Ochrana důvěrných informací – pravidla pro zaměstnance.

Nutnost ochrany důvěrných informací

Při své práci můžete přicházet do styku s informacemi, které mohou být předmětem obchodního tajemství, nebo se může jednat o osobní údaje. V případě, že je použijete nevhodným způsobem, pak můžete způsobit zaměstnavateli škodu. V případě obchodního tajemství můžete poškodit zájmy firmy, v případě osobních údajů vzhledem k platnosti nařízení EU 2016/679 (GDPR) o ochraně osobních údajů, může dojít k jejich úniku a zaměstnavatel může být pokutován vysokými sankcemi.

Důvěrné informace

Osobní údaje a informace, které jsou předmětem obchodního tajemství, jsou považovány za důvěrné informace. Dále bude uváděn jen termín důvěrné informace.

Oprávněné osoby

S důvěrnými informacemi mohou zacházet jen oprávněné osoby. Všichni zaměstnanci přicházející do styku s osobními údaji, jsou povinni zachovávat mlčenlivost a bezpečnostní opatření, jejichž porušení by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání. Přehled aktiv obsahujících důvěrné informace a odpovědné osoby, které jsou oprávněné nakládat s těmito informacemi, je uveden v tabulce č. 1.

Tabulka č. 1

Název aktiva	Kategorie	Odpovědná osoba
Evidence pro nábor zaměstnanců	Papírové dokumenty	manažer pro nábor
Osobní spisy zaměstnanců	Papírové dokumenty	personalista
Databáze Personalistiky a Mezd	Data	personalista
Datové soubory MS Office pro personální a mzdové evidence	Data	personalista
Archiv účetních dokladů	Papírové dokumenty	účetní
Náhradní plnění - databáze odběratelů	Data	administrátor
Datové soubory v různých formátech (MS Office apod) - poptávky, nabídky, marketingové analýzy	Data	vedoucí obchodního úseku
Finanční analýzy, ekonomické výstupy, rozpočty apod.	Data	manažeři středisek, účetní
Registr obchodních smluv	Data	vedoucí sekretariátu
Firemní PC, notebooky, smartphony	Počítačový hardware	dle přidělení
Kamerový systém se záznamem	Ostatní hardware	velitel PCO

Osobní komunikace

Pokud sdělujete informace uvnitř firmy nebo navenek, vždy byste měli vědět, zda a komu tyto informace můžete sdělovat nebo předávat. V případě pochybností se informujte u svého vedoucího.

- Nebavte se na veřejnosti o pracovních záležitostech, zejména pokud nevíte, kdo všechno vás může slyšet a neznáte dobře osoby, se kterými komunikujete.
- Ověřujte si, zda osoba, která po vás vyžaduje nějakou informaci, má oprávnění ji získat.

Zacházení s informacemi

Obchodní informace a osobní údaje mohou být v papírové i elektronické podobě. Může se jednat o doklady, smlouvy, různé sestavy, soubory v různých formátech, fotografie, video záznamy apod.

- Dodržujte pravidlo čistého stolu – nenechávejte na stole ve své nepřítomnosti dokumenty s těmito typy informací.
- Tyto dokumenty nevyhazujte do koše, ale provádějte jejich skartaci, nebo je uložte do bezpečnostního boxu.
- Když tiskněte dokumenty na sdílené tiskárně, zajistěte, aby se nedostaly k neoprávněným osobám a kontrolujte, zda se vám vytiskly všechny strany.
- Po skončení pracovní doby uzamkněte skříně a zásuvky s uloženými dokumenty obsahujícími důvěrné informace.

Používání IT zařízení zaměstnavatele

IT zařízení, která jsou vám svěřena zaměstnavatelem (PC, notebooky, tablety, smartphony apod.), jsou nastavena tak, aby byla měla potřebnou funkčnost a úroveň bezpečnosti. Z těchto důvodů:

- Neinstalujte na ně žádné aplikace. V případě potřeby nějaké aplikace kontaktujte IT oddělení.
- Nezasahujte do nastavení firemních IT zařízení. Pokud potřebujete nějakou úpravu nastavení, kontaktujte IT oddělení.

Používání soukromých zařízení

Používání soukromých zařízení je ve firemní síti zakázáno. Nepřipojujte do firemní (Wi-Fi) sítě svá soukromá zařízení. Wi-Fi připojení „OLM2_HOST“ je určeno pouze pro hosty na centrále.

Používání médií

Je zakázáno používat ve firmě jakákoli soukromá media (USB flash disky, CD- ROM/RW/RAM, DVD-ROM/RW/RAM, externí HDD, SSD apod.). Při používání firemních IT zařízení je možné používat pouze media, která jsou vydávaná a evidovaná IT oddělením.

Používání mobilních zařízení

Pokud máte přidělený firemní smartphone nebo tablet, jste povinni ho chránit.

- Mobilní zařízení mějte u sebe nebo uložené tak, aby ho nikdo bez vašeho vědomí nemohl používat.
- Ukládejte ho vždy na bezpečné místo, aby bylo zabezpečeno proti krádeži. Nenechávejte ho v autě, hotelových pokojích a podobných prostorách bez vašeho dohledu.
- Pro přístup do mobilního zařízení používejte PIN (heslo apod.).

Používání autentizačních předmětů

Pokud máte přidělený autentizační předmět (USB token, kartu, čip apod.), jste povinni ho používat pouze stanoveným způsobem.

- Autentizační předmět nikomu nepůjčujte.
- Chraňte autentizační předmět před krádeží a neoprávněným použitím. Za jeho neoprávněné použití nesete veškerou odpovědnost.

Oprávnění k používání systémů

Přístup do softwarových systémů je řízen pomocí stanovených oprávnění, která se vztahují k uživatelským jménům a heslům. V případě, že někdo jiný použije vaše jméno a heslo, pak veškerou odpovědnost za jeho použití systému nesete vy.

- Nikdy nezadávejte heslo tak, aby jej někdo jiný mohl odpozorovat.
- Heslo nikomu jinému nesdělujte, heslo si nikam nezapisujte.
- Nejhorší a běžně rozšířenou chybou je zapisování na papírek nalepený na monitoru.
- Nepoužívejte stejné heslo do více systémů.
- Dodržujte pravidlo čistého monitoru – při vzdálení od počítače uzamkněte obrazovku pomocí spořiče obrazovky s heslem.

Používání internetu

Při procházení webových stránek vytváříte záznamy o tom, které stránky jste navštívili a ze kterého počítače. Vzhledem k tomu můžete nevhodným chováním na Internetu poškodit svého zaměstnavatele.

- Nestahujte z Internetu aplikace, hudbu a filmy.
- Nepřispívejte do diskusních fór s výjimkou odborných fór, která jsou schválena a evidována IT oddělením
- Nesurfujte po nedůvěryhodných stránkách.
- Při zadávání přístupových hesel na internetových stránkách kontrolujte, zda je webová stránka zabezpečená. To poznáte například podle ikonky zámečku na liště internetového prohlížeče, nebo tak, že adresa webové stránky začíná zkratkou https.
- Osobní informace zadávejte vždy pouze na internetových stránkách, které bezpečně znáte.

Používání e-mailu

Při používání e-mailu můžete obdržet e-maily se škodlivým kódem, který následně může způsobit různé potíže – znemožnit používání vašeho počítače nebo firemních serverů, odesílat soubory z vašeho počítače na adresu hackera, rozesílat spamy na adresy z vašeho seznamu a jiné. Proto dodržujte tyto zásady:

- Neotevírejte e-maily, které jste obdrželi z pochybných adres, neznámých adres, s pochybným předmětem nebo e-maily podezřelé, že jsou spam. Takové e-maily ihned mažte, případně nastavte blokování odesílatele (v MS Outlook).
- Neotevírejte soubory přiložené v e-mailech, které nejsou od známých osob a které jste si i od známých osob nevyžádali nebo neočekáváte. Pokud si nejste jistí, raději si od nich ověřte, zda vám danou přílohu skutečně zasílali.
- Neklikejte na odkazy v e-mailech, kterým plně nedůvěřujete. Buďte velmi opatrní, pokud odesílatel požaduje, abyste se přihlásili na nějakou webovou stránku a zadali či aktualizovali informace o účtu, heslu, číslu karty apod.

- Do e-mailů nevkládejte důvěrné informace, jako jsou přístupová jména a hesla, čísla karet apod.

Používání vzdáleného přístupu

Pokud používáte připojování do firemního informačního systému pomocí vzdáleného přístupu, je nutné dodržovat tato pravidla:

- Nepřipojujte se přes nezabezpečené Wi-Fi sítě, mohou být odposlouchávány a útočník může získat přístup k datům ve vašem počítači.
- Nepřipojujte se vzdáleně z neznámých počítačů např. v internetových kavárnách, nelze vyloučit, že mohou zaznamenávat zadávaná jména a hesla.

Hlášení incidentů

Pokud při používání vašeho IT zařízení zjistíte, že dochází k neobvyklému chování, může to mj. znamenat, že probíhá kybernetický útok nebo došlo k nákaze počítačovým virem.
Informujte neprodleně svého nadřízeného nebo přímo osobu odpovědnou za IT bezpečnost.

Zpracoval: Mgr. Miroslav Olejár – jednatel