

Povinné postupy pro zajištění ochrany osobních údajů při používání ICT technologií

1. **Zamykejte svoje zařízení.** Počítač, notebook, tablet či smartphone nesmí být ponechán bez dozoru odemčený (s přihlášeným uživatelem). Při opuštění pracoviště s počítačem, na kterém je uživatel přihlášen svým jménem a heslem, je uživatel povinen se buď odhlásit, nebo uzamknout počítač (klávesa s logem Windows + L) a u mobilního zařízení stisknutím zamykacího tlačítka.
2. **Ukládejte soubory přednostně na osobní síťový disk X:.** Soubory obsahující osobní údaje je v případě notebooku nutné ukládat na osobní síťový disk X: Na sdílený síťový disk R: je možné takové údaje ukládat, pouze pokud uživatel zná přidělená přístupová oprávnění, tj. ví, jaké další osoby mají do dané složky přístup a tyto osoby jsou zároveň oprávněné s těmito údaji pracovat. Přidělená přístupová oprávnění pro jednotlivé složky na síťovém disku R: lze ověřit na intranetu ČRo v části [NÁVODY -> APLIKACE A SYSTÉMY -> SÍŤOVÉ SLOŽKY](#). Pokud uživatel ve výjimečných případech potřebuje ukládat tyto soubory na lokální disk (C:), je povinen požádat OIT o zašifrování tohoto disku (toto opatření je ochrana proti zcizení, a proto má smysl zejména u notebooků).
3. **Přístupujte zodpovědně k volbě hesel.** Přístupujte zodpovědně k volbě hesel a chraňte je před zcizením nebo vyzrazením. Nikdy nesdělujte jiným osobám přihlašovací údaje a hesla k vlastním účtům a službám. Nepoužívejte stejná hesla doma a v práci. Toto doporučení platí dvojnásob v případě údajů, pomocí kterých se přihlašujete do práce vzdáleně. V případě úspěšného útoku na domácí počítač je většinou snadné z prohlížečů a e-mailových klientů získat uložené přihlašovací údaje. Útočník by neměl být schopen přihlásit se pomocí hesla soukromého e-mailu také k tomu pracovnímu, případně někam dále. Vhodným způsobem pro uchovávání hesel je použití správce hesel jako je např. KeePass (můžete jej nainstalovat z aplikace Software Center). Ukládání hesel ve webových prohlížečích není pokládáno za příliš bezpečné, protože existuje několik postupů, jak uložená hesla vzdáleně odcizit. Doporučujeme si znovu projít školení NÚKIB Základy kybernetické bezpečnosti „Dávej kyber“, kde právě jedna z prvních kapitol je věnovaná tvorbě hesel.
4. **Důvěrné údaje, které posíláte ven, chraňte šifrováním.** Při komunikaci se subjekty mimo doménu ČRo není tato komunikace chráněna šifrováním a nelze ji tedy považovat za zcela zabezpečenou. V těchto případech je nutné důvěrné či citlivé údaje (např. obchodní tajemství, citlivé osobní údaje, údaje o majetkových poměrech fyz. osob jako jsou například údaje o mzdě apod.) uvést v příloze e-mailu a tuto přílohu zašifrovat pomocí komprimačního programu (WinZip, 7-Zip, WinRAR apod.). Heslo k příloze je nutné doručit příjemci jinou cestou než e-mailem (např. SMS).

Interní e-mailová komunikace (v rámci stejné domény) je bezpečná, protože je ve všech krocích šifrovaná. Zde není nutno provádět další šifrování. V odůvodněných případech lze pro komunikaci se subjekty mimo doménu ČRo nastavit ve spolupráci s OIT šifrování e-mailů s vybranou protistranou. Jedná se především o pravidelnou komunikaci s třetími subjekty, se kterými si vyměňujeme informace, které je třeba chránit. Návod na použití služby šifrování pomocí komprimačního souboru je Návod na použití služby Úložna je na intranetu v části NÁVODY -> ... ->



Návod na vytvoření
komprimovaného ZI

5. **Větší přílohy posílejte přes interní službu Úložna.** V případě příloh větších než 15 MB je nutno použít interní službu Úložna. V případě, že soubor bude obsahovat důvěrné údaje dle předchozího odstavce, je nutné jej opět zašifrovat. Nezaměňujte interní Úložnu s veřejnými službami jako je např. Úschovna. Přístup k Úložně je na intranetu ČRo, v menu: VSTUP DO APLIKACÍ – ÚLOŽNA / SDÍLENÍ SOUBORŮ. Návod na použití služby Úložna je na intranetu v části NÁVODY -> ... ->



Návod pro aplikaci
ulozna.docx

6. **Pravidelně zálohujte.** Data je nutné chránit proti ztrátě pravidelným a bezpečným zálohováním. Proto se doporučuje pracovní data ukládat pouze na síťové disky, které jsou pravidelně zálohovány (soukromý disk X:, nebo sdílený síťový disk R:, do složek, u nichž uživatel zná přidělená přístupová oprávnění viz výše bod 2).
7. **Externí zařízení chraňte šifrováním.** Při ukládání osobních údajů na externí zařízení, jako jsou externí disky a USB flash disky, je uživatel povinen tato zařízení zabezpečit šifrováním. K tomu je možné použít například BitLocker, který je součástí operačního systému vašeho pracovního počítače. Zabezpečíte tím data pro případ ztráty nebo zcizení externího zařízení. Návod na použití služby šifrování pomocí BitLockeru je na intranetu v části NÁVODY -> ... ->



Návod pro
BitLocker.docx

8. **Neznámá externí zařízení nepřipojujte do svého počítače.** Je nutné vyvarovat se použití neznámých externích úložišť, jako jsou USB flash disky a jiná paměťová média. Mohou obsahovat škodlivý kód, který se takto dostane do počítače.
9. **Vyhýbejte se veřejným Wi-Fi sítím.** Snažte se vyhýbat veřejným Wi-Fi sítím. Vždy preferujte připojení přes mobilní data. Pokud se potřebujete připojit k veřejné Wi-Fi síti a následně k systémům provozovaným na vnitřní infrastruktuře ČRo, je nezbytné použít zabezpečeného spojení VPN (kromě připojení k poštovnímu serveru ČRo v rámci ČR). Pokud se potřebujete připojit k veřejné Wi-Fi síti a následně k systémům provozovaným mimo ČRo, tj. k veřejným internetovým službám jako jsou např. cloudové služby, sociální sítě apod., VPN ČRo toto spojení nezabezpečí, a proto v takových případech neposílejte osobní údaje, ani jiné citlivé údaje. K veřejným

internetovým službám je připojení bezpečné pouze pomocí známé dobře zabezpečené Wi-Fi sítě nebo pomocí mobilních dat. Dbejte na pečlivé zabezpečení vlastní domácí Wi-Fi sítě, ve které provozujete služební zařízení.

10. **Bud'te ostražití při komunikaci na internetu a podezřelé e-maily hlase na spam@rozhlas.cz.** Při zpracovávání příchozích e-mailů je nutné být ostražitý a vyvarovat se reagování na phishingové zprávy. Tyto zprávy lze identifikovat podle toho, že se na adresáta snaží působit naléhavě nebo výstražně, adresa odesílatele není běžná nebo mohou obsahovat odkaz na stránku pro zadání přihlašovacích údajů. Je nutné pečlivě kontrolovat adresy v odkazech na webové stránky (naještěm ukazatele myši na odkaz bez kliknutí). Po případném kliknutí na odkaz je nutné zkontrolovat následně adresní řádek v prohlížeči. Vždy důkladně kontrolujte, kam zadáváte své přihlašovací údaje a v případě podezřele vypadající zprávy si telefonicky ověřte, zda není podvržená. Pokud přesto své přihlašovací údaje vyplníte, neprodleně si změňte své heslo. V případě obdržení takového e-mailu je vhodné to nahlásit jednoduše přeposláním e-mailu na adresu spam@rozhlas, která byla k tomuto účelu zřízena.
11. **Bezpečnostní incidenty vždy včas ohlaste.** Bezpečnostní incident v oblasti osobních údajů hlase Oddělení právních služeb. Upozorňujeme na povinnost nahlásit každý možný bezpečnostní incident. Jeho nahlášení je povinností každého zaměstnance zejména v těchto případech:
 - bylo ztraceno nebo zcizeno zařízení nebo dokument, které obsahovalo soubor osobních údajů;
 - byl neoprávněně osobě umožněn přístup k osobním údajům v zařízení nebo v dokumentu;
 - osobní údaje v jakékoli formě byly umístěny bez přiměřené ochrany přístupu na místě, kde se k nim mohl neoprávněně někdo dostat;
 - osobní údaje byly poškozeny nebo ztraceny;
 - osobní údaje mohly být změněny nebo upraveny, ale není možné ověřit, zda se tak stalo.