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 1.3.2. Hýsing og þjónusta 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:	

Gátlisti sem hægt er að nota við kaup á þjónustu hjá þriðja aðila. Öryggismál tengt þjónustu þriðja aðila.

A.1.3.2 Gátlisti við val á þjónustuaðilum

Samantekt yfir öryggisatriði tengt vali á þjónustuaðilum

Atriði	Athugasemdir
Stjórnkerfi og vottanir	
☐ Hefur viðkomandi þjónustuaðili fengið ISO/IEC 27001 vottun?	
ISO/IEC 27001 – stjórnkerfi upplýsingaöryggis (http://www.stadlar.is/). ISO/IEC 27001 er alþjóðlegur staðall um innleiðingu og viðhald á stjórnkerfi upplýsingaöryggis.	
☐ Ef svo er, nær umfang vottunarinnar yfir þá þjónustu sem verið er að bjóða upp á?	
☐ Ef svo er ekki, er verið að vinna eftir verklagi samkvæmt ISO/IEC 27001?	
☐ Uppfyllir þjónustuaðili PCIDSS staðalinn?	
PCI- DSS – kröfur um vistun og meðhöndlun kortaupplýsinga (http://greidsluveitan.is/fyrirtaekid/verkefni/pci/). PCI-DSS er staðall sem skilgreinir öryggiskröfur fyrir aðila sem meðhöndla greiðslukortaupplýsingar.	
☐ Starfar þjónustuaðili samkvæmt ITIL (Information Technology Infrastructure Library) stjórnkerfi um þjónustu og rekstur?	
ITIL - Information Technology Infrastructure Library (http://www.itil-officialsite.com/) - ITIL er stuðningsstaðall sem er hugsaður fyrir þjónustustjórnun upplýsingakerfa. Sjá ISO 20000 fyrir nánari upplýsingar. ISO 20000 er alþjóðlegur staðall um þjónustustjórnun upplýsingakerfa.	
☐ Er talið að þjónustuaðili búi yfir nægilegri tæknilegri þekkingu og getu til að þjónusta verkkaupa?	
☐ Liggja skriflegar lýsingar á verkferlum sem eru mikilvægar fyrir rekstur og öryggi upplýsingakerfa þjónustuaðila?	
☐ Hefur verið unnið samkvæmt skjöluðu og formföstu þróunarferli við þróun veflausna?	
☐ Hefur verið unnið samkvæmt viðurkenndum verkefnastjórnunarferlum?	
Öryggisafritunarkröfur	
☐ Hefur verið skilgreint ferli varðandi öryggisafritunarkröfur vegna þeirra gagna sem vistuð eru hjá viðkomandi hýsingaraðila?	
☐ Hefur verið skilgreint ferli varðandi hámarks endurheimtutíma ef til kerfishruns kæmi og það þyrfti að endurheimta kerfið frá öryggisafriti?	
☐ Hefur verið gerð viðlagaáætlun og mun viðkomandi veflausn falla undir þá viðlagaáætlun?	
☐ Hefur verið skilgreint ferli að prófa skuli að endurheimta kerfi frá öryggisafriti að lágmarki einu sinni á ári?	
Öryggisuppfærslur	
☐ Hefur verið skilgreint ferli við uppsetningu öryggisuppfærslna fyrir stýrikerfi og veflausnir þannig að þær verði settar inn um leið og nýjar öryggisuppfærslur eru gefnar út? Eða að lágmarki innan þriggja daga frá því að öryggisuppfærslur eru gefnar út?	
☐ Hafa öryggisuppfærslur verið prófaðar í viðeigandi umhverfi áður en kerfi eru uppfærð?	
Frávikaskráning og vöktun	
☐ Hefur verið viðhöfð frávikaskráning á rekstrarumhverfi?	
☐ Er frávikum komið á framfæri til verkkaupa með reglubundum hætti?	
☐ Eru haldnir stöðufundir með verkkaupa til að koma á framfæri upplýsingum um frávik og vandamál tengd þjónustu?	
Hýsingarumhverfi: (hýsingaraðili)	
☐ Uppfyllir hýsingarumhverfi almennt viðurkenndar kröfur um umhverfisvarnir?	
Helstu umhverfisvarnir eru varaaflgjafi, reykskynjarar, sjálfvirkt slökkvikerfi, hita- og rakaskynjarar, kælikerfi og upphækkað kerfisgólf?	
☐ Hefur aðgangur að hýsingarumhverfi verið takmarkaður við skilgreinda aðila sem þurfa aðgang starfsins vegna?	
☐ Er til staðar neyðaráætlun hjá hýsingaraðila um endurheimt veflausna ef til áfalla kemur?	

Nánari upplýsingar er að finna í handbók um opinbera þjónustusamninga