***Príloha č. 1 k Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností.***

**Bezpečnostné politiky**

**1. Všeobecné ustanovenia**

1. Dodávateľ sa zaväzuje pri plnení zmluvy dodržiavať platné a účinné všeobecne záväzné právne predpisy Slovenskej republiky ako aj právne akty Európskej únie (ďalej „EÚ").
2. Vstup a pohyb zamestnancov dodávateľa, resp. jeho subdodávateľa, prípadne iných tretích osôb, prostredníctvom ktorých dodávateľ poskytuje služby (ďalej len „tretia osoba“) do priestorov prevádzkovateľa v súvislosti splnením predmetu zmluvy s prevádzkovateľom je možný iba v sprievode na to určeného zamestnanca prevádzkovateľa.

**2. Mobilné zariadenia a práca na diaľku**

**2.1 Politika pre mobilné zariadenia**

1. Spracúvať osobné údaje a iné citlivé údaje prostredníctvom mobilného telefónu je možné len za predpokladu, že citlivé údaje sú uchovávané v zašifrovanej forme a sieťové pripojenie je zabezpečené šifrovaním.
2. Spracúvať osobné údaje prostredníctvom notebooku je možné len za predpokladu, že osobné údaje sú uchovávané v pseudonymizovanej alebo v zašifrovanej forme a sieťové pripojenie je zabezpečené šifrovaním.

**2.2 Práca na diaľku**

1. Vzdialený prístup zamestnancov dodávateľa, resp. jeho subdodávateľa, prípadne inej tretej osoby do informačných systémov a ostatného softvéru prevádzkovateľa nie je možný. Prístup je možné povoliť iba v odôvodniteľných prípadoch, a to iba s dohľadom na to určeného zodpovedného zamestnanca dodávateľa, ak sa dodávateľ s prevádzkovateľom písomne nedohodne inak.
2. Práca na diaľku sa povoľuje len pre určitý okruh zamestnancov dodávateľa, iba pre určité druhy práce, a musí byť adekvátne zabezpečený aj priestor pracoviska, z ktorého je vykonávaná.
3. Práca nesmie prebiehať na prostriedkoch v súkromnom vlastníctve, ktoré nie sú pod kontrolou dodávateľa.
4. Zamestnanec dodávateľa, jeho subdodávateľa, prípadne tretia osoba musia byť adekvátne poučený a zmluvne zaviazaný neporušiť pravidlá na zabezpečenie ochrany, odcudzenia alebo vyzradenia chránených údajov.
5. Fyzická bezpečnosť musí byť odkontrolovaná na mieste výkonu práce. Kontrolu zabezpečí dodávateľom určený zamestnanec, o čom sa vyhotoví záznam, pričom prevádzkovateľ si vyhradzuje právo kontroly priestorov dodávateľa, resp. jeho subdodávateľa, alebo tretej osoby, z ktorých sa práca na diaľku uskutočňuje.
6. Žiadosť o zriadenie vzdialeného prístupu pre zamestnanca dodávateľa, resp. jeho subdodávateľa, alebo tretiu osobu postúpi príslušný zmluvný kontakt prevádzkovateľa oddeleniu centrálneho dispečingu a monitorovania služieb IS SP. V žiadosti špecifikuje rozsah prístupových oprávnení. Po schválení žiadosti riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľa sekcie informatiky prevádzkovateľa a po doručení záznamu o vykonaní kontroly fyzickej bezpečnosti na mieste výkonu práce, zrealizuje požiadavku príslušný administrátor.

**2.3 Klasifikácia informácií**

1. Pre potrebu ochrany informácií platí ich nasledovná klasifikačná schéma:
   1. citlivé,
   2. interné,
   3. verejné.
2. Citlivé **-** sú chránené informácie, a to:
   1. osobné údaje poistencov,
   2. osobné údaje zamestnancov,
   3. osobné údaje tretích strán,
   4. mzdové náležitosti zamestnancov,
   5. vymeriavacie základy poistencov,
   6. informácie dôležité pre ochranu osobných údajov v rozsahu: analýza rizík, posúdenie vplyvu na ochranu údajov, bezpečnostný incident, bezpečnostný monitoring, bezpečnostný audit,
   7. údaje zhromaždené v IS prevádzkovateľa (ďalej len „IS SP“).
3. Interné **-** sú chránené informácie, kam patria všetky informácie, ktoré nie sú klasifikované ako citlivé alebo verejné, a ktoré:
   1. vznikajú v súvislosti s plnením pracovných činností zamestnancov a nie sú určené pre zverejnenie,
   2. boli poskytnuté externým subjektom a nie sú určené pre zverejnenie.
4. Verejné **-** nie sú chránené informácie. Patria sem informácie už zverejnené alebo určené na zverejnenie v zmysle platných právnych predpisov a vnútorných predpisov.

**2.4 Zaobchádzanie s aktívami**

K citlivým informáciám je obmedzený prístup. Prístup k nim majú len oprávnené osoby, ktoré citlivé údaje spracúvajú, alebo len úzky okruh určených osôb prostredníctvom, ktorých dodávateľ plní predmet zmluvy, schválených riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky prevádzkovateľa.

**2.5 Zmluvy o dôvernosti alebo utajení**

Dohody o zachovaní dôvernosti sú súčasťou zmlúv prevádzkovateľa s dodávateľom. Každá zmluva je pred podpisom odkontrolovaná odborom bezpečnosti informačných systémov na bezpečnostný súlad. Ak sú súčasťou zmluvy osobné údaje, k špecifikácii opatrení na ochranu osobných údajov v oblasti technickej a organizačnej zaujme stanovisko zodpovedná osoba prevádzkovateľa, ktorá vykonáva dohľad nad ochranou osobných údajov u prevádzkovateľa v zmysle GDPR a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zodpovedná osoba“).

**2.6 Ochrana testovacích údajov**

Ak je na účely testovania dodávateľom nevyhnutné použiť prevádzkové údaje, môže byť použitá iba ich pseudonymizovaná kópia na základe súhlasu riaditeľa odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľa sekcie informatiky prevádzkovateľa. Kópia prevádzkových údajov musí byť bezpečne vymazaná ihneď po skončení testovania. Dozor vykonáva zodpovedná osoba prevádzkovateľa.

**3. Riadenie vzťahov s dodávateľom**

**3.1 Informačná bezpečnosť vo vzťahoch s dodávateľom**

Cieľom je zabezpečiť ochranu aktív prevádzkovateľa, ku ktorým má prístup dodávateľ samostatne, prostredníctvom subdodávateľa alebo prostredníctvom tretej osoby.

**3.1.1 Politika informačnej bezpečnosti na vzťahy s dodávateľom**

1. Predtým, než sa dodávateľovi, prípadne jeho subdodávateľovi, alebo tretej osobe povolí prístup k chráneným informáciám prevádzkovateľa, musí byť vykonaná identifikácia rizík informačnej bezpečnosti a implementované vhodné opatrenia na pokrytie identifikovaných rizík na strane dodávateľa, prípadne jeho subdodávateľa, alebo tretej osoby. Uvedené posúdenie rizík informačnej bezpečnosti musí byť v písomnej alebo elektronickej forme dodané prevádzkovateľovi v dostatočnom časovom predstihu pred podpisom zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností na jeho preštudovanie.
2. Prístup zamestnancovi dodávateľa, resp. subdodávateľa, alebo tretej osoby k chráneným informáciám prevádzkovateľa nesmie byť dovolený skôr, ako je podpísaná zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s dodávateľom a ako sú realizované primerané bezpečnostné opatrenia na ochranu aktív prevádzkovateľa.
3. Zamestnancovi dodávateľa, resp. subdodávateľa, alebo tretej osoby sa zriaďuje prístup na dobu najdlhšie jeden rok. Po uplynutí jedného roka sa potreba prístupu prehodnocuje.
4. Zriadenie prístupu zamestnancovi dodávateľa, resp. subdodávateľa, alebo tretej osobe za účelom testovania môže byť zriadené len do testovacieho prostredia prevádzkovateľa. Nasadenie vývojovej verzie APV sa musí uskutočniť výhradne v prostredí prevádzkovateľa za prítomnosti určeného zamestnanca sekcie informatiky. Tieto činnosti musia byť zdokumentované.

**3.1.2 Ošetrenie bezpečnosti v zmluvách s dodávateľom**

1. Zmluvy na výkon činností s dodávateľom musia pokrývať všetky významné bezpečnostné požiadavky. Zmluvy na výkon činností obsahujú samostatné ustanovenia alebo klauzuly, ktoré vyplývajú z bezpečnostne relevantnej legislatívy SR, zo slovenských technických noriem a z najlepších skúseností.
2. Pred spracúvaním osobných údajov k časti bezpečnostných formulácií v návrhu zmluvy na výkon činností zaujme stanovisko zodpovedná osoba prevádzkovateľa, ktorá posúdi dostatočnosť a primeranosť špecifikovaných technických a organizačných opatrení na ochranu osobných údajov.
3. K bezpečnostným formuláciám v návrhu zmluvy na výkon činností s dodávateľom zaujme stanovisko riaditeľ odboru bezpečnosti informačných systémov, ktorý posúdi dostatočnosť bezpečnostných opatrení a notifikačných povinností, ktoré musia platiť počas celej doby platnosti zmluvy na výkon činností pre zaistenie kybernetickej bezpečnosti.
4. Nie je prípustné v zmluve na výkon činností špecifikovať bližšie neurčených subdodávateľov alebo tretiu osobu a tým následne zriaďovať prístup pre zamestnancov subdodávateľa alebo tretiu osobu.

**3.1.3 Monitorovanie a preskúmanie dodávateľských služieb**

1. Služby a záznamy poskytované dodávateľom sú priebežne kontrolované osobou zodpovednou za výkon zmluvy na výkon činností, a sú monitorované vnútornou kontrolou, bezpečnostným monitoringom, interným auditom alebo externým auditom, tak ako je to zmluvne dohodnuté. Cieľom je overenie, že opatrenia na zaistenie informačnej bezpečnosti sú dodržiavané, že sú dostatočné a že vzniknuté bezpečnostné incidenty sú riešené adekvátnym spôsobom.
2. V prípade osobných údajov spracúvaných dodávateľom, jeho subdodávateľom alebo treťou osobou túto kontrolu vykonáva aj zodpovedná osoba prevádzkovateľa.

**3.1.4 Riadenie zmien v službách dodávateľa**

Zmeny v službách poskytovaných dodávateľom sú závislé od systémov a procesov a sú súčasťou hodnotenia rizík.

**3.1.5 Zodpovednosť, postupy a informovanie o udalostiach informačnej bezpečnosti**

1. Udalosť, ktorá je považovaná za podozrenie z bezpečnostného incidentu, môže byť spôsobená objektívnymi príčinami (napr. technickou poruchou, priemyselnou haváriou), konaním fyzických osôb (napr. nedbalosť, krádež, prepad, teroristický čin) alebo živelnou pohromou (napr. zemetrasenie, povodeň).
2. Každé podozrenie z bezpečnostného incidentu musí byť nahlásené a posúdené.
3. Každý zamestnanec dodávateľa, jeho subdodávateľa alebo tretia osoba, ktorý má podozrenie, že odhalil slabé miesto, alebo zistil podozrenie z bezpečnostného incidentu, je povinný to bezodkladne oznámiť. Oznámenie vykoná nasledovne:

a) e-mailom odboru bezpečnosti informačných systémov prevádzkovateľa na adresu [BIS@socpoist.sk](mailto:BIS@socpoist.sk) a,

b) e-mailom oddeleniu centrálneho dispečingu a monitorovania služieb IS SP na adresu [dispecing@socpoist.sk](mailto:dispecing@socpoist.sk) a v kópii tomu zamestnancovi prevádzkovateľa, ktorému oznámil podozrenie ústne alebo telefonicky.

**3.1.6 Informovanie o slabinách informačnej bezpečnosti**

Každý zamestnanec prevádzkovateľa môže informovať o odhalení slabého miesta osobne, telefonicky, emailom alebo interným listom. Informáciu môže odovzdať ľubovoľnému zamestnancovi odboru bezpečnosti, alebo emailom zaslať oddeleniu centrálneho dispečingu a monitorovania služieb IS SP na adresu [dispecing@socpoist.sk](mailto:dispecing@socpoist.sk).

**3.1.6.1 Hlavné kategórie bezpečnostných incidentov**

1. V oblasti ochrany zdravia zamestnancov a klientov
   1. registrovaný pracovný úraz, ktorým bola spôsobená pracovná neschopnosť zamestnanca trvajúca viac ako tri dni alebo smrť zamestnanca, ku ktorej došlo následkom pracovného úrazu,
   2. technický stav majetku a zariadení (napr. výťah, varič, nevykonávané dezinfekcie klimatizácií, nevykonávané tepovanie kobercov aspoň raz za dva roky a pod.) ohrozujúci zdravie zamestnancov a klientov,
   3. technický stav elektrických, plynových a iných rozvodov ohrozujúci zdravie zamestnancov a klientov,
   4. konanie tretích osôb v priestoroch prevádzkovateľa ohrozujúce zdravie zamestnancov a klientov.
2. V oblasti majetku prevádzkovateľa
   1. poškodenie majetku (napr. havária vodovodného potrubia spojená so zatopením prostriedkov informačnej komunikačnej infraštruktúry prevádzkovateľa, prašnosť a pod.),
   2. odcudzenie majetku, napr. notebook, osobný počítač a pod.,
   3. pokus a narušenie jednotlivých prvkov zabezpečovacieho systému,
   4. neoprávnený pobyt v objektoch prevádzkovateľa,
   5. násilné vniknutie do budovy, do zariadení (serverovňa, pokladňa, technologická miestnosť), prípadne do automobilov (s následkom odcudzenia spisov, dát a zariadení, ktoré obsahujú informácie, ktorých stratou, zneužitím prípadne zničením by došlo k obmedzeniu služieb poistencom, porušením dôvernosti, finančným stratám),
   6. poškodenie a zničenie majetku (časti majetku, napr. klimatizačná jednotka, UPS),
   7. následky havárií (prasknutie potrubia, výpadok náhradného zdroja, požiar, zatopenie, zatečenie),
   8. odcudzenie (strata) dokladov o poistencovi prevádzkovateľa,
   9. podvod, sprenevera,
   10. preukázané použitie násilia alebo hrozby bezprostredného násilia v úmysle zmocniť sa aktív prevádzkovateľa.
3. V oblasti informačnej bezpečnosti prevádzkovateľa
   1. zverejnenie hesla používateľa,
   2. zmena alebo resetovanie hesla na účte alebo zariadení neoprávnenou osobou,
   3. diskreditácia bezpečnostného predmetu (GRID karty, tokenu, prvkov PKI),
   4. prístup neoprávnenej (cudzia osoba, nevyškolená obsluha a pod.) osoby do IS SP,
   5. vírusová infiltrácia do IS SP, zasielanie nežiadúceho obsahu, škodlivý kód,
   6. prienik do IS alebo pokus o prienik,
   7. kybernetický bezpečnostný incident,
   8. inštalácie neschváleného hardvéru a softvéru na komponentoch IS SP,
   9. neoprávnené premiestnenie technických komponentov IS SP,
   10. používateľom vykonané zmeny hardvérovej konfigurácie počítača, servera, siete, komunikačných prvkov a pod.,
   11. nevykonávanie záloh na serveroch zaradených do systému centralizovaných záloh alebo serverov s inak definovanou zálohovacou stratégiou,
   12. zničenie alebo odcudzenie médií, na ktorých sú bezpečnostné zálohy serverov,
   13. prepisovanie auditných záznamov,
   14. krádež hardvéru alebo softwaru, ktorá ovplyvňuje prevádzky schopnosť IS SP,
   15. krádež a deštrukcia dát IS SP,
   16. zámerné zneužitie prístupu k zariadeniam IS SP,
   17. neplánovaný výpadok elektrického prúdu,
   18. poskytnutie, sprístupnenie, alebo zverejnenie osobných údajov konaním osoby alebo technickou poruchou IS v rozpore s pravidlami platných vnútorných predpisov prevádzkovateľa,
   19. neoprávnené použitie vstupno-výstupných zariadení nepatriacich do vlastníctva prevádzkovateľa, spôsobujúce hrozbu nebezpečnej infiltrácie,
   20. spracúvanie osobných údajov inou ako oprávnenou osobou,
   21. porušenie bezpečnostných vnútorných predpisov prevádzkovateľa majúce za následok nedostupnosť služieb pre klientov alebo partnerov prevádzkovateľa,
   22. porušenie vnútorných predpisov prevádzkovateľa s kontrolovateľným až katastrofálnym dopadom pre prevádzkovateľa.

**3.1.7 Poučenie a záväzok mlčanlivosti**

1. Vstupné poučenie o ochrane osobných údajov musí absolvovať každý zamestnanec dodávateľa, resp. subdodávateľa a/alebo tretia osoba pri nástupe na výkon zmluvných činností na základe zmluvy na výkon činností, pretože z charakteru činností prevádzkovateľa je zrejmé, že každý zamestnanec dodávateľa, resp. subdodávateľa a/alebo tretia osoba by mohli aj náhodne prísť do styku s osobnými údajmi. Za zabezpečenie poučenia zamestnanca dodávateľa, resp. subdodávateľa a/alebo tretej osoby je zodpovedný odbor bezpečnosti informačných systémov prevádzkovateľa a to vo vzťahu ku všetkým zamestnancom dodávateľa, prípadne zamestnancom subdodávateľa a/alebo tretej osobe uvedených v Zozname osôb podľa čl. IV ods. 8 zmluvy, ktoré boli riaditeľom odboru bezpečnosti informačných systémov prevádzkovateľa a riaditeľom sekcie informatiky schválené ako osoby, prostredníctvom ktorých dodávateľ plní predmet zmluvy na výkon činností. Absolvovaním tohto vstupného poučenia sa zamestnanec dodávateľa, resp. subdodávateľa a/alebo tretia osoba nestáva oprávnenou osobou na spracúvanie osobných údajov. Dodávateľ zabezpečí, aby každý zamestnanec dodávateľa, jeho subdodávateľa a/alebo tretia osoba, ktorý majú plniť povinnosti dodávateľa, podpísal pred začatím prác u prevádzkovateľa vyhlásenie o mlčanlivosti.
2. Za nahlásenie a zabezpečenie účasti zamestnanca dodávateľa, resp. subdodávateľa a/alebo tretej osoby na vstupnom poučení o ochrane osobných údajov pred nástupom na výkon zmluvných činností na základe zmluvy na výkon činností je zodpovedný dodávateľ. Nahlásenie vykoná kontaktná osoba dodávateľa u príslušného zmluvného kontaktu prevádzkovateľa.

**Vysvetlenie skratiek**

ACL - Access Control List

AP - Access Point

BIS – Bezpečnosť informačných systémov

CSRF - Cross-Site Request Forgery

DHCP - Dynamic Host Configuration Protocol

DMZ - Demilitarized Zone - VLAN, v ktorej sú umiestnené servery poskytujúce služby do externej siete, ktorá je logicky oddelená od internej siete (komunikácia je fultrovaná sieťovým firewallom)

DNS - Domain Name System

DoS – Denial of Service

FW – Firewall

IB – Informačná bezpečnosť

ICS - Industrial Control System

MitM útok – Man in the Middle útok

MVC – návrhový vzor Model–View–Controller

MVP - návrhový vzor Model–View–Presenter

NAC – Network Access Control

NAP - Network Access Protection

NDP - Neighbor Discovery Protocol - protokol v IPv6, okrem iného, nahradzujúci ARP z IPv4

NTP - Network Time Protocol

OS - Operačný systém PVLAN – Private VLAN princíp least privilege

RDP - Remote Desktop Protocol

QoS - Quality of Service

Sieťový firewall - firewall umiestnený v sieti filtrujúci komunikáciu viacerých zariadení, prípadne sietí (nie lokálny firewall)

SNMP – Simple Network Management Protocol

SSO – Single Sign-On

Telepresence

UAC – User Access Control

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

VOIP – Voice over IP

WAF – Webaplikačný firewall - špeciálny typ firewallu, prispôsobený na zabezpečenie webového servera. Ide o filter, plugin či zariadenie ktorý aplikuje set pravidiel na HTTP prevádzku.

Whitelisting - metóda kontroly prístupu k službám, ktorá povoľuje prístup iba špecifikovaným klientom a všetkým ostatným ho zakazuje

XSS - Cross-Site Scripting

**Zdroje a Legislatívne východiská**

* [Slov-lex](https://www.slov-lex.sk/domov)
* [Eur-lex](https://eur-lex.europa.eu/homepage.html)
* [Sémantický znalostný strom vedomostí Knowww EU portál](https://knowww.eu)
* [Vláda SR](https://www.vlada.gov.sk/)
* [Ústredný portál verejnej správy](https://www.slovensko.sk/sk/titulna-stranka)
* [Rokovania legislatívnej rady vlády SR](https://hsr.rokovania.sk/rokovania-legislativnej-rady-vlady-sr/)
* [Zoznam uznesení vlády SR](https://rokovania.gov.sk/RVL/Resolution)
* [Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky](https://www.mirri.gov.sk/)
* [CSIRT](https://csirt.gov.sk)
* [NASES](https://www.nases.gov.sk/index.html)
* [NBÚ](https://www.nbu.gov.sk/)
* [Interné normy SP](http://intranet/Stranky/DMS/dms.aspx)
* [NIST](http://www.nist.gov)
* [NSA](https://www.nsa.gov/)
* [OWASP](https://owasp.org/)
* [IETF](https://trustee.ietf.org/)
* [IAB](https://www.iab.org/)
* [RFC](https://www.rfc-editor.org/)
* Zákon č. **395/2002** Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov
* Zákon č. **461/2003** Z. z. o sociálnom poistení v znení neskorších predpisov
* Zákon č. **215/2004** Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
* Trestný zákon č. **300/2005** Z. z. (trestné činy páchané pomocou elektronických prostriedkov a v elektronickom prostredí) v znení neskorších predpisov
* Zákon č. **45/2011** Z. z. o kritickej infraštruktúre v znení neskorších predpisov
* Zákon č. **305/2013** Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov
* Zákon č. **272/2016** Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov
* Zákon č. **18/2018** Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a odporúčacích opatrení (zákon o ochrane osobných údajov)
* Zákon č. **69/2018** Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
* Zákon č. **95/2019** Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
* Zákon č. **452/2021** Z. z. o elektronických komunikáciách v znení neskorších predpisov (ochrana súkromia a osobných údajov, ochrana sietí a zariadení)
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **401/2023** Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **179/2020** Z. z.ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **78/2020** Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov
* Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **85/2018** Z. z., ktorou sa ustanovujú podrobnosti o spôsobe vyhotovenia a náležitostiach listinného rovnopisu elektronického úradného dokumentu
* Vyhláška Ministerstva investícií, regionálnej rozvoja a informatizácie Slovenskej republiky č. **335/2023** Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente
* Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **70/2021** Z. z. o zaručenej konverzii v znení neskorších predpisov
* Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **547/2021** Z. z. o elektronizácii agendy verejnej správy
* Vyhláška Národného bezpečnostného úradu č. **164/2018** Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
* Vyhláška Národného bezpečnostného úradu č. **165/2018** Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
* Vyhláška Národného bezpečnostného úradu č. **166/2018** Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
* Vyhláška Národného bezpečnostného úradu č. **362/2018** Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v znení neskorších predpisov
* Vyhláška Národného bezpečnostného úradu č. **48/2019** Z. z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností
* Nariadenie GDPR - Nariadenia Európskeho parlamentu a Rady (EÚ) **2016/679** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
* Nariadenie Európskeho parlamentu a Rady (EÚ) **2018/1725** z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES
* Nariadenie Európskeho parlamentu a Rady (EÚ) **2019/881** zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti)
* Smernica Európskeho parlamentu a Rady (EÚ) **2016/1148** zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
* Smernica Európskeho parlamentu a Rady (EÚ) **2016/2102** z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora
* Smernica Európskeho parlamentu a Rady (EÚ) **2019/1024** z 20. júna 2019 o otvorených dátach a opakovanom použití informácií verejného sektora
* Smernica č. **7/2019** o riešení Bezpečnostných incidentov Vládnou jednotkou CSIRT
* Metodika Jednotný́ dizajn manuál elektronických služieb verejnej správy - Metodické usmernenie UVSR č. 002089/2018/oLŠISVS-7 zo dňa 11.05.2018 <https://www.mirri.gov.sk/wp-content/uploads/2018/10/Metodicke-usmernenie-ID-SK-publikovat.pdf>
* Metodické usmernenie pre tvorbu používateľsky kvalitných elektronických služieb verejnej správy (Číslo spisu v DKS: 004307/2019/oBI) <https://www.mirri.gov.sk/wp-content/uploads/2019/04/Metodicke-usmernenie-pre-tvorbu-pouzivatelsky-kvalitnych-elektronickych-sluzieb-verejnej-spravy.pdf>
* Metodika riadenia QAMPR

<https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html>

* Metodický pokyn k zabezpečeniu centrálneho nákupu produktov a služieb spoločnosti ORACLE v rámci Centrálnej rámcovej dohody na poskytovanie licencií a produktov ORACLE a služieb s nimi súvisiacich <https://www.mirri.gov.sk/wp-content/uploads/2020/02/Metodicky_pokyn_ORACLE_CRD_2019.pdf>
* Metodické usmernenie nariadeniu (GDPR) k spracúvaniu osobných údajov (prostredníctvom web stránok) v súlade s požiadavkami Nariadenia Rady EÚ č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20190901.html>
* Metodika pre Systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (CSIRT) – aktuálne znenie [MetodikaZabezpeceniaIKT\_v2.1.pdf (gov.sk)](https://www.csirt.gov.sk/wp-content/uploads/2021/08/MetodikaZabezpeceniaIKT_v2.1.pdf?csrt=7605654333627490631)