för de universitetsgemensamma systemen pga. användningen av lokala system skall bekostas i sin helhet av det lokala systemet. I de fall där lokala system kopplas samman med eller utbyter information med universitetsgemensamma system, finns ingen garanti för att det lokala systemet kan fortsätta fungera på detta sätt över tid. Nödvändiga förändringar i universitetsgemensamma system har företräde även om det uppstår problem i lokala system.

Hållbart nu och sedan

Livscykelanalys för IT-tjänster är en metodisk utvärdering av en tjänsts hela livscykel, från idé och utveckling till införande, drift, och slutligen avveckling eller ersättning. Denna analys hjälper till att förstå de fullständiga konsekvenserna av att införa och upprätthålla en IT-tjänst, inklusive kostnader, säkerhetsrisker, användarvänlighet och juridiska aspekter. För en organisation är livscykelanalysen avgörande eftersom den säkerställer att investeringar i IT-



UMEÅ UNIVERSITET

tjänster är hållbara och att de stödjer de långsiktiga målen för verksamheten. Genom att aktivt genomföra livscykelanalyser kan Umeå universitet optimera sina resurser, förbättra säkerheten och säkerställa att de IT-tjänster som används verkligen möter användarnas behov och bidrar till verksamhetens framgång. Därför ska alla IT-tjänster vid Umeå universitet ingå i en övergripande livscykelanalys som tydligt visar var i livscykeln de befinner sig. Systemägaren för respektive system ansvarar för att uppdatera systemets livscykelanalys utifrån instruktioner från universitetsgemensam IT.

Utveckling för fler

Umeå universitet är sedan många år tillbaka starkt investerade i Microsoft-tekniker. På senare år har mycket samlats i deras plattform M365. Detta har gjorts för att skapa en integrerad miljö där verktyg för kommunikation, samarbete och dokumenthantering smidigt samverkar, vilket minimerar behovet av att växla mellan olika system. Dessutom erbjuder M365 löpande uppdateringar och säkerhetsförbättringar, vilket säkerställer att universitetet alltid har tillgång till den senaste tekniken och de mest robusta säkerhetsfunktionerna. Genom att centralisera IT-tjänster i en plattform skapas även en mer sammanhållen IT-arkitektur, vilket underlättar för administration och support, samtidigt som det ger en stark grund för att bygga vidare på framtida teknologiska innovationer. Något som är väldigt viktigt för att detta ska falla väl ut är att verksamheten erbjuds möjligheten att upptäcka de möjligheter som erbjuds samtidigt som man får ett adekvat verksamhetsstöd i transitionen till nya arbetssätt.

Det innebär naturligtvis också risker med att använda en plattform som M365. En av de största utmaningarna för en myndighet är att kunna hålla kontroll på alla förändringar som görs och hur de eventuellt påverkar oss utifrån såväl användbarhet som regulatorisk efterlevnad. Detta är ett arbete där Umeå universitet idag ligger mycket långt fram och andra lärosäten är intresserade av hur vi arbetar. Det är även ett område där vi bör söka samarbeten inom sektorn då alla står inför samma utmaningar.

En annan sak att beakta är inlåsningseffekten till en leverantör. Därför är det av yttersta vikt att ha en väl utarbetad exitstrategi i den mån det är möjligt. Vi måste framför allt ta medvetna beslut kring inlåsningseffekten och vad den kan innebära. Detta är ett arbete som behöver bedrivas såväl på en övergripande nivå som på institutions- och användarnivå i hur man använder sig av de tjänster som erbjuds.

Ta en aktiv roll för både möjligheter och hot

Informationshantering är en central komponent för att säkerställa att universitetet fungerar effektivt och kan fatta välgrundade beslut. Det handlar inte bara om att samla och lagra information, utan också om att arkivera och gallra den på ett strukturerat sätt. Genom att aktivt hantera information kan universitetet säkerställa att endast relevant och aktuell information finns tillgänglig, vilket förbättrar effektiviteten och minskar risken för informationsöverflöd. Arkivering av viktig information möjliggör att historisk information kan bevaras för framtida referens och forskning, medan gallring av föråldrad eller irrelevant information hjälper till att upprätthålla ordning och säkerhet.

I takt med att den digitala transformationen fortsätter att accelerera, är det avgörande att Umeå universitet aktivt strävar mot att bli en mer datadriven organisation. Genom att använda information på ett strategiskt sätt kan universitetet optimera sina resurser, förbättra beslutsfattandet och driva innovation inom både utbildning och forskning. Att vara datadriven innebär att verksamheten kan analysera stora mängder information för att identifiera mönster och insikter, vilket leder till mer informerade beslut och bättre resultat.



UMEÅ UNIVERSITET

Dessutom kan en datadriven strategi hjälpa till att identifiera och utnyttja nya möjligheter, förbättra studenternas lärandeupplevelser och öka effektiviteten i administrativa processer.

I en tid då konkurrensen inom högre utbildning ökar, ger en medveten satsning på datadrivna metoder Umeå universitet en tydlig fördel, vilket stärker dess position som en framstående och innovativ institution både nationellt och internationellt. Vi har idag stora mängder data som skulle gå att använda vid universitetet, men den är utspridd och det saknas åtkomstregler etcetera för att det effektivt ska gå att hantera informationen. Därför är det av största vikt att informationstillgångar identifieras och ett ramverk för åtkomst till olika typer av information sätts upp såväl som en centraliserad åtkomst till all information. Detta blir än mer viktigt i samband med intåget av AI som sätter helt nya möjligheter när det gäller att använda information för att uppnå universitetets mål.

AI-revolutionen innebär både stora möjligheter och utmaningar för Umeå universitet. Genom att ta en aktiv roll i utvecklingen kan universitetet använda AI för att förbättra utbildningens kvalitet, effektivisera forskningsprocesser och optimera administrativa uppgifter. AI kan exempelvis användas för att analysera stora mängder information för att skapa individuellt anpassade lärandeupplevelser för studenterna eller för att identifiera nya forskningsrön och samarbeten.

Med dessa möjligheter kommer också risker och utmaningar som måste hanteras noggrant. Dessa inkluderar frågor om etik, integritet och säkerhet. Det är viktigt att säkerställa att AI-systemen används på ett ansvarsfullt sätt, skyddar användarnas information och följer gällande lagar och regler. Dessutom måste universitetet vara medvetet om risken för att bli alltför beroende av specifika teknologier eller leverantörer, vilket kan leda till inlåsnings effekter. För att framgångsrikt navigera i denna snabbt föränderliga teknologiska miljö är det avgörande att ha en tydlig strategi för AI-implementering som inkluderar robusta säkerhetsåtgärder, kontinuerlig övervakning och utvärdering av AI-systemens effektivitet och påverkan på verksamheten.

Framåtlutad för framtiden

För att universitetet ska kunna fortsätta att vara en ledande institution inom utbildning och forskning är det avgörande att IT-organisationen är framåtlutad och proaktiv i att identifiera och implementera nya teknologiska möjligheter. Genom att ständigt vara på jakt efter innovativa lösningar kan IT-organisationen inte bara förbättra den dagliga driften och effektiviteten, utan också möjliggöra nya former av undervisning, forskning och samarbete.

En framåtlutad IT-strategi hjälper universitetet att snabbt anpassa sig till förändringar i den teknologiska miljön, möta nya säkerhetsutmaningar och utnyttja de senaste teknologierna för att ge studenter och personal de bästa förutsättningarna för framgång. Dessutom bidrar en proaktiv IT-organisation till att skapa en flexibel och skalbar infrastruktur som kan växa och utvecklas i takt med universitetets behov och ambitioner, vilket i sin tur stärker universitetets konkurrenskraft och attraktionskraft på både nationell och internationell nivå.

Säkerhet skapar ett utrymme för innovation i en organisation genom att bygga en grund av tillit och stabilitet som gör det möjligt för medarbetare att fokusera på kreativt tänkande och utveckling. När robusta säkerhetsåtgärder är på plats minskar risken för informationsläckor och intrång, vilket frigör tid och resurser som annars skulle användas för att hantera och återhämta sig från incidenter. Dessutom skapar en säker miljö förtroende hos medarbetare och partners, vilket underlättar samarbete och informationsutbyte. Genom att integrera säkerhet i alla led av verksamheten kan organisationer också säkerställa att nya idéer och teknologier implementeras på ett sätt som skyddar både information och människor, vilket i



sin tur främjar en kultur av kontinuerlig förbättring och innovation. Universitetets riskapitet vid innovation kan ökas om ett robust säkerhetsramverk finns på plats för att skydda informationen.

3.1 Upphandling och licenser

För att säkerställa en effektiv och hållbar IT-miljö är det av yttersta vikt att ha en genomtänkt upphandling av IT-tjänster. Detta innefattar allt från licenser för mjukvara till tjänster som levereras via molnet, såsom Software as a Service (SaaS) och Infrastructure as a Service (IaaS). En väl fungerande upphandlingsstrategi hjälper universitetet att förvärva rätt verktyg och tjänster som möter verksamhetens behov, samtidigt som kostnaderna hålls under kontroll och säkerheten bibehålls.

Prioriteringar:

- Anpassa upphandlingsprocessen för att kunna dra nytta av teknologiska framsteg och innovationer.
- Säkerställa att de valda tjänsterna är skalbara och flexibla nog att anpassa sig till framtida krav.
- Prioritera samarbeten inom sektorn. Det ger oss såväl ökade möjligheter till kostnadseffektiva tjänster, som erfarenhetsutbyte.

Genom att noggrant utvärdera och välja rätt leverantörer och tjänster kan universitetet skapa en robust och framtidssäkrad IT-infrastruktur som stöttar både utbildning och forskning på bästa möjliga sätt.

Licensförsörjning är en annan viktig aspekt av IT-miljön vid Umeå universitet. Det är avgörande att mjukvarulicenser på ett effektivt och kostnadseffektivt sätt.

Prioriteringar:

- Genom att centralisera licenshanteringen kan universitetet säkerställa att alla enheter och användare har tillgång till de verktyg de behöver utan att onödiga kostnader uppstår. Dessutom bidrar en centraliserad licenshantering till att upprätthålla efterlevnad av licensavtal och säkerställa att endast licensierad programvara används inom organisationen. Detta minskar risken för juridiska problem och hjälper till att upprätthålla en hög standard för IT-säkerhet.

3.2 Användarstöd

I en digital värld är användarstöd en avgörande komponent för att säkerställa en smidig och effektiv användarupplevelse.

Prioriteringar:

- Kombinationen av digitala tjänster som är tillgängliga dygnet runt och personlig support med kunnig personal skapar en robust supportstruktur som kan hantera ett brett spektrum av användarbehov. Digitala tjänster, såsom chattbottar och omfattande FAQ-databaser, erbjuder omedelbar hjälp och tillgång till information när som helst, vilket är särskilt värdefullt för användare i olika tidszoner eller med akuta



behov. Å andra sidan ger personlig support från skickliga medarbetare en högre nivå av kundanpassning och expertis, vilket är nödvändigt för att lösa mer komplexa problem och ge användarna en känsla av tillit och trygghet. Denna kombination av tillgänglighet och expertis säkerställer att alla användare får den hjälp de behöver på ett effektivt och användarvänligt sätt, vilket i sin tur bidrar till ökad tillfredsställelse och produktivitet.

3.3 Identitets och behörighetshantering

Identitets och behörighetshantering (IAM), vem som får komma åt vad, är en viktig del för en väl fungerande IT-miljö samt basen för ett lyckat IT-säkerhetsarbete. Därför är det nödvändigt att tillhandahålla verifieringsprocesser av användare som med tillräcklig hög tillit kopplar en person till en av universitetet utgiven digital identitet. Något som kompliceras av att medarbetare på universitetet behöver kunna samarbeta med andra kollegor runt hela världen. En annan viktig del i detta är att i rätt tid ge ut men även ta bort behörigheter så att alla medarbetare hela tiden har tillgång till de tjänster de behöver, men inte heller mer än så.

Prioriteringar:

- Området identitets- och behörighetshantering ständigt behöver vidareutvecklas för att uppfylla verksamhetskrav, regulatoriska krav och rådande standarder.

Syftet med IAM-system är för att säkerställa att rätt personer får rätt tillgång till rätt resurser vid rätt tidpunkt av rätt anledning. Detta inkluderar autentisering, auktorisering och övervakning av användaråtkomst, vilket är avgörande för att skydda känslig information och system.

3.4 Användande av publika molntjänster

Alla publika molntjänster som erbjuds som universitetsgemensam tjänst har genomgått nödvändiga kontroller och är därmed godkända för användning i verksamheten utifrån en beskrivning av vilken information som får hanteras i tjänsten.

Prioriteringar:

- I de fall en publik molntjänst ska användas, oavsett om det är en universitetsgemensam tjänst eller för användning för en specifik process eller för särskild del av verksamheten måste såväl säkerhetsmässiga som juridiska aspekter på användandet noga utredas. Till stöd finns *Anvisning anskaffning av system eller molntjänst vid Umeå universitet*.
- Publika molntjänster får användas om kriterierna i *Anvisning anskaffning av system eller molntjänst vid Umeå universitet* är uppfyllda. Speciell hänsyn måste tas när det gäller GDPR och att myndigheten inte tillåter personuppgiftsöverföringar till tredjeland.
- Överväga utmaningen med att sprida myndighetens information till olika tjänster då detta gör det svårt att ha kontroll över var information finns och vad den används till.



3.5 Användande av AI-tjänster

De AI-tjänster som erbjuds som universitetsgemensamma tjänst har genomgått alla nödvändiga kontroller och är därmed godkända för användning i verksamheten utifrån en beskrivning av vilken information som får hanteras i tjänsten.

Användande av publika AI-tjänster innebär ytterligare utmaningar jämfört med traditionella molntjänster. AI-tjänster kräver ofta stora mängder information för att kunna leverera effektiva och användbara resultat, vilket medför ökade risker för dataexponering och dataintrång. Dessutom kan dessa tjänsters algoritmer och modeller vara svåra att granska och förstå, vilket gör det svårt att säkerställa att de följer etiska riktlinjer och juridiska krav, inklusive GDPR.

En annan viktig aspekt är transparensen i hur AI-tjänster hanterar och behandlar information. Eftersom dessa tjänster ofta utvecklas och underhålls av externa leverantörer, kan det vara svårt för användaren att få insikt i och kontroll över informationsbehandlingen.

Prioriteringar:

- Ställa höga krav på noggranna riskbedömningar och avtal som klargör ansvar och skyldigheter för både leverantörer och användare.
- Ta hänsyn till potentiella snedvridningar och partiskheter i AI-modeller, vilka kan leda till oönskade eller diskriminerande beslut. Det är därför viktigt att säkerställa att AI-tjänster implementeras med robusta mekanismer för rättvisa, ansvarsskyldighet och transparens.
- En AI-tjänst ska hanteras i enlighet med andra IT-tjänster, dvs även dessa ska uppfylla kriterierna i *Anvisning anskaffning av system eller molntjänst vid Umeå universitet*.

3.6 Användande av lokala IT-tjänster

På samma sätt som för publika molntjänster behöver alltid noggranna avvägningar göras innan ett lokalt system sätts upp eller används av till exempelvis en institution/enhet. Samma regler kring säkerhet, juridik mm gäller även för dessa, men här blir det i stället prefekt eller motsvarande som är ansvarig för bland annat regelefterlevnad och säkerhet.

Prioriteringar:

- I största möjliga mån använda universitetsgemensamma system. Där det inte är möjligt behöver riskerna vägas mot verksamhetsnyttan. Att till exempel använda ett lokalt system med motsvarande funktionalitet som ett universitetsgemensamt enbart för att man vill ha en annan leverantör är inte något som väger över för verksamhetsnytta, utan alla lokala system måste tillföra signifikant stöd till den egna verksamheten. Om en lokal IT-tjänst önskar använda universitetsgemensam infrastruktur som tex anslutning till AD krävs att tjänsten uppfyller de villkor som ställs på detta samt följa *Anvisning anskaffning av system eller molntjänst vid Umeå universitet*.



3.7 Sammanhållen IT-arkitektur

Många av de större lärosätena inom högre utbildning i Sverige, har på senare år insett vikten av och genomfört betydande satsningar på ett övergripande arkitekturarbete. Syftet med detta arbete är att samordna verksamhetens behov och förbättra verksamhetsprocesser genom att skapa en enhetlig arkitektur som är anpassad till verksamhetens krav på IT-stöd.

Ett framgångsrikt arkitekturarbete med en sammanhållen arkitektur syftar till att addera värde till verksamheten genom att skapa en strategisk ram för nuvarande behov samt förbereda verksamheten för att möta framväxande behov och hantera förändringar i omvärldsfaktorer.

Arkitekturstöd möjliggör snabbare utveckling och anpassning, nyttjande av nya teknologier och innovationer, med målet att stärka Umeå universitets position inom utbildning och forskning.

När olika system och tjänster fungerar sömlöst tillsammans, minskar risken för tekniska problem och driftstörningar. En gemensam arkitektur i linje med verksamhetsbehoven underlättar även uppfyllande av regulatoriska krav och går hand i hand med cybersäkerhet med syfte att upprätthålla hög standard på informations- och IT-säkerhet.

Prioriteringar:

- För att stödja den moderna forsknings- och utbildningsmiljön är det avgörande att vi strävar efter att göra oss oberoende av såväl tid som plats. Detta innebär att både användare och systemstöd ska kunna fungera optimalt, oavsett var de befinner sig.
- Genom att implementera molnbaserade lösningar, fjärråtkomst och andra digitala verktyg, kan vi säkerställa att vår infrastruktur är flexibel och anpassningsbar. På så sätt kan alla som är verksamma vid Umeå universitet fortsätta sitt arbete utan avbrott, vare sig de är på campus, hemma, eller någon annanstans.
- Genom att implementera tjänster över flera geografiska platser kan vi säkerställa att våra system blir mer robusta och motståndskraftiga mot lokala avbrott. Detta innebär även att vi kan minska beroendet av lokal utrustning i till exempel nätverk. Distribuerade tjänster gör det möjligt att utnyttja resurser mer effektivt och erbjuder en skalbar lösning som kan anpassas efter verksamhetens växande behov. Vidare minskar det latens, vilket är avgörande för att säkerställa en smidig och snabb användarupplevelse, oavsett var användarna befinner sig.

4. IT-strategi som stöd till forskning

Nationella system är ännu inte så utbrett inom forskning. För att komma framåt med att ge ett adekvat stöd till forskningen vid Umeå universitet behöver vi därför både söka samarbeten med andra lärosäten samtidigt som vi bygger upp de tjänster som behövs.

En bidragande faktor till lyckad forskning är ofta en IT-miljö som stödjer forskningsprocessens alla delar på ett sätt som gör att forskare kan ägna så mycket tid som möjligt till forskning. De IT-system som används ska möjliggöra samarbeten mellan lärosäten nationellt och internationellt, vara användarvänliga, men även skydda forskningsdata och följa legala krav.



UMEÅ UNIVERSITET

Datalagring på både kort och lång sikt är ett område som har stort fokus, och här gäller det att universitet kan erbjuda bra lösningar som är enkla att använda, säkra och inte minst kostnadseffektiva eftersom de datamängder som genereras växer exponentiellt i vår digitala värld.

En annan viktig aspekt som inte får förbises är vikten av säkra plattformar för lagring och bearbetning av forskningsdata. Forskningen genererar ofta mycket känslig information som kräver högsta möjliga säkerhet och integritetsskydd. Olämplig hantering eller otillräckligt skydd av denna information kan leda till allvarliga konsekvenser, inklusive dataintrång, förlust av förtroende och potentiella rättsliga åtgärder. Därför måste universitetet säkerställa att de plattformar som används för att lagra och bearbeta forskningsdata uppfyller stränga säkerhetsstandarder och följer relevanta lagar och förordningar. Det innebär att system och tjänster ska vara utrustade med robusta säkerhetsmekanismer som kryptering, åtkomstkontroll och regelbundna säkerhetsuppdateringar för att skydda information mot obehörig åtkomst och manipulation.

Forskare som söker finansiering externt förväntas producera en datahanteringsplan. Denna plan är viktig för IT eftersom den visar vilken planering forskarna har över IT-tjänster och datalagringsbehov. En tidig tillgång till planerna ger IT möjlighet att vara proaktiv och säkerställa att de efterfrågade tjänsterna finns tillgängliga när behovet kommer.

Det är viktigt att forskaren på sikt ges stöd i hela forskningsprocessen allt ifrån planering till publicering och arkivering. En forskningsportal skulle kunna vara den sammanhållande länken för olika typer av verktyg.

5. IT-strategi som stöd till utbildning

Utbildning är det område där man kommit längst med användning av nationella system. Här ska Umeå universitet fortsätta vara en aktiv partner i förvaltning och vara med och påverka inriktning för framtagande av nya funktioner/tjänster.

Vi har för något år sedan lämnat en Covid-19 pandemin bakom oss. När både studenter och personal lämnade campus blev trycket på universitetets digitala lösningar för utbildning mycket högt. Utökningen av kapaciteten gick dock mycket bra och visar att skalbarheten fungerar. Under pandemin har arbetssättet med digitala lösningar blivit ett huvudverktyg. Det har visat sig att detta sätt att arbeta på har fortsatt att användas även efter att pandemin avklingade. Ett digitalt utbildningsstöd och en modell med blandade lärmiljöer kommer att etableras som det nya normala.

För universitetets utbildningar behövs lärmiljöer. I dessa miljöer finns utbildningsmaterial samlade för studenter och personal att använda dygnet runt. Till dessa lärmiljöer behövs också samarbetsverktyg av olika slag. Pedagogisk programvara, till exempel för simuleringar och verktyg med forskningskoppling ska kunna erbjudas studenterna.

I normalfallet ska studenterna kunna arbeta med egen utrustning, telefoner, surfplattor och persondatorer men universitetet behöver även tillhandahålla tillgång till datorresurser till studenter som saknar adekvat utrustning. Universitetsbibliotekets datorer är här en bra resurs, kombinerat med datorsalar för särskilt krävande tillämpningar. Här finns möjligheter att använda molntjänster som tillhandahåller virtuella datorsalar som kan komplettera behovet av fysiska datorsalar på universitetet. Detta ger högre flexibilitet och prestanda.



UMEÅ UNIVERSITET

Experimentverksamhet inom det pedagogiska området är viktigt för att utveckla undervisningen med olika slags datorstöd. Det kan med fördel hanteras som en molntjänst med programvaror och serversystem tillgängliga när de behövs.

6. IT-strategi som stöd till administration

Forskning och utbildning behöver administrativt stöd. Det gäller allt möjligt från personal- och ekonomisystem till lokalbokningssystem. Administrativa system är svåra att byta ut beroende på sin komplexitet och att de berör många användare.

Här är det viktigt med en sammanhållen överblick över de universitetsgemensamma systemen och vilka verksamhetsprocesser som de stödjer. Vilka tillämpningar krävs för olika delar av verksamheten och vad kan samordnas?

Uppgraderingar av administrativa system kan vara så omfattande att de nästan kan ses som ett fullt systembyte. Därför måste uppgraderingar planeras i god tid och vid lämpliga tidpunkter. I planeringen måste hänsyn tas till universitetets mottagningskapacitet, man måste hantera systemförändringar så att verksamheten kan ta emot dessa utan att belastningen blir för stor. I detta är bra kommunikation ett viktigt verktyg.

Det är av största vikt att stödsystemen gör rätt saker på rätt sätt. De ska vara tillgängliga, ha god prestanda och vara fria från stoppande fel.

Umeå universitet använder M365 som samarbetsplattform för studenter och medarbetare, inom forskning, utbildning och administration, vilket ger stort utbud av tjänster och verktyg som ger verksamhetsnytta.

Genom att utnyttja flera av Microsofts molnplattformar kan Umeå universitet maximera verksamhetsnyttan genom att integrera olika system och applikationer på ett sömlöst sätt. Dynamics Customer Service till exempel, erbjuder möjlighet till ett universitetsgemensamt ärendehanteringssystem. PowerPlatform möjliggör utveckling av anpassade applikationer och automatisering av arbetsflöden utan behov av omfattande kodning, vilket effektiviserar verksamheten och frigör tid för mer strategiskt arbete. Denna integration av plattformar skapar en mer sammanhängande och flexibel IT-miljö som kan anpassas efter universitetets specifika behov och mål, vilket i sin tur leder till ökad effektivitet, bättre användarupplevelse och en starkare grund för framtida innovationer.

En gemensam samarbetsplattform ger en sammanhållen verktygslåda där användbarhet och igenkänning, i kombination med hög IT-säkerhet och följsamhet med legala krav, ger en IT-miljö som är effektiv, förvaltningsbar och utvecklingsbar för framtiden.

En annan viktig del i arbetet med administrativa processer är att kunna erbjuda IT-tjänster som underlättar i att digitalisera och förenkla de administrativa processerna. Här skulle PowerPlatform som till stor del redan ingår i de av universitetet redan inköpta licenserna för M365 kunna vara ett utmärkt verktyg. Något som flertalet användare på universitetet redan upptäckt. För att kunna använda plattformen fullt ut krävs dock att det etableras en förvaltningsorganisation som kan ta hand om övergripande governance samt ge användarstöd. Ett användande av PowerPlatform skulle även bidra positivt till universitetets utveckling att vara mer datadrivet.



7. Strategi för cybersäkerhet

I en tid där digitaliseringen blir alltmer omfattande, är cybersäkerhet av yttersta vikt. Digitaliseringen innebär att stora mängder information genereras, lagras och överförs, vilket ökar risken för dataintrång och cyberattacker. Cybersäkerhet spelar en avgörande roll för att skydda denna information och för att upprätthålla förtroendet hos användare och intressenter. Genom att implementera starka säkerhetsåtgärder kan universitetet inte bara skydda sin egen verksamhet och sina tillgångar, utan också skapa en trygg digital miljö för personal och studenter. Att prioritera cybersäkerhet är således en integrerad del av en framgångsrik IT-strategi, som möjliggör att teknologiska framsteg kan ske utan att kompromissa med säkerhet och integritet. Vi behöver kontinuerligt utvärdera och förbättra vår cybersäkerhetsstrategi för att säkerställa att cybersäkerhetsåtgärder förblir effektiva och relevanta.

Grunden till allt cybersäkerhetsarbete ska utgå från ett riskbaserat arbetssätt och en riskbedömning med regelbundna analyser för att identifiera potentiella hot och sårbarheter inom IT-infrastrukturen. Det riskbaserade arbetssättet ska utföras i enlighet med universitetets LIS.

Tekniska lösningar är en viktig del av cybersäkerheten, men utan en medveten och välutbildad personal och studenter blir de ineffektiva. Den grundläggande regeln för extra kostnader som uppstår för ökad cybersäkerhet är att de måste bäras av respektive system. Undantaget är övergripande cybersäkerhetsåtgärder.

Universitetet bör därför investera i regelbunden kompetensutveckling som syftar till att öka medvetenheten om cybersäkerhet bland alla anställda och studenter.

Detta kan innefatta workshops, e-lärande moduler, och simuleringar av phishing-attacker för att träna användare i att identifiera och rapportera misstänkta aktiviteter.

7.1 Informationshantering

Säkerhetsaspekten är avgörande i informationshantering. Genom att implementera robusta säkerhetsåtgärder kan universitetet skydda känslig information från obehörig åtkomst, dataintrång och andra säkerhetshot. En väl genomförd informationshantering minskar risken för informationsläckor och säkerställer att information hanteras i enlighet med gällande lagar och regler, vilket ytterligare stärker organisationens integritet och tillförlitlighet. Att ha tydliga processer för arkivering och gallring bidrar också till att informationssäkerheten upprätthålls genom att minska mängden information som potentiellt kan utsättas för hot.

7.2 Skydd av informationstillgångar

För att skydda känslig information och personuppgifter måste universitetet implementera robusta skyddsåtgärder. Detta inkluderar:

- Kryptering: Användning av stark krypteringsteknik för att skydda information både i vila och under överföring.
- Åtkomstkontroller: Implementering av strikta åtkomstkontroller för att begränsa åtkomst till känslig information till behöriga användare.



UMEÅ UNIVERSITET

- Säkerhetsgranskningar: Regelbundna revisioner och granskningar för att säkerställa efterlevnad av säkerhetsstandarder och policyer.
- Utbildning: Kontinuerlig utbildning av personal och studenter för att öka medvetenheten om cybersäkerhet och förebyggande åtgärder mot phishing och annan cyberbrottslighet.

7.3 Loggning/övervakning

En av de mest kritiska aspekterna av cybersäkerhet är loggning och övervakning. Genom att noggrant registrera och analysera användaraktiviteter och systemhändelser kan potentiella hot identifieras i ett tidigt skede. Detta möjliggör inte bara en snabb respons på säkerhetsincidenter, utan även insikter som kan användas för att förbättra de befintliga säkerhetsåtgärderna. Effektiv loggning och övervakning skapar en transparent och spårbar miljö där varje åtgärd kan granskas och utvärderas för att säkerställa efterlevnad av säkerhetsstandarder och för att identifiera avvikelser. Denna förebyggande strategi är en grundläggande del av en robust cybersäkerhetspolicy och bidrar till att minska risken för dataförluster och intrång, vilket i slutändan skyddar universitetets integritet och förtroende.

- Loggning och övervakning: Implementering av system för att logga och övervaka aktiviteter i infrastrukturen för att snabbt upptäcka och reagera på misstänkta aktiviteter.
- Fokus på övervakningen ska ligga på de digitala identiteterna, de anslutna klienterna samt de servrar som ingår i infrastrukturen.
- För externa system kan det krävas ytterligare åtgärder som att reglera detta via avtal i samband med upphandling.

7.4 Security Operations Center (SOC)

Ett Security Operations Center (SOC) är en central enhet som ansvarar för att övervaka, upptäcka, analysera och reagera på cybersäkerhetsincidenter. SOC-teamet arbetar dygnet runt för att säkerställa att organisationens IT-infrastruktur och information är skyddade mot cyberhot.

Att bygga upp en SOC i en organisation är både kostsamt och svårt varvid många väljer att upphandla detta från en extern leverantör som specialiserar sig på området, något som även Umeå universitetet bör göra.

Genom att ha en dedikerad SOC kan organisationer proaktivt hantera och minska riskerna för cyberattacker, vilket i sin tur skyddar deras tillgångar, information och rykte.

7.5 Incidenthantering

En effektiv incidenthanteringsprocess är nödvändig för att snabbt och effektivt kunna hantera säkerhetsincidenter.

- Incidenthantering: En välutvecklad plan för att snabbt och effektivt hantera säkerhetsincidenter och minimera skador.
- Återställningsplanering: Strategier för att upprätthålla verksamheten under och efter en säkerhetsincident genom backup och katastrofåterställning.
- Regelbundna övningar och simuleringar för att säkerställa beredskap hos personalen.

7.6 Backup och restore

En fungerande backup utgör en kritisk sista bastion i cybersäkerhet. Trots robusta försvarsstrategier kan intrång och dataförluster aldrig helt förhindras. Här spelar backup en avgörande roll genom att säkerställa att information kan återställas till sitt ursprungliga tillstånd efter en incident, vilket minimerar driftstopp och ekonomiska förluster. En välplanerad och regelbundet testad backupstrategi garanterar att universitetet snabbt kan återgå till normal verksamhet, oberoende av händelsens omfattning. Genom att regelbundet säkerhetskopiera information och system kan organisationen skydda sig mot dataförlust, ransomware-attacker och andra cyberhot, och därmed bevara sin operativa förmåga och sitt anseende.

- Backuphantering: Väl utvecklade rutiner för att säkerställa att information kan återställas i universitetets IT-miljö oberoende om det handlar om egna servrar eller molntjänster.
- Regelbunden kontroll och övning för att säkerställa att backuprutinerna fungerar.

Backup är kostnadsdrivande och återställning av stora datamängder från backup tar onekligen tid. Därför är det viktigt att påpeka att verksamheten måste bidra med att prioritera och peka ut vilka informationstillgångar som är mest kritiska och därmed har lägre tolerans för väntetider vid till exempel en större backupåterläsning. Detta har påverkan i var lagring av information sker. För att inte få en allt för komplex hantering av information inom verksamheten föreslås två nivåer, 1. Kritisk, 2. Normal. De olika nivåerna kommer att ge olika kostnadsnivåer på grund av att utökat behov av underliggande infrastruktur krävs för att möta kraven på återställningstid för kritisk information.

7.7 Kontinuitetshantering

Här måste verksamhet och IT arbeta både var för sig och tillsammans.

Verksamheten måste bidra med att tydliggöra vilka processer och därmed relevanta informationstillgångar inom myndighetens uppdrag som är absolut kritiska. Detta dels för att säkerställa adekvat skyddsnivå för kritiska tillgångar och för att kunna hantera återställningstider av dessa vid en större oönskad händelse.

Verksamheten bör även kontinuitetsplanera för hur man ska agera under den tid IT stödet är borta. Detta beroende på att vid en större oönskad händelse, där stora delar av infrastruktur och/eller datamängder står obrukbara kommer även återställning av kritiska system/information ta viss tid.

För att möta kraven på att kunna hantera återställningstider och dataintegritet för framför allt kritiska system/informationstillgångar krävs noggrann planering av underliggande infrastruktur. Detta inkluderar robust backupinfrastruktur men även alternativt (redundant) driftställe samt hård/mjukvara.

Övning av återställningsplaner och kontinuitetsplaner är en viktig del i kvalitetssäkring för att säkerställa att dessa fungerar om/när en oönskad händelse inträffar.



8. Framtida utveckling och innovation

För att säkerställa att IT-strategin förblir relevant och effektiv måste lärosätet kontinuerligt utvärdera och uppdatera sina IT-tjänster och -infrastrukturer. Detta inkluderar:

- Övervakning av teknologiska trender och innovationer för att identifiera nya möjligheter och utmaningar.
- Främjande av en kultur av kontinuerlig förbättring och innovation inom IT-avdelningen.
- Etablering av partnerskap med andra lärosäten, forskningsinstitut och industrin för att dela kunskap och resurser.

9. Kompetensförsörjning och omvärldsbevakning

Grundläggande för att kunna utforma mål och strategier är en intern behovsanalys samt omvärldsbevakning. Omvärlden förändras och förutsättningarna för universitetet ändras. Den allmänna teknikutvecklingen medför att det kommer nya lösningar på olika slags problemområden. Så långt det är möjligt så ska universitetet ta del av befintliga lösningar och idéer i stället för att uppfinna hjulet på nytt.

Det finns i storleksordningen 40 universitet och högskolor i Sverige. Grunden i verksamheten på alla lärosäten ser liknande ut vilket också innebär att behoven är likartat. Möjligheten för samarbete är hög vilket ger möjlighet till snabbare och effektivare utveckling inom olika områden genom att dela lösningsförslag och lösningar. Samarbetet i sektorn är i dagsläget organiserat inom olika forum såsom ITCF, ITHU etcetera ITCF som är IT-chefernas samarbetsorganisation har under sig ett i dagsläget 12 nätverksgrupper inom olika områden. Det är av hög vikt att samarbetet med andra lärosäten inom sektorn ska fortgå och vidareutvecklas.

Omvärldsbevakning rörande exempelvis tekniker, leverantörer, standarder och metoder bör vara ett kontinuerligt arbete.

En utmaning som vi står inför är svårigheten att ha egen kompetens inom alla specialistområden. Den snabba teknologiska utvecklingen och det breda spektrum av IT-områden innebär att det är praktiskt taget omöjligt att upprätthålla nödvändig kompetens internt för alla behov. Därför måste universitetet göra strategiska val om vilka kompetenser som ska utvecklas och behållas internt, och vilka som ska köpas in från externa leverantörer. Denna balansakt kräver en noggrann analys av kostnader, tillgänglighet av expertis, och hur kritiska olika kompetenser är för verksamheten. Genom att noggrant överväga dessa faktorer kan lärosätet optimera sina resurser och säkerställa att rätt kompetens finns tillgänglig vid rätt tidpunkt, samtidigt som man upprätthåller flexibilitet och innovation.