

Beslutsfattare: Birgitta Bergval-Kåreborn Dokumenttyp: Riktlinje Giltighetstid: tillsvidare	Beslutsdatum: Träder i kraft: 2018-10-18 Bör uppdateras före: 2020-12-31
Ev. dokument som upphävs: -	

## Riktlinje Molntjänster LTU

## Innehållsförteckning

<b>1. INLEDNING</b> .....	<b>3</b>
1.1 DOKUMENTETS SYFTE.....	3
<b>2. DEFINITION</b> .....	<b>3</b>
<b>3. TILLÄMPNING</b> .....	<b>4</b>
3.1 RIKTLINJER FÖR MOLNTJÄNSTER.....	4
3.1.1 Informations säkerhet och skydd.....	5
3.1.2 skydds krav .....	5
3.1.3 Molnrealisering .....	6
3.2 REFERENSER .....	6

## 1. Inledning

### 1.1 Dokumentets syfte

Syftet med dokumentet är att tydliggöra riktlinjer för hur universitetet bör hantera anskaffning och förvaltning av molntjänster. Dokumentet tydliggör vilka IT-system som ur ett informationssäkerhetsperspektiv passar för vilka typer av molntjänster samt hur dessa tjänster ska förvaltas.

## 2. Definition

Med molntjänster avses tillhandahållande av teknik för skalbara resurser, exempelvis processorkraft, lagring men även avancerade funktioner, hög grad av mobilitet och mobilt användande.

Universitetet har och kommer i överskådlig framtid att ha en hybrid miljö för leverans av IT-tjänster.

När en molntjänst övervägs ska verksamheten först identifiera vilken verksamhetsprocess som avser använda IT-systemet och vilken typ av information som kan komma att hanteras i systemet. Informationen i sig, ses som en tillgång och ska skyddas i paritet med dess skyddsvärde. Därför bedöms/inventeras krav på åtkomst till realtidsdata, tillgänglighet och konfidentialitets-/känslighetsnivåer.

En informationssäkerhetsklassificering ska göras på typen av information som ska hanteras och/eller lagras i systemet. Informationssäkerhetsklassificering avser olika perspektiv på risker m.a.p. Konfidentialitet, Riktighet och Tillgänglighet. Informationssäkerhetsklassificeringen sker på en skala 0-4 (där 0 är ingen eller försumbar risk för skada och 4 innebär en risk för rikets säkerhet).

Alla IT-system oavsett hur de driftas förvaltas i ett förvaltningsobjekt där också uppföljning av tjänsten sker, tex avseende att bedöma behoven av, kostnaderna för och kvaliteten på molntjänsten samt kraven på informationssäkerhet. Förvaltningsobjekten handhar även ev. utveckling av tjänsten.

Det finns olika typer av tekniska beskrivningar med perspektiv på molntjänster.

IaaS – Molnleverantör tillhandahåller nätverk, lagring och datorresurser (VM).

PaaS – En molnbaserad plattform för att bygga, testa och leverera applikationer.

SaaS – Internetanslutning till den tjänst som kunden abonnerar på ex. ekonomisystem.

Det finns olika typer av moln som beskriver perspektiv på ägande och drift av molnet

Privat moln	En molntjänst som levereras på en infrastruktur dedikerad åt endast en användare. Infrastrukturen kan hanteras av universitetet själv eller av en annan aktör.
Publikt moln	Molntjänsten ägs och hanteras av en molntjänstleverantör (tredje part) som säljer resurser till flera kunder på samma infrastruktur. Tjänster i publika moln är potentiellt tillgängliga för alla som så önskar. Även i ett publikt moln kan olika kunders information vara olika mycket separerad. Ju mer separerad, desto mindre potentiella skalfördelar. Samtidigt kan säkerhetsmässiga fördelar göra en separering inom det publika molnet rationell. (Att hantera information som omfattas av säkerhetsskyddslagen i en publik molntjänst kräver noggrann beredning.)
Hybridmoln	Termen hybridmoln avser en sammansättning av två eller flera molntyper som möjliggör kopplingar mellan olika tjänster och molntyper
Partnermoln	Partnermoln, ibland också omnämnda som ett gemenskapsmoln (community cloud) eller branschmoln, erbjuds till en begränsad och väldefinierad grupp av kunder med likartad kravbild. Den gemensamma kravbilderna kan avse t.ex. uppdrag, målsättning, säkerhetskrav och krav på efterlevnad. Partnermolnet hanteras av en eller flera av kunderna i samarbete, alternativt av, eller tillsammans med, en tredje part, och kan tillhandahållas antingen ”off premises”, utanför byggnaden, eller ”on premises”, dvs. i byggnaden. En särskild form av partnermoln är myndighetsmoln (government cloud).

### 3. Tillämpning

#### 3.1 Riktlinjer för Molntjänster

Informationssäkerhet är en viktig fråga vid användning av molntjänster. Rätt nivå av informationssäkerhetsklassning behöver bestämmas med avseende på krav på konfidentialitet, riktighet, tillgänglighet och spårbarhet.

Tekniska skyddsåtgärder (IT-säkerhet) ska väljas dels med hänsyn till hur skyddsvärd informationen är, dels med hänsyn till vilka specifika risker som finns relaterade till hanteringen av informationen. Informationen behöver exempelvis skyddas mot obehörig åtkomst, avbrott i önskad tillgänglighet samt förlust, förstörelse eller manipulation. Det kan också vara viktigt att ha möjlighet att spåra hur, och av vem, informationen har hanterats.

Varje molntjänst måste bedömas fristående med avseende på såväl nyttor som risker. I analysen ska säkerhetsrelaterade nyttor såväl som risker inkluderas, med utgångspunkt i den egna verksamhetens krav och behov.

Universitetet måste göra en legalitetskontroll i varje enskilt fall utifrån de bestämmelser som är tillämpliga för den specifika situationen. Resultatet av legalitetskontrollen kommer vara avgörande för om och hur myndigheten kan hantera den aktuella informationen i en molntjänst. Lagar kan sätta stopp för myndighetens planerade inköp av en molntjänst, exempel kan vara offentlighets- och sekretesslagen, dataskyddsförordningen, säkerhetsskyddslagen, högskoleförordningen eller arkivlagen.

### 3.1.1 Informations säkerhet och skydd

Universitetet grupperar information i olika informationssäkerhetsnivåer utifrån en konsekvensbedömning (0-4). Beroende på nivå bör olika åtgärder vidtas för att skydda informationen. Den tekniska säkerheten i molntjänster kan bero på vilka skydds krav som ställs på molnleverantören och hur avtal ska tecknas.

Åtgärder för att skydda information kan grupperas i olika aspekter

- Tekniskt enhetsskydd (IT-säkerhet)
  - Datasäkerhet (Brandväggar , Autentisering – multifaktor, Backup, Kryptering)
  - Fysisk säkerhet (Passering in i serverhall)
- Administrativa skyddsåtgärder
  - Policies, riktlinjer och rutiner
  - Utbildning, övervakning och kontroll
  - Sekretessförbindelser
  - Uppföljning av efterlevnad av avtal med leverantör och ev.underleverantör

### 3.1.2 skydds krav

Vanliga informationssäkerhetskrav som ska beaktas:

- 1) nationella rättsliga krav,
- 2) krav på ägandet av informationen,
- 3) krav på fysisk säkerhet,
- 4) rättsliga krav för kundens hantering av personuppgifter utanför EES,
- 5) krav om påföljder ifall servicenivåerna inte uppfylls,
- 6) krav kring datakryptering, och
- 7) krav på tydligt ansvar vid "förlust av data".
- 8) krav som ställs på en leverantör skall även inkludera ev. underleverantörer

För mer information se ref 2. kap 5.1.3 En myndighet är inte vilken molnkund som helst

### 3.1.3 Molnrealisering

- Information som har låga krav på Konfidentialitet (0-1).  
Denna typ av information kan troligtvis lagras i publikt moln med vissa krav på tekniska och administrativa skyddsåtgärder.
- Information som har höga krav på Konfidentialitet (2-3).  
Denna typ av information kan möjligtvis lagras i publikt moln med höga krav på tekniska och administrativa skyddsåtgärder.
- Information som har mycket höga krav på Konfidentialitet (4) , (tex forskningsdata som inkluderar information rörande rikets säkerhet).  
Denna typ av information finns enbart i privat moln, med mycket höga krav tekniska och administrativa skyddsåtgärder. (se ref 2, kap 5.1.3.2 Sekretesspröva och säkerhetsskydda : *I realiteten rör det sig sannolikt om ytterst få fall, där information som omfattas av säkerhetsskyddslagen, kan hanteras i en molntjänst. Att hantera information som omfattas av säkerhetsskyddslagen i en publik molntjänst bör därmed vara helt uteslutet.*)

## 3.2 Referenser

- 1) LTU informationssäkerhetsklassificeringsprocess
- 2) Molntjänster i staten – en ny generation av outsourcing  
<http://www.samradsgruppen.se/web/index.php/component/phocadownload/category/9-publikationer-och-foldrar?download=208:molntjanster-i-staten>