Digital Archive Compliance Checklist

Organisation	Tillståndsnummer
	SE.147.

Om en organisation står i begrepp att börja använda molntjänster eller andra digitala systemlösningar för lagring/behandling av data/examination där det föreligger risk för röjande av sekretessreglerade uppgifter är det nödvändigt att fatta beslut först efter att flera steg och åtgärder är vidtagna.

Regulation (EU) No 1321/2014

147.A.100 Facility requirements

(h) Secure storage facilities shall be provided for examination papers and training records. The storage environment shall be such that documents remain in good condition for the retention period as specified in point *147.A.125*. The storage facilities and office accommodation may be combined, subject to adequate security.

147.A.125 Records

The organisation shall keep all student training, examination and assessment records for an unlimited period.

147.A.135 Examinations

(a) The examination staff shall ensure the security of all questions.

Checklistans 9 första huvudpunkter är framtagna av eSams expertgrupp för säkerhet och eSams expertgrupp för juridik. Den tionde punkten är framtagen av Transportstyrelsen.

Ytterligare information finns i följande standarder: ISO/IEC 27017 (Cloud Security), ISO/IEC 27001:2014 (Infrastruktur Security Management System), ISO/IEC 27002:2014 (Controls).

Kursiv text vid respektive punkt är framtagen av TS-arbetsgrupp Del 147 som stöd för nödvändiga betänkanden.

Transportstyrelsen
601 73 Norrköping
Besöksadress
Olai kyrkogata 35, Norrköping

transportstyrelsen.se
kontakt@transportstyrelsen.se

Telefon 0771-503 503
Telefax 011-185 256

		Transportstyrelsen ***stödkommentarer "att tänka på".***	**Organisationens kommentar/ Referens till MTOE kapitel/annat dokument**
1.	**Har ni analyserat verksamhetens behov? (Verksamhetsanalys)**	*Vilken typ av Molnbaserad lagring, passar organisationens behov och vilka olika risker finns i de olika typerna?* *IaaS- Infrastructure as a Service (Storage, Virtual Machines, Servers, Network.* *PaaS- Platform as a Service (databases, Webservers, Applications servers.* *SaaS- Software as a Service (g-mail, Office365, Salesforce, etc.)*	
2.	**Har ni bedömt rutiner och arbetsinsatser för att hålla sekretessreglerade uppgifter eller uppgifter med hög säkerhetsklass utanför? (Säkerhetsskyddslagen**)	*Vem ansvarar för säkerheten och hantering av krypteringsnycklar samt hur bedöms risker för om Molntjänsten upphör? Finns alternativa lagringsmöjligheter om man med kort varsel måste göra ändring i lagringsmodell, vem är då ansvarig för bevakning och snabb åtgärd? Finns ansvarsområdet beskrivet i MTOE-handboken?*	
3.	**Har ni analyserat de rättsliga kraven? Finns det rättsliga förutsättningar för att kunna nyttja en molntjänst? (Rättslig analys) Checklista 2018-10-31 2 (2)**		
4.	**Har ni värderat vilken betydelse och vilket värde den information som ska behandlas i molntjänsten har för verksamheten? (Informationsklassning)**	*Framgår IT-policy/riskklassning av dokumentation hos er, samt kopplas detta till lagringskraven angivna i MTOE?*	

5.	**Vilka risker finns det för verksamheten att nyttja tilltänkt molntjänst, vilka risker finns det kopplat till den informationsbehandling som man tänkt göra i molntjänsten (Riskbedömning1)**	*Kryptering: Ägs/ finns det krypteringsnyckel för att kryptera information innan det hamnar i molnet?* *Nyckelhantering: Vem förvarar och hur hålls säkerheten?* *Tillgänglighet: Finns tillgänglighet till internet för att nå tjänsten? (Redundanta kopplingar, olika leverantörer)* *Inloggning till molntjänst: lösenord, Tvåfaktors identifiering, Certifikat, VPN* *Säkerställs Molnstandarden i enlighet med ISO/IEC 27017 eller annan godtagbar standard?*	
6.	**Vilka funktionella och icke-funktionella krav behöver verksamheten ställa för molntjänsten samt leverantören av molntjänsten utifrån det som framkommit av Verksamhetsanalys, Rättslig analys, Informationsklassning, Riskbedömning?**	*MTOE ska ha en beskriven Moln-Policy/riktlinje som även beskriver vad/vilka delar som exkluderas då de har bedömts till hög säkerhetsklass (ex. examinationsdatabas). Om kontroll tappas i sådana hänseenden, riskerar verksamheten att tillståndet påverkas.* *Därav bör provbank hållas utanför molnbaserade lösningar alternativt skall särskilda åtgärder vidtas för att garantera säkerheten.*	
7.	**Hur ska verksamheten arbeta med uppföljning och leverantörsstyrning kopplat till molntjänsten?**		

8.	**Har ni gått igenom avtalet och förstått innebörden av avtalsvillkoren, exempelvis om villkoren ensidigt kan ändras av leverantören?**	**Juridik i molnet: Är informationen fysiskt i Sverige eller EU/EES/ USA eller någon annanstans?** **Finns adekvat säkerhet för personuppgifter(Safe Harbour, Privacy Shield)?** **Tecknande av Avtal med molntjänstleverantör:** *Ett avtalspaket bör innehålla; • Personuppgiftsbiträdesavtal (i förekommande fall)* *Personuppgiftsbiträdesavtal-(imy.se)* *• EU-kommissionens standardavtalsklausuler för överföring av personuppgifter till tredje land (i förekommande fall)* *• SLA, Service Level Agreement* *• Säkerhetspolicy, kan vara ISO/IEC 27000* *• Integritetspolicy, ingår i ISO/IEC 27000* *• Användarvillkor* *• ISO/IEC 27000* *– ISO/IEC 27001 och ISO/IEC 27002 generell InfoSäk* *– ISO/IEC 27017 och 27018 har ytterligare säkerhetskontroller för molntjänster* *• Om molnleverantören är ISO/IEC 27000 certifierad kan man utgå ifrån att det går att lita på deras processer, I praktiken är det ofta det enda man kan göra.*	
9.	**Finns en strategi för att i framtiden kunna lämna tilltänkt molntjänst (exitplan)**	*Vem bevakar molnföretagets fortlevnad (risk vid konkurs, bolagsemissioner)* *Finns en exitplan beskriven i handbok eller i refererade avtal?*	

10	E-examinationer E-examinationer **kan medföra bättre analys- och arkiveringsmöjligheter samt minska det administrativa arbetet som är förknippat med examinationer.** Företaget som används bör risksäkras initialt med en internaudit samt även ingå i fortsatt kvalitetsuppföljning enligt auditplan. Många punkter hur man kvalitetssäkrar molnbaserad tjänst kan användas om det används en modul för online digital examination. - Programvarorna ska finnas på en egen exklusiv server med en extra säkerhet (ex. Secure Exam Browser (S.E.B.). Programmet bör visa examinatorn information från examinerande elever om vilka som är aktiva och vilken tid som återstår av examinationen (ev. låsa datorn så att studenten kan inte lämna examinationen utan att ange en kod som enbart examinatorn har tillgång till). - Examinationerna ska ske i godkända lokaler emligt beskrivning i MTOE med datorer (eller annan särskilt avsedd IKT-utrustning ex. surfplatta) som bara används för examination med ett låst lokalt nätverk utan möjlighet till uppkoppling till internet. Eleverna får en ny inloggning till varje examination och ska inte kunna använda ”datorn” till någonting annat än examinationen. Hela proceduren ska vara beskriven i MTOE och den här ändringen är en signifikant ändring som ska ansökas om och granskas av TS innan den implementeras i och med att TS är på plats vid den första examinationen för en tillträdesgranskning.	

Granskat av	Datum	Signatur

Transportstyrelsens noteringar
