Dnr UFV 2016/896

UPPSALA
UNIVERSITET

Riktlinjer inom IT-området

Uppsala universitet

Fastställda av universitetsdirektören 2013-06-25
Reviderade 2013-10-30
Reviderade 2016-06-13

Innehållsförteckning

1 Inledning

Utvecklingen inom informationsteknikens område går mycket snabbt – vi möter oavbrutet ny teknik som förändrar vår vardag och även vårt förhållningssätt till tekniken. Ett effektivt och säkert utnyttjande av informationsteknik förutsätter tydliga riktlinjer till stöd för verksamma vid Uppsala universitet.

Detta dokument avser att beskriva universitetets riktlinjer inom olika informationstekniska områden, baserat på de övergripande mål och strategier som beskrivs i *Program för användning och utveckling av IT vid Uppsala universitet*, Dnr UFV 2009/872. Till de övergripande riktlinjerna finns riktlinjer och stöddokument på en mer detaljerad nivå.

Parallellt med riktlinjer inom IT-området finns riktlinjer inom andra områden med en nära koppling till informationsteknik, som *riktlinjer för informationssäkerhet*, Dnr UFV 2010/424.

2 Ansvar

2.1 Efterlevnad

Ansvaret för efterlevnad av universitetets riktlinjer inom IT-området fördelar sig enligt följande:

Rektor har det övergripande ansvaret.

Prefekt/motsvarande vid sin institution, avdelning eller motsvarande.

Områdesföreståndare för samordning inom sitt intendenturområde.

IT-chef för planering, samordning och uppföljning samt kontroll av efterlevnad.

Verksamma vid universitetet för att följa riktlinjerna.

Ansvaret för externa parter, exempelvis IT-konsulter, avseende tillgång till universitetets IT-resurser ska vid behov tydligt regleras i avtal.

2.2 Uppdatering av riktlinjerna

IT-chefen ansvarar för att dessa riktlinjer uppdateras kontinuerligt samt fastställer riktlinjer på detaljerad nivå.

Större revideringar av dessa övergripande riktlinjer ska fastställas av universitetsdirektören.

3 Definitioner

Verksam innefattar i detta dokument kategorierna anställd, student och övrigt verksam. Till övrigt verksam räknas person som ej uppbär lön från universitetet och har en aktiv och tydlig koppling till en institution.

Systemägare beskriver i detta dokument den roll som har det övergripande ansvaret för förvaltning och drift av ett eller flera IT-system. Rollen objektägare, som används inom de delar av organisationen som tillämpar pm3-modellen, innefattas i begreppet system-ägare.

IT-resurser innefattar i detta dokument datornät, datorer och annan informationsteknisk utrustning.

IT-utrustning innefattar i detta dokument både stationär och mobil utrustning med syfte att samla in, bearbeta, lagra, visa och/eller kommunicera information.

Stationär utrustning innefattar i detta dokument datorer, skrivare och nätverksprodukter med mera.

Mobil utrustning innefattar i detta dokument bärbara datorer, olika typer av surf- och läsplattor, mobiltelefoner och liknande.

Portabla lagringsmedia innefattar i detta dokument minneskort, USB-minnen, externa hårddiskar och liknande.

4 Omfattning

Utöver aktuell lagstiftning gäller nedanstående riktlinjer, där de två inledande avsnitten fokuserar på stödet för den enskilde användaren.

4.1 Användning av Uppsala universitets IT-resurser

Följande riktlinjer gäller vid all användning av universitetets IT-resurser, oavsett hur anslutning sker.

4.1.1 Användning av universitetets datornät

För all användning av datornät vid Uppsala universitet gäller följande:

- Konton, lösenord och koder är personliga och får endast användas av innehavaren. Tidsbegränsat undantag från denna princip medges för att personadresserad myndighetspost ska kunna hanteras vid tjänstemans frånvaro. Se information angående *Medgivande att öppna personadresserad post*, Dnr UFV 2011/814.
- För funktionskonton och tillfälliga konton gäller att en person är ansvarig för kontot. Flera personer kan dock beredas tillgång till kontot.
- Användning av universitetets datornät syftar till att underlätta studier, forskning och utförande av ordinarie arbetsuppgifter. Annan användning kan vara tillåten under förutsättning att den inte inkräktar på ordinarie arbetsuppgifter eller kommer universitetet till skada. Prefekt/motsvarande svarar för bedömningen.
- SUNET:s etiska regler reglerar tillåten användning. SUNET fördömer som oetiskt när någon
    - försöker få tillgång till nätverksresurser utan att ha rätt till det
    - försöker dölja sin användaridentitet
    - försöker störa eller avbryta den avsedda användningen av nätverken
    - uppenbart slösar med tillgängliga resurser (personal, maskinvara eller programvara)
    - försöker skada eller förstöra den datorbaserade informationen
    - gör intrång i andras privatliv
    - försöker förolämpa eller förnedra andra.
- IT-resurser som ansluts till Uppsala universitets datornät ska ha relevant skydd.

4.1.2 Användning av persondatorer, mobil utrustning och portabla lagringsmedia

Personlig utrustning som används vid studier eller i tjänsteutövning ska, oavsett om den ägs av universitetet eller enskild verksam, hanteras på ett säkert sätt som minimerar risken för informationsförluster och intrång i universitetets datornät.

Generellt gäller följande:

- Enheten ska skyddas på ett sådant sätt att känslig information inte kommer i orätta händer. Nivån på skyddet ska bedömas utifrån graden av känslighet på den information som lagras i eller som på annat sätt kan nås via enheten.
- Innehavaren är ansvarig för att säkerhetskopiering sker med relevant periodicitet och på ett säkert sätt.

För persondatorer, stationära såväl som bärbara, gäller utöver ovanstående att

- enheten ska skyddas med ett antivirus-program
- utrustning och den grundläggande programvaran måste vara uppdaterad. I den mån leverantören inte längre underhåller denna får utrustningen inte anslutas till universitetets nät och/eller tjänster.

Uppdateringar, antivirus och säkerhetskopiering sköts i normalfallet av IT-ansvarig/dataansvarig på respektive institution/motsvarande eller av intendenturen. Prefekt/motsvarande kan besluta om undantag från detta.

4.1.3 Anslutning av trådlösa nät (WLAN) till UpUnet och UpUnet-S

För att ett WLAN ska få anslutas till UpUnet/UpUnet-S krävs att oidentifierade användare inte tillåts använda nätet och att lösenord och annan känslig information inte exponeras utan krypteras på tillräcklig nivå.

4.2 Stöd och support

Stöd och support ska erbjudas samtliga verksamma vid universitetet. Support ges lokalt på olika nivåer i universitetets organisation och via universitetets centrala helpdesk. Studentsupport ger användarstöd och råd till studenter.

För att stöd och support ska kunna ges på ett tillfredställande sätt ska

- en IT-ansvarig/dataansvarig finnas utsedd vid varje institution.
- en IT-intendent finnas utsedd vid varje intendenturområde.
- arbetet med support organiseras så att supportfunktioner på lokal nivå, studentsupport och universitetets centrala helpdesk kan samverka för alla verksammas bästa.

4.3 Anskaffning, utveckling och förvaltning av IT-system

Väl fungerade IT-system utgör en grundläggande förutsättning i det arbete som bedrivs vid universitetet, både inom kärnverksamhet och stödverksamhet.
Faktorer som rör säkerhet, användbarhet och kostnadseffektivitet ska vara vägledande i allt arbete med anskaffning, utveckling och förvaltning av system.
Riktlinjerna för informationssäkerhet beskriver de krav som ställs på IT-system som används vid Uppsala universitet och ger stöd i arbetet med att uppfylla dessa.
I övrigt gäller följande inom detta område:

- En systemägare ska finnas utsedd tidigt i processen vid anskaffning/utveckling.
- Systemet ska ha stöd för en fungerande behörighetsadministration samt autentisering på rätt nivå av säkerhet med avseende på informationens känslighet.
- Avtal som beskriver överenskommen servicenivå ska upprättas före driftsättning. Ansvarig för förvaltningsorganisationen och ansvarig för driftorganisationen utgör parter vid upprättande av avtal.
- Efter upphandling/utveckling ska systemet överlämnas till lämplig förvaltningsorganisation.
- För administrativt arbete och myndighetsutövning ska likartade behov i olika delar av organisationen samordnas via gemensam upphandling/utveckling.
- Anskaffning via upphandling, egen utveckling eller samverkan med andra lärosäten utgör exempel på alternativa vägar i sammanhanget. Det mest fördelaktiga alternativet med avseende på ekonomi och funktion ska väljas.
- Allt arbete relaterat till IT-system ska präglas av ett livscykelperspektiv. Frågor som rör exempelvis ekonomi och systemunderhåll ska bedömas med hänsyn tagen till hela systemets livslängd.
- Grundläggande säkerhetskrav ska beaktas vid nyttjande av extern IT-konsult. En konsult ska följa universitetets regler vad gäller tillträde till datornät och lokaler, undertecknande av sekretessförbindelse etc.
- Användbarhetsaspekter ska beaktas vid all anskaffning och utveckling. En strävan mot enhetlighet ska vara en naturlig del i allt arbete med utformning av gränssnitt för universitetets olika system.
- Aspekter som rör tillgänglighet för personer med funktionsnedsättning ska beaktas.

4.4 Avveckling av IT-utrustning och IT-system

Avveckling av system och tjänster som spelat ut sin roll kräver, i likhet med anskaffning och utveckling, god planering.

Planering inför avveckling ska inkludera följande moment:

- Analys av konsekvenser. Finns exempelvis samband med andra system som fortfarande är i drift?
- Användare av systemet och övriga intressenter ska vara väl införstådda med planeringen av avvecklingen.
- Avtal som inte längre kommer att vara aktuella ska sägas upp.

För utrangering av IT-utrustning gäller att

- utrangerade enheter ska hanteras på ett sådant sätt att känslig information inte kommer i orätta händer. Se riktlinjerna för informationssäkerhet
- utrangering sker på ett sätt som är korrekt ur miljösynpunkt

4.5 Hantering av programvarulicenser

Enbart legal programvara ska användas vid Uppsala universitet. Universitet förväntas, som statlig myndighet, leva upp till grundläggande krav på god ordning bland programvarulicenser.

För att skapa denna goda ordning ska vi vid universitetet

- föra ett licensregister över tecknade licenser, för att därigenom kunna styrka vårt licensinnehav
- ha en funktion med uppgiften att se till att universitetet hanterar licensiering på ett korrekt sätt, d.v.s. att avtalslicenser betalas för de, och endast de, upphovsrättsligt skyddade programvaror som används i verksamheten
- informera verksamma vid universitetet gällande regler och ansvar

Prefekt/motsvarande ansvarar för information gällande regler och ansvar vid den egna institutionen.

Enheten för upphandling och inköp ansvarar för licenshantering och licensregister över de licenser som förmedlas via universitetets centrala programvarudistribution. Prefekt/motsvarande har motsvarande ansvar för programvaror som upphandlas direkt vid institutionen.

Licensregister behöver inte inbegripa programvaror som ligger under en öppen licens såsom t.ex. GPL, BSD, Apache eller liknande.

4.6 Serverdrift

Definitionen av vad en server är kan skifta från sammanhang till sammanhang. I detta fall syftas på en enhet som, till skillnad mot en persondator, nyttjas av ett flertal personer i syfte att leverera en särskild funktion eller en särskild tjänst. För sådan utrustning gäller följande:

- En driftorganisation med ett tydligt definierat ansvar för servern ska finnas utsedd.

- Servern ska vara rätt placerad med avseende på klimat och säkerhet. Serverns användningsområde ska vara vägledande vid bedömning av placering och vilken nivå på säkerhet som kan anses nödvändig.
- Servern ska konfigureras på ett säkert sätt så att den inte blir till en sårbar punkt i universitetets infrastruktur.
- Driftorganisationen ansvarar för att säkerhetskopiering sker med relevant periodicitet och på ett säkert sätt.
- Vid uppsättning av servrar som kräver särskilt hög nivå av tillgänglighet ska redundans övervägas. Informationsklassning ger stöd i bedömningen. Prefekt/motsvarande är ansvarig för att sådan genomförs.
- Grundläggande säkerhetskrav ska beaktas vid nyttjande av extern IT-konsult. En konsult ska följa universitetets regler vad gäller tillträde till datornät och lokaler, undertecknande av sekretessförbindelse etc.
- Administrativ åtkomst till servern ska vara begränsad men ej personberoende.
- Enheter som inte längre får säkerhetsuppdateringar av tillverkaren av enheten får inte anslutas till universitetets nät och/eller tjänster.

4.7 Domännamnshantering vid Uppsala universitet

- Institutioner och motsvarande ges underdomäner till uu.se på formen *inst*.uu.se. Motsvarande princip gäller även andra organisatoriska enheter som vetenskapsområden, fakulteter och särskilda inrättningar. Vägledande är om enheten finns representerad i universitetskatalogen.
- Enheter, projekt, forskargrupper, konferenser och annat som organisatoriskt ligger under en institution/motsvarande ges inte egna domäner utan placeras under respektive institution/motsvarande.
- Universitetsgemensamma IT-system, portaler och liknande tjänster ges underdomäner till uu.se på formen *tjanst*.uu.se.
- Enheter, projekt, forskargrupper, konferenser och annat som inte faller under ovanstående punkter ges inte egna domäner utan placeras under www.uu.se/*namn*. För e-postadresser till motsvarande enheter etc. används domänen uu.se.
- *inst*, *tjanst* och *namn* skall vara entydiga och lätt kunna associeras till institutionens, tjänstens etc. fullständiga namn på svenska eller engelska.