Upplýsingar um gátlista

Gátlistinn er hugsaður sem tól til að aðstoða vefstjóra við kaup á þjónustu frá þriðja aðila, sérstaklega er varðar öryggisþætti. Í gátlistanum er að finna upplýsingar um öryggiskröfur sem þjónustuaðilar þurfa að uppfylla þegar kemur að hýsingu á veflausnum og tengdri þjónustu.

Gátlistinn er ekki tæmandi og er eingöngu hugsaður sem tól sem vefstjórar geta leitað í þegar keypt er þjónusta sem snertir veflausnir og vefsíður viðkomandi stofnunnar.

Ekki er ætlast til að vefstjórar búi yfir þekkingu á öllum þeim atriðum sem koma fram í gátlistanum.
Gátlistinn styður við kafla 1.3.1. Vefumsjónarkerfi val út frá öryggissjónarmiðum 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:	

UT-Vefhandbók

A.1.3.1 Gátlisti við val á veflausn - öryggisþættir

Gátlisti sem hægt er að nota við val á veflausn.
Helstu öryggiskröfur veflausnar eru listaðar upp.

Samantekt yfir atriði tengt vali á veflausn

Atriði	Athugasemdir
Öryggisúttekt	
☐ Hefur verið framkvæmd öryggisúttekt á viðkomandi veflausn samkvæmt kafla 2.5. í vefhandbók?	
☐ Ef slík öryggisúttekt hefur verið framkvæmd, var það gert af óháðum þriðja aðila?	
☐ Hefur verið gerð skýrsla um niðurstöður öryggisúttektar?	
☐ Hafa verið birtar upplýsingar um þekkta veikleika í vefumsjónarkerfi?	
Öryggisuppfærslur	
☐ Hafa verið gefnar út öryggisuppfærslur fyrir vefumsjónarkerfið?	
☐ Er gert ráð fyrir að öryggisuppfærslur verði viðskiptavinum að kostnaðarlausu?	
Tilkynningar	
☐ Hefur verið skilgreint ferli um að viðskiptavinir verði upplýstir um nýjungar í þróun lausnarinnar og þá sérstaklega ef öryggisgallar finnast í veflausninni?	
☐ Hefur verið skilgreint ferli um að tilkynnningar verði reglulega gefnar út með tilliti til öryggisveikleika sem hafa fundist og verið lagaðir?	
☐ Hafa uppfærslur á veflausn verið skjalaðar og upplýsingum um áhrif breytinga komið á framfæri við verkkaupa?	
Dulkóðun og öryggi	
☐ Styður lausnin dulkóðun upplýsinga í gagnagrunni?	
☐ Styður lausnin við þekkta auðkennistaðla s.s. HTTPS/SSL, SFTP o.s.frv.? SSL (Secure Socket Layer) er samskiptastaðall sem tryggir dulkóðuð samskipti. Hægt er að nota SSL til þess að dulkóða ýmis samskipti, meðal annars vefumferð (Hyper Ttext Transfer Protocol), þá er talaða um HTTPS (Hyper Text Transfer Protocol Secured). SFTP stendur fyrir Secured FTP og eru þá dulkóðuð FTP samskipti.	
☐ Býður lausnin upp á dulkóðun viðkvæmra gagna s.s. kortaupplýsinga, lykilorða o.s.frv.?	
Lykilorðastefna	
☐ Hafa kröfur til lykilorða í veflausninni, bæði fyrir aðgang umsjónaraðila og notenda, verið skilgreindar?	
☐ Ef svo er, hafa kröfur verið virkjaðar í samræmi við bestu starfsvenjur? Er Islykilinn notaður þar sem því verður komið við? I öðrum tilfellum þar sem notast verður við notendanöfn og lykilorð er þá hugað að lengd lykilorða, líftíma lykilorða, flækjustigi (samblanda af hástöfum, bókstöfum, táknum) og endurnýjun lykilorða.	
☐ Eru lykilorð dulkóðuð í gagnagrunni veflausnar?	
Annað	
☐ Styður veflausnin fullnægjandi aðgangsstýringar í samræmi við áhættumat? T.d. að gagnagrunni, vefviðmóti, adminkerfum o.fl.?	
☐ Býður lausnin upp á aðskilnað milli þróunar- og raunumhverfis?	
☐ Styður lausnin aðgangsstýringar byggðar á aðgangshópum og hlutverkum?	