Upplýsingar um gátlista

Gátlistinn er hugsaður sem tól til að aðstoða vefstjóra við stjórnun aðgangs að veflausn og undirliggjandi kerfum. Í gátlistanum er að finna upplýsingar um hvað ber að hafa í huga þegar kemur að aðgangsstjórnun að veflausn og hvaða kröfur eru gerðar til öryggisþátta.

Gátlistinn er ekki tæmandi og er eingöngu hugsaður sem tól sem vefstjórar geta leitað í vegna öryggi 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.

Útfyllt af:	
Dags:	
vefsvæði / lén:	

INNANRÍKISRÁÐUNEYTIÐ

Gátlisti varðandi aðgangsstýringar að veflausn og gögnum.

UT-Vefhandbók

A. 1.6.2 Gátlisti varðandi aðgangsstýringar

Samantekt yfir atriði tengt aðgangsstýringum

Atriði	Athugasemdir
Viðkvæmni gagna	
☐ Hefur viðkvæmni gagna sem verið er að vinna með verið kortlögð og þörf á dulkóðun metin?	
☐ Er búið að virkja SSL/TLS? SSL (Secure Socket Layer) er samskiptastaðall yfir/um dulkóðun. Hægt er að nota SSL til þess að dulkóða ýmis samskipti, meðal annars vefumferð (Hyper Text Transfer Protocol), þá er talað um HTTPS (Hyper Text Transfer Protocol Secured). TLS (Transfer Layer Security) er dulkóðunar samskiptastaðall sem hefur tekið við af SSL.	
☐ Ef verið er að nota SSL/TLS, eru rafræn skilríki staðfest af viðurkenndum aðila? Dæmi um viðurkennda aðila: Verisign, Comodo, NetLock, GlobalSign o.fl.	
☐ Eru aðgerðir notenda í veflausninni skráðar (atburðaskráning aðgerða)?	
Aðgangsstjórnun að veflausn og undirliggjandi gagnagrunni	
☐ Hefur aðgangsstýringarferli að veflausn verið skilgreint? Hvernig á að óska eftir aðgangi? Hvernig á að óska eftir því að aðgangi sé lokað? Hverjir þurfa að samþykkja aðgangsbeiðnir?	
☐ Hefur aðgangur þjónustuaðila verið skilgreindur fyrir ákveðið tímabil? Æskilegt er að aðgangur þjónustuaðilans sé eins takmarkaður og mögulegt er.	
☐ Er skilgreindur aðgangur hópa byggður á starfshlutverki og ábyrgð?	
☐ Hafa aðgangsheimildir verið skilgreindar þannig að notendur fá eingöngu aðgang að þeim heimildum sem eru nauðsynlegar (least privilege)?	
☐ Hafa eigendur og ábyrgðaraðilar að veflausn og gögnum lausnarinnar verið skilgreindir?	
☐ Hefur verið ákveðið að notast sé við einkvæm (persónuleg/persónubundin) notendanöfn?	
☐ Hefur verið ákveðið hvenær beri að rýna aðgangsheimildir að vefkerfinu? Æskilegt er að það sé gert að lágmarki árlega.	
Lykilorðastefna	
☐ Hafa lágmarkskröfur til lykilorða umsjónaraðila og notenda í veflausninni verið skilgreindar?	
☐ Ef svo er, er búið að virkja kröfur í samræmi við bestu starfsvenjur? Lengd lykilorða, líftími lykilorða, flækjustig (samblanda af hástöfum, bókstöfum, táknum), endurnýjun lykilorða.	
☐ Hafa lykilorð verið dulkóðuð í gagnagrunni veflausnar?	