FIXME pouze přílohy zamýšlené bezpečnostní směrnice

# Příloha č. 1: Pravidla bezpečného chování zaměstnanců (bezpečnostní minimum)

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| **0** | **Úvodní ustanovení a vysvětlení pojmů** | | | |
| | 1 | Bezpečnostní minimum obsahuje pravidla pro minimální bezpečnostní politiku organizace, se kterými byl zaměstnanec/ext. pracovník seznámen a svým podpisem na prezenční listině nebo el. potvrzením prohlašuje, že bude daná bezpečnostní pravidla dodržovat a řídit se jimi tak, aby nedošlo ke škodě způsobené organizaci-zaměstnavateli (viz další smluvní ujednání mezi oběma smluvními stranami). | | |
| | 2 | Prezenční školení bezpečnostního minima je povinné pro každého nového zaměstnance/ext. pracovníka s přístupem k citlivým datům organizace a pro každého, kdo byl přistižen při porušení těchto bezpečnostních pravidel. Pro ostatní jsou opakovaná prezenční školení dobrovolná. | | |
| | 3 | Porušení těchto bezpečnostních pravidel je porušením pracovněprávních povinností se všemi důsledky z toho vyplývajícími. Porušením pravidel se rozumí i neúčast na povinném prezenčním školení nebo nepotvrzení přečtení nové verze bezpečnostního minima. | | |
| | 4 | Pravidla jsou často závislá na sobě a zřetězená, celý systém bezpečnosti je tak silný, jak "silný" je nejslabší článek. | | praktický příklad: zamknutý dům s klíčem ve dveřích |
| | 5 | Za technické zajištění pravidel bezpečnostního minima (tzn. za bezpečnost dat) na svém IT vybavení zodpovídá jeho uživatel (zaměstnanec/ext. pracovník). | | |
| | 6 | Každý je povinen hlásit bezpečnostní incident na uvedené kontakty. | | incident@mestokm.cz;<br>Pavel Kopecký 731 555 257;<br>Petr Procházka 605 478 802 |
| | | | | bezpečnostní incident je událost, která může způsobit:<br>- narušení bezpečnosti informací v informačních systémech<br>- narušení bezpečnosti služeb a sítí elektronických komunikací<br>- únik citlivých dat |
| | | | | i jen podezření na bezpečnostní incident je incidentem! |
| | 7 | Důvěrná (citlivá) data organizace jsou blíže popsána v Příloze č. 2. | | |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | 8 | Osobní údaje jsou (dle GDPR) veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (např. jméno, adresa, rodné číslo, e-mail atd.) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. | | |
| | 9 | Subjekt údajů je (dle GDPR) každá fyzická osoba žijící v EU. | | |
| | 10 | Podoba osobních údajů: | (otevřený) osobní údaj = z údaje lze identifikovat konkrétní identitu (např. jméno, adresa, rodné číslo, e-mail atd.) | |
| | | | pseudonymizovaný osobní údaj = z údaje lze identifikovat konkrétní identitu pouze se znalostí nějakého převodního klíče (nějaký kód, např. osobní číslo zaměstnance) | |
| | | | anonymizovaný osobní údaj = z údaje nelze identifikovat konkrétní identitu (náhodný shluk znaků, hash apod.) | |
| | 11 | DPO = datový pověřenec (dle GDPR), konkrétně Ing. Bc. Martina Pinďáková | | |
| | 12 | OIT = Administrátor IT, konkrétně http://hd.mestokm.cz | | |
| | 13 | Autorizovaný = mající oprávnění přistupovat. | | |
| | 14 | Červeně zvýrazněné = změna oproti předchozí verzi dokumentu. | | |
| | 15 | Další užitečný studijní materiál: | Buď pánem svého prostoru | |
| | | | Jak na internet | |
| | | | Nebojte se internetu | |
| | | | Kybertest | |
| **1** | | **Pravidla pro zabezpečení IT vybavení** | týká se libovolného zařízení či datového média, která má přístup k (nebo obsahuje) citlivé informace | konkrétně PC/notebook, tablet, smartphone, přenosný harddisk, CD/DVD, USB flashdisk |
| | 1 | ručně zamykat obrazovku při přerušení práce | platí i u smartphone/tabletu | Windows: [Win]+[L], jak nastavit zamykání obrazovky |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | zásada prázdného displeje u zařízení bez přímého dozoru | |
| | | | na zaheslovaném zařízení nezobrazovat žádné informace (např. obsahy SMS na smartphone nebo nápovědu pro heslo) | |
| | 2 | šifrovat data na harddisku v PC/notebooku, přenosných harddiscích, flashdiscích, smartphonech a tabletech | Windows/macOS zaheslovaný MS Office nebo PDF dokument | |
| | | | Windows/macOS soubor Zip | |
| | | | Android má nativně (v některých typech/verzích se musí zapnout) | jak zapnout šifrování na Androidu |
| | | | macOS FileVault | jak šifrovat disk Macu pomocí FileVaultu |
| | | | iOS má nativně | |
| | 3 | neinstalovat nelegální nebo z pochybných zdrojů získané aplikace | mobilní aplikace je možno instalovat pouze z oficiálních zdrojů (App Store pro Apple iOS, Google Play pro Android) | schválené nedůvěryhodné aplikace viz Příloha č. 4 |
| | | | | |
| | 4 | používat sw zajišťující zabezpečení PC/notebooku | osobní firewall | zajišťuje OIT, doporučeno pro domácí PC |
| | | | antivir | zajišťuje OIT, doporučeno pro domácí PC |
| | | | blokátor reklam | zajišťuje OIT, doporučeno pro domácí PC |
| | 5 | udržovat aktuální software | BIOS v PC/notebooku aktualizovat nejpozději do 7. pracovního dne | zajišťuje OIT, doporučeno pro domácí PC |
| | | | pro smartphony/tablety platí pouze v případě, že mají přístup k citlivým datům (např. e-mail) | |
| | 6 | nepoužívat pro napájení IT vybavení veřejné USB napájecí porty | pokud je to nutné, tak používat USB data blocker | |
| **2** | **Pravidla pro bezpečnou práci s citlivými informacemi** | | | |
| | 1 | neposkytovat citlivé informace neautorizovaným příjemcům | dávat si pozor na odeslání emailu s citlivými informacemi neautorizované osobě omylem | |
| | | | nepoužívat soukromý e-mail pro pracovní komunikaci | |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | nepoužívat pracovní e-mail pro registraci soukromých služeb | |
| | | | na soukromých sociálních profilech neuvádět žádné informace týkající se záležitostí organizace | nijak nekomentovat interní poměry v organizaci; neuvádět informace týkající se kolegů, zákazníků nebo dodavatelů |
| | | | nepřistupovat do interních IS (s výjimkou webmailu organizace a cloudových služeb povolených pro interní komunikaci a sdílení dat) ze soukromého IT vybavení;<br>VPN připojení organizace používat pouze z pracovního IT vybavení (platí pouze pro interní zaměstnance) | povolené cloudové služby viz Příloha č. 3 |
| | | | neumožnit používat pracovní PC/notebook jinými osobami (a to ani rodinnými příslušníky), pokud tyto osoby na zařízení nemají vlastní profil (identitu);<br>neumožnit používat pracovní smartphone/tablet jinými osobami (a to ani rodinnými příslušníky), pokud má přístup k citlivým datům (např. e-mail) | |
| | | | zvážit nutnost uložení metadat (např. aktuální poloha a čas) v digitální fotografii (EXIF, IPTC, XMP) | |
| | | | zvážit potřebu trvale se dívající kamery na notebooku | |
| | | | zvážit nutnost ukládat citlivé informace k tel. kontaktům (adresa, foto obličeje) | |
| | | | minimalizovat množství automaticky doplňovaných formulářových polí v browseru (např. číslo bank. účtu, tel. číslo); | |
| | | | vypnout automatické vyplňování hesel (uložených v password manageru) bez potvrzení uživatelem | použití hesla z password manageru musí uživatel vždy potvrdit |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | dávat si pozor při veřejných prezentacích plochy vlastního zařízení | ukončit nepotřebné aplikace;<br>zavřít nepotřebná okna potřebných aplikací;<br>platí i pro veřejné selfpromo organizace |
| | | | při sdílení dokumentů e-mailem preferovat jeho uložení na schválené sdílené úložiště a zaslání odkazu e-mailem před přímým zasláním dokumentu jako přílohy e-mailu | |
| | | | je zakázáno sdílet e-mailem soubory otevřených osobních údajů | otevřený = nepseudonymizovaný;<br>citlivá data v e-mailu zabezpečit šifrováním |
| | | | zvážit nutnost použití, množinu příjemců a obsah automatické odpovědi na e-mail v nepřítomnosti | min. neuvádět důvod nepřítomnosti a místo, kde se během nepřítomnosti vyskytujete |
| | | | zvážit nutnost použití reálného domácího pozadí při video hovorech z home office | použít falešné nebo rozmazané pozadí |
| | 2 | citlivá data sdílet pouze přes schválená úložiště | nepoužívat přenosná média (přenosné harddisky, flashdisky, CD/DVD) pro citlivá data | |
| | | | na PC/notebooku nemít trvale zapnutá neomezená bezdrátová sdílení (např. BlueTooth nebo AirDrop) | s vyjímkou použití bezdrátové klávesnice, myši nebo tiskárny |
| | | | schválená úložiště dat jsou:<br>- interní síťové úložiště (pro libovolná pracovní data);<br>- cloudové úložiště (pouze pro data správců hesel a pro zálohy smartphone/tabletu)<br>- privátní nebo cloudové úložiště externího smluvního partnera<br>- Podklady pro radu a zastupitelstvo<br>- SeaFile | interní síťová úložiště jsou obvykle mapovaná jako lokální disky v PC/notebooku (N:, S:, X:); |
| | | | | privátní nebo cloudové úložiště konkrétního externího smluvního partnera schvaluje vedoucí OIT nebo tajemník, aktuálně je povoleno používat:<br>- E-ZAK QCM |
| | | | | návod na používání SeaFile je na Intranetu |
| | | | uvědomit si vlastní plnou zodpovědnost při akceptaci žádostí o sdílení vlastních dokumentů jiným uživatelům přes schválená cloudová úložiště | |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | pro sdílení dat a interní komunikaci používat pouze schválené cloudové služby | schválené/zakázané cloudové služby viz Příloha č. 3 |
| | 3 | vždy kontrolovat důvěryhodnost toho, kdo po mě žádá citlivé informace nebo se někde autentizovat | autorizovat každého, kdo po mně citlivé informace žádá telefonicky | |
| | | | kontrolovat el. podpis toho, kdo po mně citlivé informace (nebo se někde přihlásit) žádá mailem | |
| | | | zvýraznit (barevně odlišit) podepsané a/nebo šifrované maily v poštovním klientovi; dávat si pozor především na takto nezvýrazněné maily | |
| | | | kontrolovat validnost URL a el. certifikátu serveru, na kterém běží přihlašovací obrazovka | |
| | | | zvýraznit (barevně odlišit) zabezpečené servery v prohlížeči | |
| | | | kde je to možné, preferovat anonymní mód prohlížeče (nepoužívat cookies) | |
| | 4 | neotevírat přílohy zprávy a neklikat na odkazy ve zprávě, která není vyžádána | platí pro maily, příspěvky na soc. sítích, SMS, IM zprávy, iMessage, chatboty... | csirt.cz hinty k rozpoznání podezřelého mailu |
| | | | | govcert.cz hinty k rozpoznání podezřelého mailu |
| | | | nevyžádáná zpráva = zpráva od neznámého či neočekávaného odesílatele, ve které není na první pohled vidět jeho adresa | |
| | | | nastavit e-mail klienta tak, aby vždy zobrazoval přípony souborů v přílohách | |
| | | | na odkazy v nevyžádaných e-mailech opravdu neklikat | |
| | | | pozor na zkrácené odkazy v e-mailech | zkrácené odkazy, které je možno považovat za bezpečné:<br>- mapy.cz |
| | | | | kam ukazuje zkrácený odkaz je možno zjistit pomocí nástroje wheregoes.com |
| | | | neklikat na odkaz jiného webového sdílení než toho, které patří schválené cloudové službě | schválené/zakázané cloudové služby viz Příloha č. 3 |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | Office aplikace: zakázat všechna makra s oznámením, povolit jen důvěryhodná makra | |
| | 5 | s citlivými dokumenty pracovat pokud možno v el. podobě | pokud je nutno je tisknout, tak je po použití bezpečně zlikvidovat | |
| | | | pokud je nutno je tisknout, tak bez možnosti zneužití v procesu tisku (být fyzicky přítomen u tiskárny, tisk s odložením) a s kontrolou, že jsou skutečně kompletně vytištěny | |
| | | | pokud je nutno s nimi pracovat v papírové podobě, tak dodržovat pravidla pro fyzickou bezpečnost | |
| | 6 | neznámá datová média nevkládat do počítače | zlikvidovat je nebo předat OIT | |
| | 7 | mazat tabule a likvidovat nepotřebné flipchart papíry s citlivými informacemi ve veřejných prostorách | v zasedacích místnostech | |
| | 8 | bezpečně používat neznámé WiFi sítě | známé WiFi přístupové body jsou typicky v interní síti organizace a v domácí síti | známé a důvěryhodné WiFi sítě organizace: mukm |
| | | | pracovní IT vybavení (s výjimkou smartphone/tabletů) nikdy nepřipojovat do WiFi sítě organizace pro návštěvy | radnice_free |
| | | | vlastní (soukromé) IT vybavení připojovat v zaměstnání pouze do free WiFi sítě organizace (WiFi pro návštěvy) | |
| | | | při připojení přes neznámou WiFi síť vždy preferovat šifrované spojení (SSL) | SSL pro přístup na web: v URL musí být na začátku https://, poté je spojení šifrované |
| | | | v neznámých WiFi sítích se nikdy nikam nepřihlašovat bez šifrovaného spojení | |
| | | | nepřipojovat se automaticky k neznámým WiFi sítím | |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | zabezpečit domácí síť, pokud se do ní připojuje pracovní IT vybavení | na domácím routeru (modemu) pro připojení do internetu<br>- pravidelně aktualizovat sw;<br>- používat jiné než defaultní heslo pro administraci;<br>- vypnout možnost administrace na veřejném (WAN) rozhraní |
| | | | | na WiFi přístupovém bodu v domácí síti nastavit heslo pro připojení a šifrování WPA2 |
| | | | do captive portálu (přihlašovacího dialogu) přístupového bodu v neznámé WiFi síti nikdy nezadávat žádné údaje (max. souhlas s nějakými podmínkami) | co vyžaduje nějaké údaje, to je vysoce podezřelé |
| | 9 | zálohovat data | pro zálohování dat organizace z PC používat pouze její zálohovací nástroje | data zálohovat na osobní disk N: |
| | | | pro zálohování dat organizace ze smartphonů/tabletů používat cloudové nástroje výrobce zařízení | zálohování smarthone/tabletu nástrojem jeho výrobce schvaluje OIT |
| | | | | povolené cloudové zálohovací služby viz Příloha č. 3 |
| | | | nepoužívat zálohovací nástroje organizace pro zálohování soukromých dat uložených na zařízení organizace (typicky na pracovním PC) | |
| | | | pro zálohy důležitých dat se doporučuje dodržovat pravidlo 3-2-1 (3 kopie záloh na 2 typech médií, 1 kopie ve fyzicky jiné lokalitě) | |
| | | | životně důležitá data nosit jen bezpečně u sebe (=v hlavě) | |
| | 10 | chránit citlivá data v exportech z různých IS | preferovat pseudonymizované (nebo lépe anonymizované) exporty, tzn. obsahující minimum dat (nebo lépe vůbec neobsahující data), které vedou k odhalení konkrétní identity | |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | pokud exporty obsahuji osobní údaje, tak je šifrovat a ukládat do speciálních složek k tomu určených | speciální složka určená k ukládání exportů: kdekoli na síťovém disku N: |
| | | | nepotřebné exporty bezpečně mazat | |
| | 11 | chránit citlivá data při tvorbě analýz a souhrnných statistik | při poskytování takových dokumentů (typicky tabulek) jiným uživatelům v nich ponechat zdrojová data v anonymizované podobě | vždy z takových tabulek mazat zdrojová data obsahující osobní údaje |
| | 12 | proaktivně, pravidelně a bezpečně mazat nepotřebné soubory obsahující citlivá data | mazat soubory především z typických lokálních "odkládacích" míst:<br>- Plocha<br>- Koš<br>- složka Stahování<br>- e-mailová schránka<br>- složka pro dočasné ukládání příloh e-mailů<br>- složky k ukládání exportů na disku N: | |
| **3** | **Pravidla pro fyzickou bezpečnost** | | | |
| | 1 | zamykat zamykatelné kanceláře, skříně, zásuvky a šuplíky | pokud obsahují citlivá data | |
| | | | kanceláře zamykat v případě, že se v nich nevyskytuje žádný zaměstnanec | |
| | | | nikdo neautorizovaný nesmí mít ke klíčům přístup | |
| | 2 | upozornit na výskyt neznámých osob bez doprovodu na místech s citlivými informacemi | spisovna, odborový archiv, serverovna | |
| | | | nezaměstnanci se v těchto místech musí vždy pohybovat v doprovodu zaměstnance | |
| | | | neznámá osoba se musí být vždy schopna prokázat svým dokladem totožnosti | pokud lustrace neznámé osoby není možná, předat/nahlásit ji Městské policii |
| | 3 | nepropůjčovat vlastní vstupní přístupovou kartu/čip | nepropůjčovat svoji fyzickou identitu | |
| | 4 | neponechávat IT vybavení, AAA média a papírové dokumenty s citlivými daty bez dozoru na veřejně dostupných místech | vč. zaparkovaných aut | |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | sporadicky používané IT vybavení a média obsahující citlivá data skladovat v uzamykatelných úložných prostorách | |
| | | | AAA médium = cokoli, co slouží pro autentizaci či autorizaci (identifikační a přístupové karty a čipy, klíče, razítka...) | |
| | | | zásada prázdného stolu vzhledem ke všemu, co lze fyzicky zneužít | |
| | | | citlivá data obsahují i běžné papírové dokumenty typu:<br>- vizitky<br>- adresáře a tel. seznamy | |
| | 5 | z nepoužívaného IT vybavení před odevzdáním bezpečně smazat veškerá citlivá data | odevzdání probíhá např. při předávání hw jinému uživateli;<br>týká se i chytrých telefonů | bezpečné mazání pro Linux: shred |
| | | | | bezpečné mazání pro IOS: iShredder |
| | | | | bezpečné mazání pro Android: iShredder 3, Secure delete |
| | | | | bezpečné mazání pro macOS: srm -v, rm -P |
| | | | | bezpečné mazání pro Windows: CCleaner, Eraser |
| | | | přesunout do Koše neznamená smazat | |
| | | | na požádání před odevzdáním zajistí OIT | |
| | | | zašifrované data je nejjednodušší smazat bezpečným "zapomenutím" hesla/klíče pro šifrování | |
| | 6 | nepotřebné papírové dokumenty s citlivými daty nevyhazovat, ale skartovat | | |
| | 7 | nepotřebná datová média s citlivými daty nevyhazovat, ale bezpečně zlikvidovat | nebo předat k likvidaci OIT;<br>CD/DVD média lze sešrotovat ve skartovačce | |
| | 8 | citlivé a důvěrné záležitosti diskutovat pouze se zainteresovanými lidmi a za zavřenými dveřmi, na místě bez kamer | ani na chodbě, ani v kuchyňce, ani na toaletách, ani v restauraci... | |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| **4** | **Pravidla pro přístupové kódy** | | platí pro libovolná hesla, PINy a certifikáty | |
| | 1 | při generování jakéhokoliv hesla se řídit zásadami pro bezpečné a silné heslo | min. síla hesla:<br>- musí obsahovat alespoň 12 znaků;<br>- musí obsahovat znaky ze tří z následujících čtyř kategorií:<br>1. velká písmena anglické abecedy (A až Z);<br>2. malá písmena anglické abecedy (a až z);<br>3. základních 10 číslic (0 až 9);<br>4. jiné než alfanumerické znaky (například !, $, #, %);<br><br>pokud je délka hesla kratší než 20 znaků, tak nesmí obsahovat slovo, zkratku, jméno nebo název v libovolném jazyce;<br><br>pokud používat webové generátory hesel, tak vygenerované heslo lehce pozměnit | hinty k dodržování zásad<br>zjištění úrovně bezpečnosti hesla |
| | 2 | pokud to systém umožňuje, tak pravidelně měnit | nejpozději po 12 měsících používání | |
| | 3 | nerecyklovat | nepoužívat po čase kdysi již používané | |
| | 4 | nepoužívat stejné heslo v různých systémech | v každém systému mít unikátní heslo | neplatí pro systémy, které používají centralizovanou správu identit, konkrétně:<br>- SSL (spisová služba);<br>- VITA |
| | 5 | distribuovat pouze zabezpečeným způsobem | SMS | |
| | | | papír v zalepené obálce | |
| | 6 | pokud to systém umožňuje, tak změnit ihned po jeho přijetí od správce systému | | |
| | 7 | nesdělovat neautorizovaným osobám | nepropůjčovat svoji digitální identitu | |
| | | | nesdělovat neprověřeným osobám po telefonu, především osobám volajícím | na podezřelé volání reagovat zpětným zavoláním |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | pokud je heslo nutné sdělit OIT, tak si ho změnit co nejdříve je to možné | |
| | | | za autorizované osoby se považují pouze nadřízení (s písemným souhlasem tajemníka) a orgány činné v trestním řízení | |
| | | | zaměstnavatel má právo znát přístupové kódy k šifrovaným datům na IT vybavení v jeho vlastnictví (typicky HDD v PC/notebooku nebo zálohy dat) | |
| | 8 | pouze v rozumné míře používat přihlašování účtem třetí strany | decentralizovat svoji digitální identitu a nespoléhat se na nedůvěryhodné třetí strany jako poskytovatele identity:<br>- pro důležité přístupy používat pouze vyhrazenou identitu;<br>- nemít pro všechny přístupy pouze jeden Facebook účet;<br>věnovat pozornost tomu, ke kterým všem informacím ve vlastním účtu se třetí strana může dostat | státem provozovaný poskytovatel identity se považuje za důvěryhodný |
| | 9 | nezadávat do systému, pokud se někdo dívá | i bezp. kamera se dívá...<br>pozor na otisky prstů na displeji chytrého telefonu (rutinně otírat displej) | |
| | 10 | ukládat pouze na bezpečných místech | hlava;<br>zapečetěná obálka v trezoru;<br>specializovaná online aplikace (tzv. správce hesel, password manager), lze použít i pro bezpečné uložení PINů, certifikátů a dalšího tajemství | možné password managery: Keepass (preferováno zaměstnavatelem), Keychain Access (Klíčenka), Bitwarden |
| | | | browser není bezpečné místo pro uložení hesel, neukládat hesla přímo v něm | |
| | | | neukládat hesla v emailové schránce | |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | neukládat hesla v čitelné, nezašifrované podobě v souboru nebo ve schválených cloudových úložištích | |
| | | | neukládat hesla na papíře v blízkosti počítače | |
| | 11 | používat pouze ty bezpečnostní otázky, na které není možné uhodnout odpověď pomocí sociálního inženýrství | nebo použít nesmyslné odpovědi a ty si bezpečně uložit | |
| | 12 | kde je to možné, tam používat vícefaktorové ověření | kromě hesla se pro přihlášení k účtu použije další faktor, např.:<br>- něco mít (SMS s jednorázovým kódem, osobní čip, autentizační aplikace)<br>- někým být (biometrický údaj, např. otisk prstu)<br>- někde být (geolokační údaj, např. aktuální poloha) | |
| | | | 2FA = dvoufaktorové ověření (např. heslo a jednorázový SMS kód) | |
| | | | pokud možno používat pouze ty aplikace, které 2FA umožňují (Google, iCloud, Dropbox, Facebook, Twitter, el. bankovnictví) | |
| | | | zásadně používat 2FA u veřejných účtů organizace na sociálních sítích | |
| | | | zásadně používat 2FA u poštovních účtů, které slouží pro zajištění jednorázového přístupu bez hesla do systému, do kterého bylo ztraceno/zapomenuto heslo | |
| | 13 | rušit nepoužívané přístupové účty | bezpečně smazat odpovídající přístupové kódy | |
| | 14 | okamžitě změnit při podezření na únik | | |
| **5** | **Pravidla pro biometrická data** | | definice biometrie | |

| Číslo | | Pravidlo | Poznámka | Upřesnění, technické opatření |
|---|---|---|---|---|
| | | | jako podklad pro biometrická data slouží typicky:<br>- otisk prstů<br>- vzorek DNA<br>- vlastnoruční podpis<br>- fotografie vlastního obličeje nebo oční sítnice<br>- záznam vlastního hlasu | |
| | 1 | chránit vlastní biometrická data | ke všem biometrickým datům se chovat jako k citlivým údajům | |
| | | | neukazovat bříška prstů (prsty do Victory) do objektivu fotoaparátu | |
| | | | nerozdávat biometrické (citlivé) data bez vědomí jejich majitele | |
| | | | nevystavovat na internet fotografie/video osob bez jejich souhlasu | |
| | | | neidentifikovat obličej (ani svůj, ani cizí) na fotografiích uložených v sociálních sítích a na svém vlastním účtu dobře zvážit, zda povolit/zakázat tuto identifikaci (min. Facebook to povolit/zakázat umožňuje) | |

# Příloha č. 2: Citlivá data organizace (zaměstnavatele)

| | | |
|---|---|---|
| 1 | veškeré skutečnosti organizačního, technického, investičního, finančního, účetního, daňového, právního, smluvního, administrativního, pracovně-právního, manažerského nebo strategického charakteru souvisejícího s činností organizace, které nejsou běžně dostupné | vč. ekonomických plánů a výsledků organizace, účetních dokladů, smluvních dokumentů, technických konfigurací a logů veškerého používaného hw/sw a záloh dat |
| 2 | veškeré osobní údaje fyzických osob, se kterými přijde uživatel do styku; jde zejména o osobní údaje ostatních uživatelů, občanů, obchodních partnerů a jejich zástupců či zaměstnanců | |
| 3 | přístupová hesla a jiné prostředky ochrany a zabezpečení informací organizace | |
| 4 | obsah vnitřních předpisů organizace | |
| 5 | údaje o mzdových podmínkách organizace (včetně mzdových podmínek uživatele) | |
| 6 | jiné skutečnosti, které by mohly přivodit újmu organizaci, včetně poškození obchodních zájmů nebo dobrého jména | |
| 7 | skutečnosti, které organizace výslovně za citlivé (důvěrné) označí | |

## Příloha č. 3: Cloudové služby

| |
|---|
| cloudové služby zakázané pro interní komunikaci a sdílení dat |
| Facebook Messenger |
| uloz.to |
| Google Disk |
| cloudové služby povolené pro interní komunikaci a sdílení dat |
| CESNET OwnCloud |
| CESNET FileSender |
| cloudové služby povolené pro sdílení dat mezi vlastními zařízeními |
| *- vlastní zařízení je libovolné zařízení, které používám pouze já (pracovní i soukromé)* |
| *- je zakázáno je používat pro sdílení dat se zařízeními někoho jiného* |
| Bitwarden |
| iCloud |
| cloudové služby povolené pro zálohování dat |
| iCloud *(pouze v případě, že je stejný iCloud účet používán i pro sdílení dat mezi vlastními zařízeními)* |
| cloudové služby výrobců Android smarthonů (Google, Samsung cloud, Huawei cloud, Xiomi cloud, Lenovo Cloud) |

## Příloha č. 4: Software

| schválené nedůvěryhodné aplikace |
| --- |
| PDF Creator v 1.7.3 |