HØGSKULEN I VOLDA
VOLDA UNIVERSITY COLLEGE

IKT-188 - Retningslinjer for bruk av skytjenester #1.0

Dokumenteier:			**Skrevet ut:**	
Siste revisjon:	15.10.2014	**Revidert av:**	PS	
Antall sider:		**Godkj/Sign.:**		

1. Formål

Hensikten med denne retningslinjen er å informere om lovlig bruk av skytjenester for tilsette ved HVO. Bestemmelser gitt i Informasjonssikkerhetspolicy for HVO kap 3.4 Klassifisering og kontroll og kap 3.7.9 Ekstern serviceleverandør gjeld.

2. Skytjenester / Cloud Computing

Skytjenester eller såkalt "Cloud Computing/Cloud Storage" er en type tjeneste som har blitt svært utbredt de siste årene. Tjenestene omfatter alt fra dataprosessering og datalagring, til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet Internett.

Disse tjenestene leveres av kommersielle aktører, er lett tilgjengelige og kan innebære store besparelser for brukeren.

Eksempler på skytjenester er tjenester levert av selskapet Microsoft (OneDrive) DropBox, Google docs og Apple (iCloud).

3. Utfordringer

Hovedutfordringene rundt skytjenestene kan oppsummeres slik:

IT-sikkerhet:

- spesielt fare for sensitive data på avveie som følge av datainnbrudd og påfølgende datatap
- fare for data blir tilgjengeliggjort, enten ved en glipp fra leverandørs side eller fordi leverandørens opphavslands myndigheter ønsker innsyn
- fare for at skyleverandøren mister kontroll med brukers data noe som kan resultere i at data ikke kan gjenfinnes, og
- fare for at data er utilgjengelig fordi tjenesten er utilgjengelig

Immaterialrett (opphavs-, patent og designrett):

- på grunn av svakheter ved sikkerhetsløsninger kan bruker oppleve at for eksempel forskningsmaterialet blir gjort tilgjengelig for allmennheten uten at opphavsmann er klar over det
- oppleve at forskningsmaterialet forsvinner i skyen, uten at leverandør tar ansvar praktisk (hjelpe til med å lokalisere det) eller økonomisk

Yteevne/tilgjengelighet, herunder hvorvidt tilgang til egne data er konstant og holder akseptabel leveringskvalitet

Særlig det at leverandørene i dag ikke kan gi brukeren en garanti for at data blir håndtert ihht til gjeldende norske lover i forhold til IT-sikkerhet gjør at HVO ser seg nødt til å regulere bruken av disse tjenestene.

All bruk av både HVO-interne og eksterne tjenester til alle former for behandling av HVO-data og -informasjon reguleres av bestemmelsene i informasjonssikkerhetspolicy for HVO.

4. Retningslinje for bruk av skytjenester ved behandling av HVO-data og – informasjon

4.1Informasjon/data som kan lagres i skyen:

Skytjenester kan fritt anvendes for data som er klassifisert som ”Offentlig” jmf (kap3.4 i informasjonssikkerhetspolicy for HVO).

Informasjonsressurser i denne klassen er ressurser som inneholder data der det ikke påhviler noen restriksjoner for hvem som kan ha tilgang. Vær oppmerksom på at dataen/informasjonen kan påhvile opphavsrettslige begrensinger eller være underlagt spesielle lisenser. Der dette er tilfellet skal dette fremgå tydelig ved merking.
Offentlig informasjon kan fritt sendes i e-post, transporteres ukryptert over nett og sendes ukryptert i post. Den kan lagres hos tredjepart uten spesiell avtale, med mindre opphavsrett eller lisensiering forhindrer dette.

For nærmere informasjon om ”Offentlig” se (kap 3.4 i informasjonssikkerhetspolicy for HVO).

For ytterligere informasjon om retningslinjer for sikker overføring av data til tredjepart, se informasjonssikkerhetspolicy for HVO kap 3.7.21 Lagring og overføring av fortrolige opplysninger

4.2 Informasjon og data som verken skal eller kan lagres i skyen:

Alle data som er klassifisert som enten ”Intern” eller ”Unntatt Offentlig” kan og skal aldri legges ut i skyen.

a. Intern informasjon er data som er beregnet kun på HVO-ansatte, studenter ved HVO eller andre navngitte enkeltpersoner eller grupper ved institusjoner som HVO samarbeider med. Typiske eksempler kan være interne håndbøker og rutiner, referat fra interne møter og informasjon som man av andre grunner ikke ønsker åpent på Internett.

b. Unntatt offentlig -informasjon er konfidensielle data som behandles på IT-utstyr ved HVO. Dette kan være taushetspliktig informasjon, økonomiske data, data med stor kommersiell verdi, medisinske data, sensitive personopplysninger eller andre data med stort beskyttelses-og/eller konfidensialitetsbehov.
For nærmere informasjon om klassifisering av data ved HVO, se se (kap3.4 i informasjonssikkerhetspolicy for HVO).