ZÁKLADNÉ ZÁSADY INFORMAČNEJ BEZPEČNOSTI

Štandard

**Ústav výskumu sociálnej komunikácie SAV**

**Interná smernica 3/2019**

|  |  |  |  |
| --- | --- | --- | --- |
| **Vypracoval:** | **Overil:** | **Schválil:** | **Dátum registrácie/účinnosť** |
| **Meno / funkcia**:  **Ing. Tomáš Hettych, Ratio Services s.r.o.** | **Meno / funkcia:**  Ing. Ivan Kundrata/pracovník IT | **Meno / funkcia:**  **Mgr. Barbara Lášticová, PhD., riaditeľka** | **3. 7. 2019** |
| **Podpis**: | **Podpis**: | **Podpis**: |  |

|  |  |
| --- | --- |
| **Evidencia zmien** | |
| **Číslo revízie** | **Obsah zmeny** |
| 0 | Návrh smernice |
| 1 | Smernica upravená pre potreby ÚVSK SAV |

OBSAH

[1 DEFINÍCIE A KĽÚČOVÉ POJMY 3](#_Toc525472583)

[2 CHARAKTERISTIKA PREDPISU 8](#_Toc525472584)

[3 VŠEOBECNÉ ZÁSADY STAROSTLIVOSTI O INFORMAČNÉ AKTÍVA 8](#_Toc525472585)

[4 PRAVIDLÁ MANIPULÁCIE S AUTENTIZAČNÝMI PRVKAMI 9](#_Toc525472586)

[5 PRAVIDLÁ MANIPULÁCIE S HW PROSTRIEDKAMI 9](#_Toc525472587)

[6 ZÁSADY POUŽÍVANIA APLIKÁCIÍ 10](#_Toc525472588)

[7 ZÁSADY KOMUNIKÁCIE 10](#_Toc525472589)

[8 ZÁSADY MANIPULÁCIE S TLAČENÝMI DOKUMENTAMI 13](#_Toc525472590)

[9 ZÁSADY POUŽÍVANIA PAMÄŤOVÝCH MÉDIÍ 13](#_Toc525472591)

[10 ZÁVEREČNÉ USTANOVENIA 13](#_Toc525472592)

[11 ZÁVEREČNÉ USTANOVENIA 14](#_Toc525472593)

[12 ZÁZNAMY 14](#_Toc525472594)

# DEFINÍCIE A KĽÚČOVÉ POJMY

* 1. Táto kapitola definuje významnosť resp. dôležitosť požiadaviek. Pokiaľ je termín v ďalšom texte napísaný VEĽKÝMI PÍSMENAMI interpretuje sa nasledovne:

|  |  |
| --- | --- |
| Termín | Definícia |
| MUSÍ  JE POŽADOVANÝ  VYŽADUJE SA | Príslušné ustanovenie sa použije bez výnimky. |
| NESMIE  NEMÔŽE  ZAKAZUJE SA  JE ZAKÁZANÉ | Príslušné ustanovenie sa nepoužije nikdy. |
| MAL BY  ODPORÚČA SA  JE ODPORÚČANÉ | Príslušné ustanovenie sa použije vždy, s výnimkou prípadov, keď by jeho použitie vyvolalo nepriaznivé účinky. |
| NEMAL BY  NEODPORÚČA SA  NIE JE ODPORÚČANÉ | Príslušné ustanovenie sa nepoužije nikdy, s výnimkou prípadov ak je zrejmé, že jeho použitie nevyvolá nepriaznivé účinky. |
| MÔŽE  JE VOLITEĽNÝ | Uplatnenie ustanovenia je na rozhodnutí používateľa. |

* 1. Vysvetlenie pojmov a skratiek

|  |  |  |
| --- | --- | --- |
| **Pojem** | **Skratka** | **Výklad** |
| aktívum |  | Hmotné alebo nehmotné ekonomické prostriedky, ktoré pre Ústav priamo alebo nepriamo predstavuje súčasnú, alebo potenciálnu hodnotu. (Aktívami sú najmä: procesy, dáta, informácie, software, služby, objekty a priestory Ústavu). |
| autentizácia |  | Autentizácia osôb (subjektov vo všeobecnosti) je proces overenia identity. U osôb sa jedná o overenie totožnosti používateľa, t.j. zistenie, či identita, ktorú používateľ uviedol, je naozaj pravá (autentická). |
| autentizačný prvok |  | Tiež autentizačný údaj, autentizačná informácia. V prípade údaja/informácie sa jedná o údaj/informáciu, ktorá je známa len a výhradne jej vlastníkovi. Slúži na potvrdenie pravosti a dôveryhodnosti identity vlastníka. Takouto informáciou, alebo údajom je napríklad heslo, PIN, alebo grid karta.  V prípade autentizačného prvku sa spravidla jedná o elektronické hardvérové zariadenie. Používa sa v prípadoch potreby silnej autentizácie. |
| bezpečnosť |  | ochrana fyzických a informačných aktív pred stratami, ktoré by mohli vzniknúť v dôsledku incidentov |
| bezpečnostný incident |  | Udalosť, v rámci ktorej došlo ku strate integrity, alebo dôvernosti dát, zničeniu dát, prelomeniu integrity systému alebo obmedzeniu, či odmietnutiu dostupnosti služby, priestupok alebo riziko priestupku proti bezpečnostnej politike, prípadne proti akceptovateľnému použitiu bezpečnostných politík, alebo nesplnenie štandardných postupov. |
| vlastník informácie |  | Osoba ktorá má detailné znalosti o informáciách z podnikateľského hľadiska a zodpovedá za klasifikáciu informácií vo svojej kompetencii a zabezpečenie ich označenia klasifikačným stupňom. Spravidla sa jedná o manažéra organizačnej jednotky, v ktorom informácia vznikla. |
| dešifrovanie |  | Opačný proces šifrovania, t.j zmena zo zašifrovaného textu do otvoreného textu (viď „šifrovanie“). |
| externé pamäťové médium |  | Typicky CD disk, DVD disk, USB kľúč, USB disk, pamäťová karta. |
| hrozba |  | Akákoľvek okolnosť či udalosť, ktorá môže potenciálne využiť zraniteľné miesto informačných alebo fyzických aktív a spôsobiť Ústavu škodu. |
| identifikácia |  | Identifikácia objektov znamená určenie ich totožnosti.  Identifikácia osôb je proces, v ktorom sa používateľ predstavuje systému (identifikuje) ako platný používateľ. Identifikácia a autentifikácia nasledujú ako dva na seba nadväzujúce, neoddeliteľné procesy. |
| informačné aktíva |  | Všetky objekty a informácie, ktoré pre Ústav priamo alebo nepriamo predstavujú súčasnú alebo potenciálnu hodnotu, alebo ktorých narušenie integrity, dôvernosti a dostupnosti môže mať na Ústav negatívny dopad. |
| informačný zdroj |  | Na účel tohto predpisu - akýkoľvek informačný systém, ktorý poskytuje technologickú podporu poskytovaným službám, alebo ktorý umožňuje elektronické spracovanie dát. |
| IT prostriedok |  | Každý HW komponent zabezpečujúci prevádzku IT služby. |
| IT služba |  | Služba poskytovaná prevádzkou IT pre interného a externého klienta, je súčasťou servisného katalógu vytvoreného procesom SLM (Service Level Management). Podmienky a parametre poskytovania IT služby sú definované v SLA (Service Level Agreement). |
| klasifikované informácie |  | Informácie uložené v informačnom systéme, súborovom dokumente, v tlačenej podobe explicitne označené klasifikačným stupňom (Verejné, Interné, Citlivé, Prísne citlivé). Pri klasifikovaných súborových a tlačených dokumentoch sa klasifikačný stupeň nachádza vždy v pravom hornom rohu. |
| kontinuita činností |  | Schopnosť Ústavu nepretržito poskytovať služby a produkty na vopred definovanej akceptovateľnej úrovni aj v prípade incidentu, výpadku zdrojov, krízy, alebo havárie |
| monitoring |  | Vo všeobecnosti sledovanie, kontrola, získavanie informácie o stave, o pohybe, o zmene, o činnosti, o procese alebo o udalostiach a to nezávisle od vedomia sledovaného. Pravidlá pre vykonávanie elektronického monitorovania v Ústavu a zároveň zodpovednosti a právomoci zamestnancov v tejto oblasti sú stanovené samostatným predpisom. |
| neautorizovaná osoba |  | Vo vzťahu prístupu k informačným aktívam Ústavu sa rozumie fyzická osoba, ktorá nemá zo svojej pracovnej role prístup ku klasifikovaným informáciám, resp. fyzická osoba s iným ako zamestnaneckým vzťahom ku Ústavu, ktorej sa informácie netýkajú, nemá na takýto prístup povolenie od vlastníka informácií, resp. ktorá nie je oprávnená oboznamovať sa s informáciami a pristupovať k hodnotám nad rozsah, ktorý jej určený, alebo ak jej nevyplýva zo zákona. |
| obchodné tajomstvo |  | Obchodné tajomstvo sú všetky skutočnosti obchodnej, výrobnej alebo technickej povahy súvisiace s podnikom, majúce skutočnú alebo potenciálnu materiálnu či nemateriálnu hodnotu, nie sú v príslušných obchodných kruhoch bežne dostupné, majú byť podľa vôle podnikateľa utajené a podnikateľ zodpovedajúcim spôsobom ich utajenie zabezpečuje. Definované v zákone  č. 513/1991 Z.z. Obchodný zákonník v znení neskorších predpisov. |
| ochrana |  | Starostlivosť o odvrátenie nebezpečenstva; prostriedok na chránenie; prevencia - súhrn opatrení na odvrátenie alebo zmiernenie škodlivých vplyvov a následkov incidentov, mimoriadnych udalostí a krízových situácií. |
| organizačné opatrenia |  | Systém administratívnych pravidiel, ktoré vymedzujú pravidlá správania sa zamestnancov a tretích strán v súvislosti s ochranou fyzických a informačných aktív. |
| Osobné údaje |  | Osobnými údajmi sú údaje týkajúce sa identifikovanej, alebo identifikovateľnej fyzickej osoby, pričom takou osobou je osoba ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora, ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu. |
| partneri |  | Na účely tohto predpisu sú myslení zamestnanci tretích strán, pôsobiacich v Ústavu na základe zmluvného vzťahu. |
| porušenie ochrany osobných údajov |  | Porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim. |
| používateľ |  | Osoba, ktorá spracúva (vytvára, používa, mení, premiestňuje) informačné aktíva Ústavu v preddefinovaných procedúrach počas vykonávania pridelených úloh – špecificky zamestnanec Ústavu, alebo zamestnanec tretej strany. |
| priestory Ústavu |  | Priestory, ktoré sú vlastnené alebo prenajaté Ústavom a ktoré sú chránené technickými zabezpečovacími prostriedkami a mechanickými zábrannými prostriedkami |
| riešenie bezpečnostných incidentov |  | Aktivity vedúce k identifikácii, analýze, odozve na incident, odvráteniu hrozieb s úmyslom preventívne pôsobiť na možné opakovanie incidentu; návrh zrozumiteľného, predvídateľného a opakovateľného procesu odozvy na bezpečnostné incidenty. |
| riziko |  | Funkcia pravdepodobnosti, že hrozba zneužije konkrétnu zraniteľnosť a spôsobí škodlivú udalosť s následnou možnosťou ujmy, negatívneho dopadu alebo škody pre Ústav. Bezpečnostné riziko je výraz na označenie potenciálnej možnosti narušenia bezpečnosti. |
| skupina |  | Právnické osoby, priamo alebo nepriamo ovládané Ústavom. |
| Ústav |  | Organizácia. |
| šifrovanie |  | Proces zmeny otvoreného obsahu textu do nezrozumiteľnej podoby (zašifrovaného textu) použitím kryptografických metód. Operácia šifry je riadená algoritmom a kľúčom. Kľúč je tajný parameter (v zásade je známy iba príjemcovi a odosielateľovi) pre špecifickú zámenu obsahu správy. |
| tretia strana |  | Orgán verejnej moci, právnická osoba alebo fyzická osoba, ktorá vo vzťahu k dôvernej informácii a hodnotám nie je považovaná za oprávnenú osobu, pokiaľ nie je týmto predpisom určené inak. |
| udalosť (Event) |  | Akýkoľvek pozorovateľný jav v systémoch a v sieťach, (napr. prihlásenie používateľa, spustenie programu, aktivita sieťovej vrstvy a pod). Udalosť nemusí nevyhnutne indikovať bezpečnostný incident, môže však poskytnúť indície, ktoré po vyhodnotení môžu odhaliť nezvyklú aktivitu. |
| WiFi |  | Set štandardov pre zriaďovanie a prevádzku bezdrôtových lokálnych počítačových sietí v rádiofrekvenčnom pásme. Pre účely tohto dokumentu sa pod WiFi rozumie ľubovoľná počítačová sieť založená na štandarde IEEE 802.11. |
| WiFi prístupový bod |  | Zariadenie slúžiace na pripojenie bezdrôtových WiFi zariadení do WiFi siete. |
| zamestnanci |  | Na účely tohto predpisu sú myslení zamestnanci Ústavu a dcérskych Spoločností. |
| zraniteľnosť |  | Slabé miesto  fyzického alebo informačného aktíva, slabé miesto v bezpečnostných procedúrach systému, opatreniach alebo ich implementácii, ktoré môže aktivovať alebo využiť nositeľ hrozieb (hrozba). |

# CHARAKTERISTIKA PREDPISU

* 1. Bezpečnostné pravidlá uvedené v tomto predpise sú záväzné pre všetkých používateľov.
  2. Cieľom týchto pravidiel je upraviť spôsob práce s informačnými aktívami Ústavu tak, aby boli minimalizované bezpečnostné, prevádzkové, operačné a právne riziká pôsobiace na informačné aktíva Ústavu.
  3. Tento predpis sa vzťahuje na prácu s informačnými aktívami Ústavu, a to bez ohľadu na ich fyzické umiestnenie (umiestnenie vo vyhradených priestoroch Ústavu alebo mimo priestory Ústavu )..

# VŠEOBECNÉ ZÁSADY STAROSTLIVOSTI O INFORMAČNÉ AKTÍVA

* 1. Každý používateľ JE POVINNÝ používať štandardné pracovné postupy, procesy a procedúry (t.j. vnútorné predpisy a inštrukcie zodpovedných zamestnancov).
  2. Každý používateľ JE POVINNÝ chrániť všetky informačné aktíva a informácie Ústavu pred ich vyzradením neautorizovanej osobe, neautorizovanou modifikáciou alebo stratou.
  3. Zvláštnu pozornosť pri ochrane informácií pred vyzradením neautorizovaným osobám, MUSÍ každý používateľ venovať ochrane informácií klasifikovaných ako Citlivé alebo Prísne citlivé a ochrane informácií obsahujúcich bankové tajomstvo, osobné údaje alebo obchodné tajomstvo.
  4. Sprístupnenie informácií klasifikovaných ako Interné tretím stranám MUSÍ byť explicitne autorizované biznis vlastníkom informácie alebo biznis gestorom informácie.
  5. Sprístupnenie informácií klasifikovaných ako Citlivé alebo Prísne citlivé iným zamestnancom Ústavu alebo tretím stranám ako tým, ktorí sú uvedení v zozname „Prístupné pre“ uvedenom na klasifikovanej informácii, MUSÍ byť explicitne autorizované biznis vlastníkom informácie alebo biznis gestorom informácie.
  6. JE ZAKÁZANÉ spracovávať a ukladať citlivé alebo klasifikované informácie špecifikované v bode 3.3 na súkromných IT zariadeniach používateľov.
  7. Za správnu klasifikáciu informačného aktíva je zodpovedný vlastník informačného aktíva. Klasifikácia sa vykonáva v zmysle samostatnej formálnej procedúry.
  8. Pokiaľ je stanovený postup na ukladanie dát, používateľ je POVINNÝ vytvárané a upravované dáta ukladať zásadne na určené miesto, určeným spôsobom a včas.
  9. ODPORÚČA SA, aby používateľ zabezpečil pravidelné zálohovanie všetkých dôležitých dát (napr. uložením dát do domovského adresára, zdieľaného adresára odboru, adresára projektu).
  10. Neštandardné správanie sa systémov a osôb, ktoré by mohlo byť podozrením na možný bezpečnostný incident alebo príznakom prebiehajúceho bezpečnostného incidentu, je používateľ POVINNÝ bezprostredne po zistení oznámiť zodpovedným zamestnancom určeným spôsobom.

# PRAVIDLÁ MANIPULÁCIE S AUTENTIZAČNÝMI PRVKAMI

* 1. Heslá sú najdôležitejším autentizačným prvkom používateľa. Od používateľov SA VYŽADUJE, aby vytvárali heslá podľa odporučení platných pre jednotlivé systémy a zásadne ich uchovávali v tajnosti pred inými osobami (vrátane iných používateľov).
  2. Používateľ JE POVINNÝ zabezpečiť, aby iné osoby nepoužili jeho virtuálnu identitu (tzn. prihlasovacie meno, prístupové oprávnenie do systému, certifikát, používateľský profil, používateľské konto, e-mailovú adresu) - a to ani jednorazovo alebo na krátky čas, pod zámienkou zastupovania, testovania, opravy alebo úpravy systému alebo aplikácie.
  3. Aj pri krátkodobom opustení pracoviska, alebo pri strate vizuálneho kontaktu s počítačom, je používateľ POVINNÝ „zamknúť“ pracovnú plochu počítača (použitím kombinácie kláves „Ctrl-Alt-Del“ a následne kliknutím na tlačidlo „Lock Computer“, alebo použitím klávesy „Windows logo“ súčasne v kombinácii s klávesom „L“). Pri dlhodobom opustení pracoviska (napr. odchod z práce) je používateľ POVINNÝ počítač vypnúť, alebo sa z počítača odhlásiť (vykonať logoff).
  4. Používateľ zásadne NESMIE vyhovieť akýmkoľvek výzvam známych či neznámych osôb o zaslanie, prezradenie alebo zapožičanie autentizačných prvkov (napr. hesla, tokenu, PINu, certifikátu a pod.). Je prísne zakázané písať autentizačné údaje do emailov, aplikácie Service Desk, zapisovať si ich napr. na papier a ponechať ich na mieste prístupnom inej osobe.
  5. JE ZAKÁZANÉ požadovať od iných používateľov zaslanie, prezradenie, alebo zapožičanie autentizačných prvkov (napr. hesla, tokenu, PINu, certifikátu a pod.).
  6. Na vstup do informačného systému JE ZAKÁZANÉ používať heslá používané na iné ako na vopred definované účely (napr. heslá na prístup do domáceho počítača, prístup na súkromný e-mail, prístup k službe poskytovateľa internetových služieb, na registráciu na iné internetové služby, atď.).
  7. Pri podozrení na prezradenie, stratu, odcudzenie alebo odtajnenie autentizačných informácií je používateľ POVINNÝ bezodkladne zmeniť, alebo požiadať o zmenu svojich autentizačných údajov (heslo, PIN, atď.) a zároveň oznámiť podozrenie na bezpečnostný incident spôsobom uvedeným v bode 3.10 tohto predpisu.

# PRAVIDLÁ MANIPULÁCIE S HW PROSTRIEDKAMI

* 1. Od používateľa SA VYŽADUJE, aby chránil HW prostriedky Ústavu pred poškodením, alebo zničením a to tak, že sa najmä vyvaruje:
* hrubého alebo neprimeraného narábania s HW prostriedkami,
* svojvoľnému premiestňovaniu pracovných staníc, ktoré nie sú určené na mobilnú prácu (ako napr. PC, tlačiarne a pod.),
* jedeniu a pitiu nad klávesnicou pracovnej stanice alebo nad notebookom.
  1. Používatelia nie sú oprávnení akokoľvek zasahovať do konfigurácie HW prostriedkov.  Používateľom SA ZAKAZUJE, spúšťať a inštalovať na pracovných staniciach a notebookoch softvér, ktorý nebol na používanie v Ústave schválený. Výnimku z tohto ustanovenia majú pracovníci IT. Zásah do konfigurácie IT prostriedkov vykonaný pracovníkmi úseku IT však MUSÍ BYŤ vykonaný výhradne v zmysle práv a povinností, ktoré im vyplývajú z ich pracovných náplní. V žiadnom prípade NESMIE zmenou konfigurácie dôjsť k odstaveniu bezpečnostného mechanizmu alebo k zníženiu ich účinnosti.
  2. Používateľom SA ZAKAZUJE zdieľať, dať používať alebo akýmkoľvek iným spôsobom sprístupniť IT prostriedky Ústavu (napr. notebooky a mobilné telefóny) iným osobám a to vrátane rodinných príslušníkov.
  3. Používateľ zásadne NESMIE ponechávať prenosné zariadenia výpočtovej techniky (napr. notebook, mobilný telefón) prenosné médiá, resp. dokumenty obsahujúce citlivé alebo klasifikované informácie špecifikované v bode 3.3. bez dozoru, odložené v motorových vozidlách bez posádky, v reštauračných zariadeniach, dopravných prostriedkoch, šatniach, rokovacích miestnostiach a kanceláriách bez toho, aby mal prehľad o prípadnej neoprávnenej manipulácii s týmito zariadeniami, médiami, alebo dokumentmi.
  4. Prenášanie notebookov v inom ako vypnutom stave (režim spánku – „stand by“ a dlhodobého spánku – „hibernation“) mimo chránené priestory Ústavu JE ZAKÁZANÉ.
  5. JE ZAKÁZANÉ pripájať do internej počítačovej siete Ústavu cudzie zariadenia výpočtovej techniky. Akékoľvek pripojenie cudzieho IT zariadenia musí byť vopred autorizované.
  6. JE ZAKÁZANÉ pripájať IT zariadenia Ústavu do Internetu alebo obdobných sietí iným, ako schváleným spôsobom.
  7. Súčasné pripojenie IT zariadení do internej siete Ústavu a iných sieti (napr. Internet) JE ZAKÁZANÉ.
  8. JE ZAKÁZANÉ zriaďovať neautorizované bezdrôtové WiFi siete na IT zariadeniach Ústavu,, ako aj pripájanie neautorizovaných WiFi prístupových bodov k internej počítačovej sieti.
  9. Používanie súkromných mobilných zariadení na lokálne spracovanie a ukladanie citlivých informácii Ústavu je považované za výnimku z tohto predpisu a  MUSÍ BYŤ explicitne schválené.

# ZÁSADY POUŽÍVANIA APLIKÁCIÍ

* 1. JE ZAKÁZANÉ sprístupniť aplikáciu Ústavu neautorizovaným osobám, alebo klientom Ústavu a to najmä:
* sprístupnením počítača inému, než aktuálne prihlásenému používateľovi,
* natáčať monitor počítača tak, aby boli informácie z  aplikácie Ústavu čitateľné klientovi,
* povoliť klientovi vkladanie údajov do aplikácie Ústavu.
  1. Používateľom JE ZAKÁZANÉ akoukoľvek formou upravovať (mazať, kopírovať, editovať, presúvať) alebo inak zasahovať do súborov iných používateľov bez vedomia ich vlastníka.

# ZÁSADY KOMUNIKÁCIE

* 1. Používatelia SÚ POVINNÍ zaistiť dostatočné bezpečnostné opatrenia pre ochranu citlivých alebo klasifikovaných informácií špecifikovaných v bode 3.3 pri ich ukladaní, spracovaní, prevoze a prenose nezávisle od ich formy (t.j. v elektronickej podobe, fyzicky vytlačené na papieri alebo verbálne komunikované).
  2. Je PRÍSNE ZAKÁZANÉ používať pre komunikáciu citlivých informácií elektronické komunikačné kanály, ktoré neposkytujú možnosť šifrovej ochrany informácií. V prípade že je potrebné poslať citlivú informáciu elektronickým komunikačným kanálom MUSÍ byť táto informácia zašifrovaná.
  3. Na šifrovú ochranu informácii JE ODPORÚČANÉ používať iba schválený softvér, algoritmy a kľúče.
  4. Používanie neplatených a anonymných mailových a cloudových služieb SA NEODPORÚČA.
  5. Využívanie pracovnej elektronickej komunikácie na súkromný účel v rozsahu, ktorý negatívne neovplyvní riadne a včasné plnenie pracovných úloh a nie je v rozpore s bezpečnostnými pravidlami nie je v rozpore s dobrou praxou. Avšak použitie súkromných adries na pracovné účely JE ZAKÁZANÉ.
  6. Prístup na web-mailové rozhrania z nedôveryhodných zariadení SA NEODPORÚČA.
  7. Citlivé alebo klasifikované informácie špecifikované v bode 3.3 musia byť pri posielaní elektronickou poštou chránené šifrovaním. Posielanie klasifikovaných informácií špecifikovaných v bode 3.3 v akejkoľvek otvorenej, nechránenej forme JE ZAKÁZANÉ.
  8. Používateľom SA NEODPORÚČA spúšťať alebo otvárať neznáme prílohy a linky nevyžiadaných e-mailov.
  9. Používateľ NESMIE komunikovať o  citlivých alebo klasifikovaných informácií špecifikovaných v bode 3.3 na verejných miestach (napr. v reštauráciách, hromadných dopravných prostriedkoch, atď.), alebo aj pred nezainteresovanými klientmi.
  10. Používateľ NESMIE na počítačoch vytvárať zdieľané adresáre a prostredníctvom nich zdieľať informácie do verejných sietí.
  11. Na šifrovú ochranu informácii MÔŽE používateľ použiť iba Ústavom schválený softvér, algoritmy a kľúče.
  12. Dokument klasifikovaný ako Citlivé, Prísne citlivé, môže byť vydaný tretej strane výhradne so súhlasom biznis vlastníka alebo autora dokumentu. Každý elektronický dokument alebo tlačený dokument klasifikovaný ako Citlivé, Prísne citlivé, ktorý bude daný tretím stranám, musí byť registrovaný a tretia strana musí podpísať preberací protokol, ktorý určuje jej povinnosti pri manipulácii s odovzdaným dokumentom. Na ochranu klasifikovaných dokumentov v elektronickej podobe sa vzťahuje bod 9.3. Ochrana klasifikovaných dokumentov v tlačenej podobe pred neautorizovanými osobami MUSÍ BYŤ zabezpečená uložením dokumentu do obalov alebo obálok s ochranou na detekciu neautorizovaného otvorenia alebo zmeny obsahu. Prenos MUSÍ BYŤ zabezpečený autorizovanou osobou.
  13. Používateľ NESMIE používať prostriedky elektronickej komunikácie na činnosti, ktoré:
* sú v rozpore so zákonmi Slovenskej republiky, s pravidlami hospodárskej súťaže a dobrými mravmi
* by mohli poškodiť niekoho dobré meno
* by mohli viesť k úniku alebo neautorizovanému sprístupneniu citlivých informácií
* plytvajú kapacitou siete, počítačov a pracovných síl
* obmedzujú súkromie iných používateľov
* sa snažia získať neoprávnený prístup ku zdrojom na sieti
* sa snažia získať prístup ku nelegálnemu obsahu, alebo obsahu chráneného autorskými právami
* nepriaznivo pôsobia na prevádzku siete, jednotlivých sieťových služieb, alebo bránia niektorým používateľom v prístupe k týmto službám
* pôsobia výhražne, urážlivo, vulgárne, obscénne, hanlivo alebo znepokojujúco.
  1. Za takéto činnosti sa považujú a preto sú ZAKÁZANÉ najmä nasledujúce činnosti:
* posielanie, prijímanie a sťahovanie akéhokoľvek rasovo, nábožensky či etnicky motivovaného obsahu
* posielanie, prijímanie a sťahovanie akéhokoľvek nenávistne, násilne, protištátne, militantne, anarchisticky alebo teroristicky motivovaného obsahu
* posielanie, prijímanie a sťahovanie akéhokoľvek obsahu obsahujúceho, alebo propagujúceho alkohol, omamné látky, psychotropné látky, jedy, prekurzory a ostatné látky ktoré by mohli byť spôsobilé nepriaznivo ovplyvniť psychiku človeka alebo jeho ovládacie alebo rozpoznávacie schopnosti, alebo sociálne správanie
* posielanie, prijímanie a sťahovanie akéhokoľvek obsahu obsahujúceho, alebo propagujúceho hry, hazardné hry a stávky
* posielanie, prijímanie a sťahovanie akéhokoľvek erotického, pornografického, sexuálne explicitného obsahu, alebo s obsahom týkajúceho sa sexuálnych aktivít
* používanie elektronickej komunikácie na mimopracovné hromadné diskusie a komunikáciu v automatických distribučných skupinách
* používanie elektronickej komunikácie na šírenie politických názorov a osobnej reklamy
* rozosielanie, prijímanie a sťahovanie multimediálneho obsahu, ktorý priamo nesúvisí s obsahom pracovnej náplne zamestnanca
* úmyselné posielanie, prijímanie a sťahovanie škodlivého kódu
* posielanie, prijímanie a sťahovanie anonymného obsahu, t.j. obsahu bez možnosti jednoznačnej identifikácie zdroja, resp. autora
* rozosielanie a sťahovanie obsahu chráneného autorskými právami na ktorý odosielateľ nemá súhlas držiteľa práv, resp. licenciu. (napr. softvér, dokumenty, elektronické knihy a pod.)
* rozosielanie a sťahovanie nelegálneho a neautorizovane pozmeneného softvéru (warez) resp. softvéru slúžiaceho na neautorizovanú zmenu iného autorsky chráneného softvéru (cracking)
* rozosielanie a sťahovanie softvéru a informácií slúžiacich na obchádzanie bezpečnostných opatrení a hackovanie systémov
* posielanie a sťahovanie reklamy a komerčných ponúk (s výnimkou komunikácie v rozsahu pracovnej náplne zamestnanca).
* posielanie alebo komunikovanie citlivých informácií prostredníctvom elektronickej komunikácie bez adekvátnej šifrovej ochrany informácií
* používanie iných ako schválených elektronických komunikačných kanálov (freemail služby, chatovacie služby a pod.)
* akékoľvek obchádzanie bezpečnostných nastavení a obmedzení elektronických komunikačných kanálov

# ZÁSADY MANIPULÁCIE S TLAČENÝMI DOKUMENTAMI

* 1. Používatelia SÚ POVINNÍ dôsledne dodržiavať zásadu čistého stola, t.j. neponechávať v rokovacích miestnostiach a  kanceláriách po opustení pracoviska voľne dostupnú dokumentáciu, ktorá obsahuje citlivé alebo klasifikované informácie špecifikované v bode 3.3.
  2. Citlivé alebo klasifikované dokumenty špecifikované v bode 3.3 odoslané na vytlačenie, kopírované alebo faxované dokumenty je používateľ POVINNÝ bezodkladne vyzdvihnúť z tlačového výstupu tlačiarne, kopírky alebo faxu.
  3. Už nepotrebné citlivé alebo klasifikované dokumenty v tlačenej forme špecifikované v bode 3.3, ktoré nepodliehajú archivácii je používateľ POVINNÝ bezodkladne fyzicky zničiť skartovaním.
  4. V prípade, že používateľ neúmyselne získa v tlačenej forme informácie klasifikované ako Citlivé alebo Prísne citlivé je POVINNÝ tento fakt bezodkladne oznámiť biznis vlastníkovi alebo biznis gestorovi informácie a ohlásiť to ako bezpečnostný incident spôsobom definovaným v bode 3.10.

# ZÁSADY POUŽÍVANIA PAMÄŤOVÝCH MÉDIÍ

* 1. Pred prijatím neznámeho obsahu v elektronickej forme na prenosných pamäťových médiách je používateľ POVINNÝ vykonať nad obsahom aktívnu kontrolu pomocou antivírového programu.
  2. Na externom pamäťovom médiu JE ZAKÁZANÉ súčasne ukladať alebo prenášať citlivé pracovné informácie Ústavu spolu so súkromnými informáciami.
  3. Citlivé alebo klasifikované dokumenty špecifikované v bode 3.3 MUSIA BYŤ pri ich prenose na externých pamäťových médiách mimo chránené priestory Ústavu ošetrené prostriedkami šifrovej ochrany.
  4. Používateľ BY MAL dbať na to, aby na externom pamäťovom médiu, určenom na prenášanie informácií boli uložené len tie informácie, ktoré potrebuje na práve vykonávanú alebo plánovanú činnosť. ZAKAZUJE SA na externých pamäťových médiách určených na prenášanie informácií, zhromažďovať, alebo ináč agregovať citlivé alebo klasifikované dokumenty špecifikované v bode 3.3.
  5. Citlivé alebo klasifikované dokumenty špecifikované v bode 3.3, uložené na externých pamäťových médiách, MUSIA BYŤ po ukončení používania z média bezpečne zmazané (prepísaním). Alternatívou je fyzické zničenie média tak, aby sa informácie z nich nedali znovu obnoviť.

# ZÁVEREČNÉ USTANOVENIA

* 1. Riadiaci manažéri  zodpovedajú za presadzovanie zásad informačnej bezpečnosti a za správnu a včasnú klasifikáciu informačných aktív Ústavu v súlade so stanovenými pravidlami.
  2. Všetky výnimky z tohto predpisu musia byť vopred schválené. Výnimky sa zadávajú a schvaľujú výhradne písomne.
  3. Porušenie povinností vyplývajúcich z tohto predpisu môže byť považované za menej závažné až závažné porušenie pracovnej disciplíny.
  4. Tento predpis súvisí s nasledujúcimi politikami a procedúrami:
* Bezpečnostné ciele a bezpečnostná stratégia
* Pracovný poriadok
* Bezpečnostná politika
* Ochrana dôverných informácií
* Zverejňovanie dôverných informácií
* Klasifikácia informačných aktív
* Základné zásady riadenia informačnej bezpečnosti
* pre používanie internetu a elektronickej pošty

# ZÁVEREČNÉ USTANOVENIA

* 1. Táto verzia predpisu nenadväzuje na predchádzajúce verzie
  2. Tento predpis neruší žiaden iný predpis
  3. Súvisiace predpisy
* politika Riadenie informačnej bezpečnosti v platnom znení,
* politika Riadenie informačných aktív
* politika Riadenie IT služieb
* politika Audit informačnej bezpečnosti

# ZÁZNAMY

|  |  |  |
| --- | --- | --- |
| Kód dokumentu | Názov dokumentu | Zodpovedný za dokument |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |