Príloha 4
Bezpečnostné opatrenia

Číslo opatrenia	Bezpečnostné opatrenie		
C	Dôvernosť		Ano-Nie
C1	**Základná úroveň**		
C1F	***Fyzické opatrenia***		
C1F01	Všetky súčasti systému sú uložené v uzamykateľných priestoroch	**PR-C1-01 až PR-C1-04**	
C1T	***Technické opatrenia***		
C1T01	Na perimetri siete je umiestnený sieťový firewall , ktorý filtruje prevádzku smerom do infraštruktúry aj z infraštruktúry na princípe least privilege for most specific	**PR-C1-01, SE-C1-01 až SE-C1-04, SE-C2-01 a SE-C2-02**	
C1T02	Na všetkých pracovných staniciach je implementovaná ochrana voči škodlivému kódu a prebieha pravidelná kontrola	**SE-C1-01 až SE-C1-04, SE-C2-05**	
C1T03	Na poštových serveroch je implementovaná ochrana pred spamom a antimalware ochrana	**SE-C1-01 až SE-C1-04, SE-C2-05**	
C1T04	Pravidelná aktualizácia pracovných staníc (operačných systémov, kancelárskych balíkov, prehliadačov súborov, webových prehliadačov)	**SE-C1-01 až SE-C1-04**	
C1T05	Všetky heslá musia byť ukladané v nereverzibilnom formáte	**PR-C2-01, PR-C3-01, SE-C2-07, SE-C2-08, SS-C3-01**	
C1T06	Používatelia pracujú pod používateľskými kontami. Každý používateľ má vlastné konto	**PR-C2-01, PR-C3-01, SE-C1-10, SE-C2-07, SE-C2-08, SS-C3-01**	
C1OR	***Organizačné opatrenia***		
C1OR01	Všetci zamestnanci sú poučení o pravidlách používania prostriedkov povinnej osoby z hľadiska informačnej bezpečnosti	**SE-C1-10, SE-C1-13**	
C1OR02	Je vypracovaná smernica o pravidlách používania IKT prostriedkov povinnej osoby	**SE-C1-13, SE-C1-17**	
C1OR03	Na pracovných staniciach aj serveroch je inštalovaný len legálny softvér z dôveryhodného zdroja.	**SS-C4-01**	
C1OR04	Je vypracovaná a pravidelne aktualizovaná sieťová topológia	**SE-C1-21, SS-C3-01, SS-C3-03, SS-C5-01**	

	a dokumentácia		
C1OR05	Každé aktívum má svojho vlastníka	**SE-C1-21, SS-C3-01, SS-C3-03**	
C1OR06	Vypracovaná bezpečnostná politika a smernica o bezpečnom používaní.	**SE-C1-21, SS-C3-01, SS-C3-03, SS-C5-01**	
C1OR07	Implementácia klasifikácie aktív, postupov označovania a zoznam aktív	**PR-C2-10, PR-C2-15**	
C1OR08	Nastavená expirácia hesla, komplexnosť hesla na základe odporúčaní CSIRT.SK	**PR-C2-01 PR-C3-01, PR-C2-10**	
C2	**Zvýšená úroveň**		
C2F	***Fyzické opatrenia***		
C2F01	Serverové a sieťové komponenty sú uložené v uzamykateľných rackoch	**PR-C1-02, PR-C1-07**	
C2F02	Serverovňa je pod dohľadom CCTV	**PR-C1-02, PR-C1-07**	
C2F03	Obmedzenie prístupu osôb na základe need-to-use, minimalizácia prístupov k serverovým, sieťovým a bezpečnostným zariadeniam	**PR-C1-04, SE-C1-21**	
C2F04	Implementovaná kontrola vstupu do budovy		
C2T	***Technické opatrenia***		
C2T01	Na perimetri siete a prepojoch s verejne dostupnými sieťami je implementovaný L7 firewall implementujúci prístup least privilege for most specific	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T02	Na perimetri siete je implementované IDS zariadenie	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T03	Pravidelná aktualizácia všetkého softvéru na pracovných staniciach	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T04	Na všetkých serveroch je implementovaná ochrana voči škodlivému kódu	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T05	Všetky servery , sieťové a bezpečnostné prvky prístupné z verejne dostupných prvkov sú hardenované	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T06	Je implementovaný centrálny IDM manažment používateľov	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T07	Všetky prenosné počítače majú implementované Full disk encryption	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T08	Centrálne úložiská dát sú šifrované	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T09	Všetky zálohy sú šifrované	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T10	Implementovaný manažment záplat na klientskych systémoch	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T11	Implementovaný manažment záplat na serveroch	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T12	Implementovaný manažment záplat na sieťových a bezpečnostných prvkoch	**PR-C1-04, SE-C1-21, SE-C2-01**	

C2T13	Implementovaná kontrola pristupovaných webových stránok	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T14	Implementovaná kontrola prístupov zamestnancov k dôležitým dátam	**PR-C1-04, SE-C1-21, SE-C2-01**	
C2T15	Uchovávanie prístupových logov minimálne 6 mesiacov	**SE-C3-08**	
C2T16	VPN je pripojená do samostatných segmentov, ktoré sú chránené prostredníctvom IPS	**SE-C1-05**	
C2T17	Komunikačné káble môžu viesť iba v priestoroch, ktoré má povinná osoba pod kontrolou alebo sú v nich dáta šifrované	**SE-C1-05**	
C2T18	Všetky systémy v sieti musia mať implementovanú synchronizáciu času s NTP serverom	**SE-C1-05**	
C2T19	Prístup používateľov k internetu a k službám mimo siete je možný iba cez proxy server. Jediný povolený DNS server všetkých interných systémov je interný DNS server.	**SE-C1-05**	
C2T20	Zálohovanie logov aspoň 6 mesiacov	**SE-C1-02, SE-C1-21**	
C2T21	Systémy na sieti musia byť autentifikované, implementované NAC	**SE-C1-02, SE-C1-05**	
C2T22	Obmedzenie konektivity systémov do iných sietí na minimum.	**SE-C1-05**	
C2T23	Implementácia port security a ochrany pred ARP poisoningom	**SE-C1-05, SE-C1-21**	
C2T24	Implementovaná segmentácie siete aspoň na perimeter, klientov, servery a manažment	**SE-C1-05, SE-C1-21**	
C2OR	***Organizačné opatrenia***		
C2OR01	Implementácia riadenia prístupu k údajom na základe need-to-know	**SE-C1-16, PR-C2-02, PR-C2-14**	
C2OR02	Implementovaný systém riadenia informačnej bezpečnosti	**PR-C2-02, PR-C2-14**	
C2OR03	Vypracovaná analýza rizík systému	**PR-C2-02, PR-C2-14**	
C2OR04	Implementovaná analýza uskutočniteľnosti implementácie bezpečnostných opatrení	**PR-C1-14, PR-C1-15**	
C2OR05	Pravidelný audit aktív	**PR-C3-01 až PR-C3-06**	
C2OR06	Pravidelné školenia zamestnancov o informačnej bezpečnosti	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR07	Podpísané dohody o mlčanlivosti	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR08	Vypracovaný proces prepúšťania zamestnancov (odoberanie prístupových oprávnení)	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR09	Vypracovaný proces bezpečného mazania údajov a ničenia dátových nosičov	**SE-C1-21**	

C2OR10	Rozdelenie oprávnení na návrh, schválenie a nastavenie prístupových oprávnení.	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR11	Pravidelná kontrola prístupových opatrení	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR12	Vypracovaný a implementovaný proces o vzdialenej práci	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR13	Vypracovaný a aktualizovaný zoznam privilegovaných prístupových oprávnení a pravidelný ročný audit ich potreby	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR14	Oddelenie používateľskej a administrátorskej identity používateľa	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR15	Kontrola prístupu tretích osôb k zariadeniam	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR16	Implementovaný manažment zmien	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR17	Tretie osoby majú prístup iba pod kontrolou zamestnanca organizácie	**SE-C1-09, SE-C1-12, SE-C1-16**	
C2OR18	Pre každé zariadenie existuje aktualizovaný inštalačný záznam	**SS-C1-01**	
C2OR19	Vypracované interná riadiaca dokumentácia povinnej osoby v rozsahu Bezpečnosť mobilných zariadení, Bezpečnosť prenosových médií, Riadenie prístupu, Politika čistého stola, Politika zálohovania, Smernica o implementácií bezpečnostných opatrení a správe zariadení, Smernica o riešení bezpečnostných incidentov	**SE-C1-01 až SE-C1-04, SE-C1-06**	
C3	**Vysoká úroveň**		
C3F	***Fyzické opatrenia***		
C3F01	Všetky vchody , východy sú pod dohľadom kamier	**SE-C1-02**	
C3F02	Miestnosti v ktorých sú umiestnené serverové a sieťové komponenty systému nesmú mať okná, alebo sú nerozbitné a z vonkajšej strany nepriehľadné	**SE-C1-02**	
C3F03	V miestnostiach, v ktorých sú umiestnené servery a sieťové prvky musia byť certifikované bezpečnostné dvere, tehlové alebo betónové múry a pohybové senzory	**SE-C1-02**	
C3F04	Bezpečnosť budovy a jej okolia je zabezpečená strážnou službou. Na mieste incidentu, musí byť služba schopná byť do 5 minút	**SE-C1-02**	
C3F05	Poplachové senzory sú napojené na policajnú stanicu a je pravidelne vykonávaná kontrola efektivity	**SE-C1-02**	
C3F06	Tretia osoba sa v priestoroch organizácie nesmie pohybovať bez	**SE-C1-02**	

	sprievodu		
C3F07	Komunikačné káble môžu viesť iba v priestoroch, ktoré má organizácia pod kontrolou a sú zabezpečené	**SE-C1-02**	
C3F08	Vstupy na pracoviská sú kontrolované a riadené prístupovými tokenmi	**SE-C1-02**	
C3T	***Technické opatrenia***		
C3T01	Na všetkých pracovných staniciach je implementované HIPS	**SE-C1-02, SE-C1-14, SE-C1-21, SE-C2-02 až SE-C2-05**	
C3T02	Na všetkých serveroch je implementované HIPS	**SE-C1-02, SE-C1-14, SE-C1-21, SE-C2-02 až SE-C2-05**	
C3T03	Všetky servery , sieťové a bezpečnostné prvky prístupné sú hardenované	**SE-C1-02, SE-C1-14, SE-C1-21, SE-C2-02 až SE-C2-05**	
C3T04	Na perimetri siete a prístupových bodoch k citlivým dátam je implementované IPS zariadenie	**SE-C1-02, SE-C1-14, SE-C1-21, SE-C2-02 až SE-C2-05**	
C3T05	Na všetkých verejne dostupných a všetkých kritických webových portáloch je implementované WAF	**SE-C1-02, SE-C1-14, SE-C1-21, SE-C2-02 až SE-C2-05**	
C3T06	Implementované SSL inspection	**SE-C1-02, SE-C1-14, SE-C1-21, SE-C2-02 až SE-C2-05**	
C3T07	Centrálny IDM pre administrátorov, kontrola činnosti administrátorov	**SE-C1-02, SE-C1-14, SE-C1-21, SE-C2-02 až SE-C2-05**	
C3T08	Všetky prístupy k citlivým údajom sú logované.	**SE-C3-08**	
C3T09	Implementované šifrovanie súborov a emailov	**SE-C3-01 až SE-C3-03**	
C3T10	Implementovaný manažment šifrovacích kľúčov	**SE-C3-01 až SE-C3-03**	
C3T11	Pravidelne vykonávané penetračné testy a ohodnotenia zraniteľností	**SE-C3-01 až SE-C3-03**	
C3T12	Implementovaný log manažment	**SE-C3-01 až SE-C3-03**	
C3T13	Implementovaný centrálny antimalware manažment	**SE-C3-01 až SE-C3-03**	
C3T14	Implementovaný SIEM systém	**SE-C3-01 až SE-C3-03**	
C3T15	Všetky pracovné stanice majú implementované FULL disk encryption	**SE-C3-01 až SE-C3-03**	
C3T16	Všetky servery majú implementované FULL disk encryption	**SE-C3-01 až SE-C3-03**	
C3T17	Implementované DLP riešenia pre kritické dáta	**SE-C3-01 až SE-C3-03**	
C3T18	V siete je zakázané používať bezdrôtové pripojenie k sieti	**SE-C1-21**	
C3T19	Monitorovanie pripojené k systému Themis	**SE-C3-08**	

C3T20	Manažment vymeniteľných médií a prenositeľných dátových nosičov	**SE-C1-21**	
C3T21	Všetky prístupy k citlivým dátam a všetky administrátorské prístupy sú logované	**SE-C3-08**	
C3T22	Implementované uchovávanie bezpečnostných logov aspoň 12 mesiacov	**SE-C3-08**	
C3T23	Každý prístup zo segmentov VPN je kontrolovaný IPS a loguje sa aspoň 24 mesiacov	**SE-C3-08**	
C3T24	Dvojfaktorová autentifikácia používateľa do systému	**SE-C1-21**	
C3T25	V sieti musí byť implementované antimalware riešenie od iného výrobcu ako IPS / IDS	**SE-C1-21**	
C3T26	Musí byť implementované sieťové a host–based antimalware riešenie	**SE-C1-21**	
C3T27	Pracovné stanice sú hardenované	**SE-C1-21**	
C3T28	Organizácia musí mať vlastný NTP server	**SE-C1-21**	
C3T29	Implementácia segmentácie siete na základe rovnakých bezpečnostných a funkčných zón	**SE-C1-21**	
C3T30	Implementovaná sieťová behaviorálna analýza	**SE-C1-21**	
I	**Integrita**		
I1	**Základná úroveň**		
I1OR	***Organizačné opatrenia***		
I1OR01	Implementovaná smernica o zákaze neoprávnenej modifikácie dát	**SE-C1-11, SE-C1-17, SS-C6-01, SS-C6-02**	
I2	**Zvýšená úroveň**		
I2T	***Technické opatrenia***		
I2T01	Dáta sú v informačnom systéme doplnené o kontrolný súčet (hash)	**SE-C3-01 až SE-C3-07**	
I2T02	Prenášané dáta sú elektronicky podpísané a prijaté dáta sú overované	**SE-C3-01 až SE-C3-07**	
I2T03	Všetky emaily musia byť podpísané	**SE-C3-01 až SE-C3-07**	
I2T04	Na serveroch je implementovaná technológia na zabezpečenie integrity konfigurácie	**SE-C3-01 až SE-C3-07**	
I2T05	Prístupy k dátam a ich modifikácia je logovaná	**SE-C3-08**	
I3	**Vysoká úroveň**		
I3T	***Technické opatrenia***		
I3T01	Dáta sú v informačnom systéme doplnené o kontrolný súčet (hash), ktorý	**SE-C1-01, SE-C1-02, SE-C1-21**	

	je podpísaný		
I3T02	Proces zmeny dát je technicky vynucovaný	**SE-C1-01, SE-C1-02, SE-C1-21**	
I3T03	Všetky zmeny dát v systéme sú logované vrátane časovej pečiatky zmeny a podpísané	**SE-C1-01, SE-C1-02, SE-C1-21**	
I3T04	V infraštruktúre implementované DNSSEC pre lokálne systémy	**SE-C1-01, SE-C1-02, SE-C1-21**	
I3T05	Na všetkých systémoch je implementovaný systém na zabezpečenie integrity	**SE-C1-01, SE-C1-02, SE-C1-21**	
I3T06	Na systémoch je implementovaný, vynucovaný a auditovaný prístupový model RBAC, DAC alebo MAC	**SE-C1-01, SE-C1-02, SE-C1-21**	
A	**Dostupnosť**		
A1	**Základná úroveň**		
A1F	***Fyzické opatrenia***		
A1F01	Implementovaná protipožiarna ochrana vo všetkých priestoroch povinnej osoby	**PR-C1-02, PR-C1-17**	
A1F02	Implementovaná ochrana proti prírodným hrozbám (povodeň, zásah bleskom)	**PR-C1-02, PR-C1-14, PR-C1-15**	
A1T	***Technické opatrenia***		
A1T01	Zabezpečené spoľahlivé napájanie elektrickým prúdom	**PR-C1-05**	
A1T02	Dáta sú aspoň raz mesačne zálohované	**PR-C3-21**	
A1OR	Organizačné opatrenia	**PR-C1-11, PR-C3-13, PR-C3-14, SE-C1-20**	
A1OR01	Implementovaná smernica o zálohovaní a zodpovednosti za zálohovanie	**PR-C3-16, PR-C3-17, PR-C3-18**	
A2	**Zvýšená úroveň**		
A2F	***Fyzické opatrenia***		
A2F01	Vo všetkých priestoroch povinnej osoby je implementovaná ochrana voči prírodným hrozbám na základe analýzy rizík	**PR-C1-01 až PR-C1-03**	
A2T	***Technické opatrenia***		
A2T01	Všetky dáta na serveroch, dátových úložiskách a iných dôležitých umiestneniach (pracovné stanice, notebooky) sú pravidelne zálohované a archivované; úplnosť, správnosť a obnoviteľnosť dát je testovaná aspoň raz ročne	**PR-C1-01, PR-C1-04 až PR-C1-08, PR-C3-12, PR-C3-13, PR-C3-16**	

A2T01	Všetky kritické časti systému sú zapojené v HA	**PR-C1-15, PR-C1-16**	
A2T02	Pre systémy, kde je to možné je implementovaný key escrow	**PR-C1-15, PR-C1-16**	
A2T03	Dáta sú uložené na úložiskách s diskami v RAID 1, 5 alebo 6	**PR-C1-15, PR-C1-16**	
A2T04	Implementovaný prevádzkový dohľad 8x5	**PR-C2-17, PR-C3-08**	
A2OR	***Organizačné opatrenia***		
A2OR01	Zálohy sú umiestnené v zabezpečenom priestore s riadením vstupu	**PR-C3-22, SE-C1-07**	
A2OR02	Vypracované plány bussiness continuity a disaster recovery pre scenáre výpadku dôležitých komponentov informačných systémov	**SE-C1-17 až SE-C1-21**	
A2OR03	Pri každej zmene vypracovaný a aktualizovaný inventár aktív povinnej osoby	**SE-C2-07, SE-C2-08**	
A2OR04	Určení zamestnanci pri plánoch obnovy a ich zástupcovia	**SE-C1-09, SE-C1-17 až SE-C1-21**	
A2OR05	Je implementovaný systém pohotovosti 24/7/365	**PR-C3-08, SE-C1-02**	
A2OR06	Pre všetky zašifrované dáta je k dispozícií kópia šifrovacieho kľúča, ktorý je možné v prípade potreby získať autorizovanou osobou	**SE-C1-01 až SE-C1-04**	
A2OR07	Vypracovaná BIA pre všetky kritické časti systému	**SE-C1-01 až SE-C1-04**	
A2OR08	Pravidelná technická revízia technickej spôsobilosti zariadení (serverov, prvkov)	**SE-C1-01 až SE-C1-04**	
A2OR09	K dispozícií sú náhradné disky a kritické komponenty a sú podpísané SLA s ich dodávateľmi pre prípad výpadku tak, aby oprava prebehla najneskôr do 48 hodín	**PR-C3-02 až PR-C3-05**	
A2OR10	Pravidelná kontrola technického stavu zariadení a funkčnosti aplikácií (log review)	**SE-C1-14, SE-C1-20**	
A3	**Vysoká úroveň**		
A3T	***Technické opatrenia***		
A3T01	Všetky časti systému sú napájané elektrickou energiou z aspoň dvoch zdrojov	**PR-C1-05, PR-C1-07, PR-C1-08**	
A3T02	Implementované UPS a záložné zdroje na beh aspoň 12 hodín na serveroch a pracovných staniciach	**PR-C1-05, PR-C1-07**	
A3T03	Implementované riešenie na dlhodobé udržiavanie zariadenia v chode pri výpadku elektrickej energie (naftové generátory)	**PR-C1-05, PR-C1-07**	

A3T04	Všetky dáta na serveroch, dátových úložiskách a iných dôležitých umiestneniach (pracovné stanice, notebooky) sú pravidelne zálohované a archivované	**PR-C1-13, PR-C3-16, PR-C3-19**	
A3T05	Pre systém existuje warm site vzdialená aspoň 4 km od budovy v ktorej sa prevádzkuje informačný systém.	**PR-C1-13, PR-C1-16, PR-C3-12**	
A3T06	Implementovaný prevádzkový dohľad 24/7	**PR-C1-13, PR-C2-16, PR-C3-08**	
A3OR	***Organizačné opatrenia***		
A3OR01	Zálohy sú umiestnené v zabezpečenom priestore s riadením vstupu v dvoch rôznych lokalitách	**PR-C1-13, PR-C3-16, PR-C3-22**	
A3OR02	Vypracované plány bussiness contitnuity a disaster recovery pre scenáre ohrozenia budovy v ktorej je prevádzkovaný informačný systém a pre výpadok 50 percent kritických zamestnancov, hrozbu teroristického útoku a prírodnej katastrofy	**PR-C1-15, PR-C1-16, PR-C3-03, SE-C1-18**	
A3OR03	K dispozícii sú náhradné disky, kritické komponenty a sú podpísané SLA s dodávateľmi komponentov pre prípad výpadku tak, aby oprava prebehla najneskôr do 24 hodín	**PR-C3-03**	
A3OR04	Zabezpečená 100 percentná zastupiteľnosť, formálne definovaná a testovaná	**PR-C1-15, SE-C1-20, SE-C1-21**	

PR, SE, SS, EL Oblasti katalógu Vládneho cloudu viď. Príloha č.1D