Štandardy kybernetickej bezpečnosti ISVS

Výnos č. 55 /2014

Ministerstva financií SR o štandardoch pre informačné systémy verejnej správy

ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

Štandardy pre architektúru riadenia

§29 Riadenie informačnej bezpečnosti

a) vypracovanie a schválenie bezpečnostnej politiky povinnej osoby

b) zabezpečenie realizácie a dodržiavania schválenej bezpečnostnej politiky povinnej osoby;

c) určenie osoby/ osôb zodpovedných za IB vrátane zodpovednosti za bezpečnosť všetkých ISVS;

d) určenie jednotlivých úloh osoby/osôb zodpovedných za IB v súlade s bezpečnostnou politikou povinnej osoby;

e) zabezpečenie koordinácie aktivít organizačných zložiek povinnej osoby pri riešení IB;

f) určenie konkrétnej zodpovednosti za jednotlivé aktíva povinnej osoby;

g) určenie privilegovaných používateľských rolí v ISVS, určenie bezpečnostných požiadaviek na jednotlivé privilegované používateľské roly a určenie, ktoré používateľské roly nie je možné navzájom zlúčiť; (privilegované použ. roly najmä: správca systému, operátor, používateľ, audítor a programátor).

§30 Personálna bezpečnosť

a) všetci zamestnanci povinnej osoby, ktoré vykonávajú činnosti pre povinnú osobu musia byť poučení o schválenej bezpečnostnej politike (BP) povinnej osoby a povinnostiach z nej vyplývajúcich;

b) poučenie o právach a povinnostiach predtým, ako získajú zamestnanci prístup k ISVS;

c) zabezpečenie , aby povinnosti vyplývajúce z BP a z pracovného zaradenia zamestnanca boli uvedené v pracovnej zmluve alebo inom dokumente;

d) vypracovanie postupu pre disciplinárne konanie v prípade porušenia BP;

e) zabezpečenie povinnosti zamestnancov oznamovať bezpečnostné incidenty (**§37);**

f) Vypracovanie postupu pri ukončení pracovného pomeru vlastného zamestnanca/ ext. Spolupracovníka.

§31 Manažment rizík pre oblasť informačnej bezpečnosti

Štandardom pre manažment rizík pre oblasť informačnej bezpečnosti

a) implementácia systému riadenia a monitorovania rizík v súvislosti s ISVS, pravidelné zbieranie relevantných údajov súvisiacich s rizikami;

b) používanie systému riadenia a monitorovania rizík pri všetkých procesoch riadenia IB;

c) identifikácia, analýza a hodnotenie rizík spojených s využívaním aktív a ISVS mimo priestorov povinnej osoby a zavedenie primeraných postupov a opatrení na redukciu týchto rizík;

d) analyzovanie procesov povinnej osoby, ktoré sú podstatné pre plnenie činnosti povinnej osoby z hľadiska ich závislosti na ISVS a určenie procesov, ktoré nemôžu prebiehať v prípade výpadku alebo obmedzenia funkčnosti príslušných ISVS; tieto procesy sú kritickými procesmi;

e) analyzovanie rizík, vyplývajúcich z hrozieb pre ISVS, od ktorých závisia kritické procesy, tieto IS sú kritickými ISVS;

f) vypracovanie plánov na obnovu činnosti nefunkčných, poškodených alebo zničených kritických ISVS.

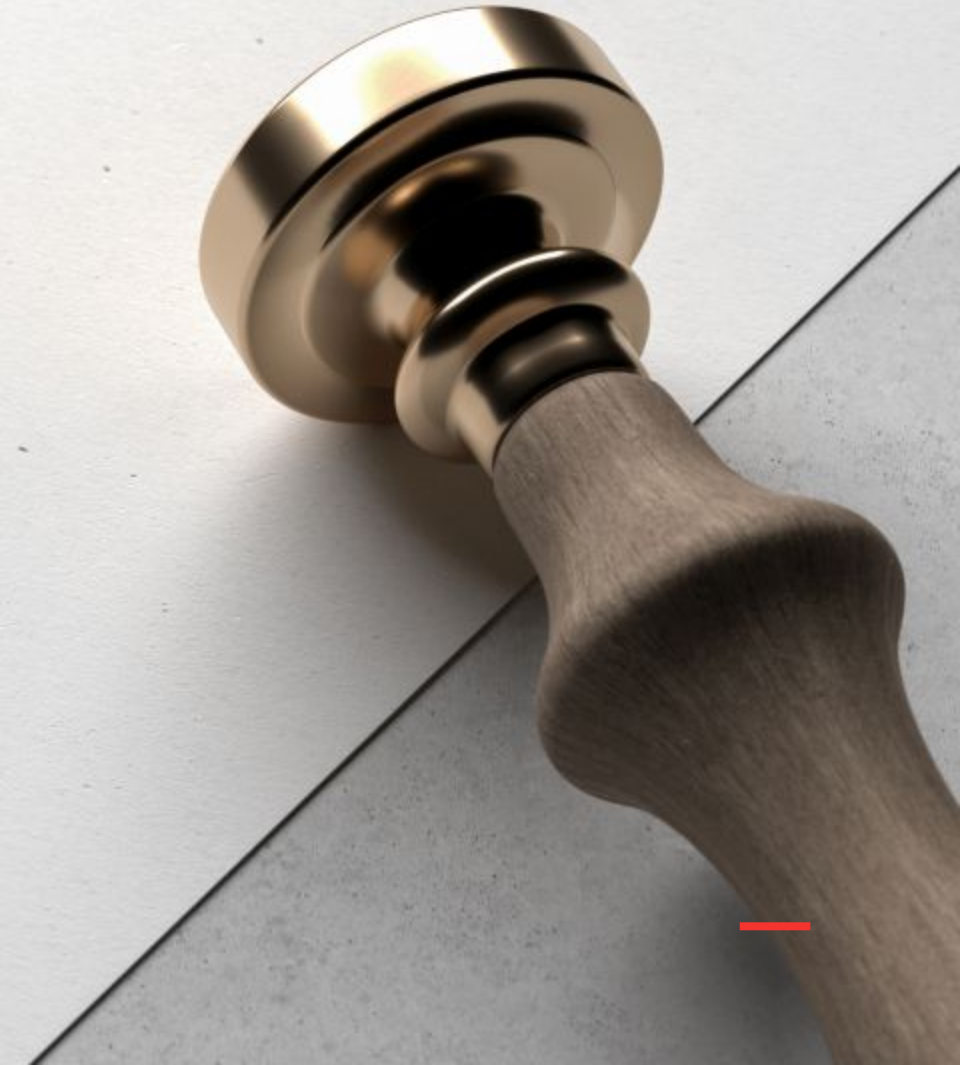
§32 Kontrolný mechanizmus riadenia informačnej bezpečnosti

Štandardom pre kontrolný mechanizmus riadenia informačnej bezpečnosti je:

a) dodržiavanie bezpečnostnej politiky povinnej osoby a zabezpečenie a vykonávanie vnútornej kontroly alebo auditu informačnej bezpečnosti, ktorého periodicita sa určuje v bezpečnostnej politike povinnej osoby,

b) zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ.

Ďakujem
za pozornosť



magdalena.sergovicova@vicepremier.gov.sk