Upplýsingar um gátlista

Gátlistinn er hugsaður sem tól til að aðstoða vefstjóra við framkvæmd öryggisafritunar. Í gátlistanum er að finna upplýsingar um hvað ber að hafa í huga þegar kemur að öryggisafritun og vistun og meðhöndlun öryggisafrita.

Gátlistinn er ekki tæmandi og er eingöngu hugsaður sem tól sem vefstjórar geta leitað í þegar kemur að afritun á gögnum veflausnarinnar.

Ekki er ætlast til að vefstjórar búi yfir þekkingu á öllum þeim atriðum sem koma fram í gátlistanum.
Gátlistinn styður við kafla 1.6.2 Dulkóðun og öryggismál í UT handbókinni.
Ef vefstjórar nota gátlistann er gott að setja inn athugasemdir þar sem við á og vista eintak af gátlistanum til uppflettingar.

INNANRÍKISRÁÐUNEYTIÐ

Útfyllt af:	
Dags:	
vefsvæði / lén:	

Gátlisti sem fjallar um afritun á gögnum veflausnar og framkvæmd prófanna á afritunarferlinu.

UT-Vefhandbók

A.1.6.2 Gátlisti sem fjallar um afritun á gögnum

Samantekt yfir atriði tengd afritun gagna

Atriði	Athugasemdir
Öryggisafritun	
☐ Hefur verið skilgreint hvaða gögn eru vistuð í veflausn miðað við tilgang lausnarinnar?	
☐ Hefur verið skilgreint ferli við athugun á hvort kortaupplýsingar, innskráningargögn, persónugreinanlegar upplýsingar o.fl. séu vistuð í veflausn?	
☐ Hefur verið skilgreint hvaða gögn og/eða veflausn á að taka öryggisafrit af?	
☐ Hefur lýsing á afritun gagna verið skjöluð (afritunarstefna)?	
☐ Hefur verið gerð krafa um vistun gagna samkvæmt opinberum kröfum, s.s. lögum um persónuvernd, reglum Þjóðskjalasafns um rafræn opinber gögn og skil á þeim?	
☐ Hefur verið skilgreint hversu oft þarf að taka öryggisafrit af viðkomandi gögnum og/eða veflausn? Í þessu samhengi er oft talað um ásættanlegt gagnatap. Ef öryggisafrit er tekið einu sinni á dag, þá þýðir það að það sé ásættanlegt að tapa gögnum sem bárust og voru vistuð síðustu 24 klukkutímana.	
☐ Hefur geymslutími gagna verið skilgreindur og skjalaður?	
☐ Hefur ábyrðaaðili gagna í veflausn verið skilgreindur?	
☐ Hafa verið gerðar verklagsreglur um hvenær og hvernig eyða skuli gögnum?	
☐ Ef afritun gagna er útvistuð, hefur verið skilgreindur ábyrgðaraðli fyrir eftirlit með framkvæmd afritunar?	
Prófanir öryggisafritunar	
☐ Hefur verið skilgreint hversu oft og hvenær beri að prófa að endurheimta gögn frá öryggisafriti? Þetta er gert til þess að staðfesta annars vegar að verið sé að afrita viðkomandi gögn á endurheimtanlegan hátt og hins vegar að hægt sé að endurheimta veflausnina í heild sinni með nauðsynlegri virkni.	
☐ Hafa verið gerðar prófanir á endurheimt gagna í skjöluðu ferli og endurheimt staðfest af ábyrgðaraðila? Ef brotist er inn á veflausn / vefsíðu, er tryggt að öryggisveikleiki sé ekki til staðar ef endurheimta á af öryggisafriti.	
Vistun öryggisafrita og framkvæmd	
☐ Hafa afrit verið vistuð á öruggum stað í hæfilegri fjarlægð frá frumgögnum?	
☐ Hafa afritunarmiðlar verið merktir á fullnægjandi hátt?	
☐ Hafa frávik í afritun verið skráð niður og þeim fylgt eftir af ábyrgðaraðila?	
☐ Hefur aðgengi að afritum verið takmarkað við samþykkta aðila?	