**Obec Jindřichov**

# Směrnice pro užívání IT techniky a počítačových programů

## 1. Všeobecná ustanovení

### 1.1. Vlastnictví

Data, která jsou vytvářena v počítačových systémech organizace, se stávají jejím vlastnictvím a podléhají přiměřené míře utajení. Informace, které zaměstnanec zpracovává a vytváří, mohou být klasifikovány jako citlivé, důvěrné nebo podléhající zvláštnímu režimu, např. podle zákona č. 101/2000 Sb. o ochraně osobních údajů. Citlivými informacemi mohou být například (avšak nejen): vnitřní sdělení, obchodní tajemství, informace krizového řízení, osobní data zaměstnanců a funkcionářů. Zaměstnanci jsou povinni učinit všechny nezbytné kroky, aby zabránili neautorizovanému přístupu k těmto informacím.

Udržujte svoje hesla v bezpečí a nesdílejte přístupová oprávnění.

### 1.2. Bezpečnost

Všechny počítače používané zaměstnanci a připojené k počítačové síti, Internetu či Intranetu, ať již jsou vlastnictvím organizace nebo zaměstnanců, musí mít trvale spuštěn program chránící před škodlivým software s pravidelně aktualizovanou databází. Zaměstnanci musí být mimořádně opatrní při otevírání příloh elektronické pošty přijatých od neznámého odesílatele, protože tyto mohou obsahovat viry nebo jiný škodlivý kód.

Zprávy elektronické pošty odeslané zaměstnanci z účtů elektronické pošty organizace do diskusních skupin na Internetu musí obsahovat výslovné upozornění, že vyjádřený názor je výhradně jejich soukromým názorem, s výjimkou zpráv odeslaných v souvislosti s výkonem práce.

Přenosné počítače nesmí být používány na veřejných místech, pokud pracují s aplikacemi organizace, není-li to z demonstračních důvodů. Jsou-li přenosné počítače ponechány bez dozoru, musí být bezpečně uzamčeny.

### 1.3. Nepřijatelné používání

Za žádných okolností není zaměstnanci společnosti dovoleno se zúčastnit jakýchkoliv aktivit, které jsou nelegální z pohledu národních či mezinárodních zákonů, použít při tom prostředky ve vlastnictví organizace a to na úrovni lokální počítačové sítě i internetu. Následující aktivity jsou všeobecně zakázány. Níže uvedený seznam není vyčerpávající, avšak snaží se poskytnout rámec pro určení aktivit spadajících do kategorie nepřijatelného užívání prostředků výpočetní techniky.

#### 1.3.1. Systémové a síťové aktivity

a. Porušovat práva jakékoliv osoby nebo organizace chráněná autorským právem, obchodním tajemstvím, patentem nebo jiným druhem ochrany duševního vlastnictví, nebo podobných zákonů a nařízení, včetně (avšak ne pouze) instalace nebo šíření „pirátských“ kopií nebo jiného programového vybavení, které není náležitě licencováno pro použití v organizaci.

b. Kopírovat materiály chráněné autorským právem (ale nejen jím) digitalizovat a šířit fotografie z časopisů, knih nebo jiných zdrojů chráněných autorským právem, autorským právem chráněnou hudbu, a instalovat jakýkoliv software chráněný autorským právem, k němuž nemá organizace nebo uživatel řádnou licenci, je přísně zakázáno.

c. Vnášet zlomyslné a škodlivé programy jako jsou viry, červi, trojské koně apod. a umísťovat je v počítačové síti nebo na servery.

d. Vnášet a instalovat na počítače společnosti jakýkoliv software bez vědomí a povolení starosty a správce sítě.

e. Prozradit hesla ke svým účtům jiným osobám nebo povolit jiným osobám pracovat pod svým účtem. To včetně vlastních rodinných příslušníků a členů domácnosti v případě, že práce je vykonávána doma.

f. Použít výpočetních prostředků organizace k aktivnímu získávání nebo přenášení materiálů, které jsou v rozporu se zákony a předpisy o sexuálním obtěžování nebo nepřátelském pracovním prostředí podle Zákoníku práce.

g. Vytvářet klamavé nabídky produktů nebo služeb pod jakýmkoliv uživatelským účtem v organizaci.

h. Vytvářet prohlášení o zárukách, výslovně vyjádřených nebo odvozených, s výjimkou případů, kdy je to součástí řádných pracovních úkolů.

i. Využívat bezpečnostních mezer nebo vytvářet útoky na komunikaci v počítačových sítích. Bezpečnostní mezery zahrnují přístup k datům, jichž není zaměstnanec zamýšleným příjemcem, přihlašování na server nebo účet zaměstnancem, který není k tomuto přístupu výslovně oprávněn, s výjimkou případů, kdy tyto aktivity jsou součástí řádných pracovních úkolů.

j. Provádět port scanning (zjišťování otevřených síťových portů) nebo security scanning (bezpečnostní skenování) je výslovně zakázáno s výjimkou případů, kdy je toto prováděno po předchozím oznámení správci sítě.

k. Provádět jakoukoliv formu monitorování počítačové sítě, které může vést k zachycení dat, která nejsou určena pro počítač příslušného zaměstnance, pokud tato aktivita není součástí jeho řádných pracovních úkolů.

l. Obcházet autentizaci uživatele nebo obcházet zabezpečení jakéhokoliv počítače, počítačové sítě nebo uživatelského účtu.

m. Provádět jakékoliv aktivity vedoucí k omezování nebo odepírání služeb jiným uživatelům než sám sobě (například útokem denial of service - DOS).

n. Užívat jakékoliv programy, skripty nebo příkazy, nebo zasílat zprávy v jakékoliv formě, s úmyslem omezit nebo znemožnit poskytování služeb nebo terminálových relací, lokálně nebo přes počítačovou síť, Internet nebo Intranet.

o. Poskytovat informace o zaměstnancích nebo seznamy zaměstnanců organizace osobám nebo organizacím stojícím mimo organizace, pokud tato aktivita není součástí řádných pracovních úkolů.

#### 1.3.2. Komunikace a elektronická pošta

a. Zasílat elektronickou poštou nevyžádané zprávy, zejména reklamního či nabídkového charakteru, které způsobují příjemci dodatečné výdaje nebo jej obtěžují.

b. Jakákoliv forma obtěžování pomocí elektronické pošty či telefonu, ať již řečí, frekvencí, nebo velikostí zpráv.

c. Neautorizovaně používat nebo padělat hlavičky zpráv elektronické pošty.

d. Žádat o zasílání zpráv elektronické pošty na další adresy, jiné než je adresa odesílatele pošty, s úmyslem obtěžovat nebo sbírat odpovědi.

e. Vytvářet nebo rozesílat řetězové dopisy nebo jiné formy tzv. pyramidových her.

f. Používat nevyžádaných zpráv elektronické pošty vytvořených v počítačové síti organizace nebo jiných poskytovatelů internetu v zájmu nebo k nabídce jakýchkoliv služeb adresátům umístěným v adresáři organizace, nebo připojených k síti organizace.

g. Neúčastnit se diskuzí v internetových fórech.

## 2. Práva a povinnosti zaměstnavatele

2.1. Zaměstnavatel umožní zaměstnanci ukládání a využívání dat na technických zařízeních zaměstnavatele (např. na pevných discích pracovních stanic a serverů) a využívání dat z výměnných médií. Rozsah tohoto oprávnění zaměstnance stanoví příslušný zaměstnanec zaměstnavatele, který je dále také oprávněn rozhodnout o změně tohoto oprávnění.

2.2. Zaměstnavatel se zavazuje umožnit v rámci uděleného oprávnění ukládání dat, jejich užívání a přístup k nim, pokud není omezení tohoto oprávnění nutné v zájmu provozu technických prostředků zaměstnavatele.

2.3. Zaměstnavatel je oprávněn nakládat s veškerými daty a softwarem na všech médiích zaměstnavatele pokud toto není v rozporu s právy třetích osob.

2.4. Zaměstnavatel určí pověřené pracovníky, kteří budou moci provádět instalace, opravy či jiné formy nakládání s počítačovými programy. Jejich seznam a kontaktní informace budou zveřejněny e-mailem všem pracovníkům organizace.

2.5. Zaměstnavatel je povinen poskytnout zaměstnanci základní proškolení, na kterém jej seznámí s ustanoveními vycházející z tohoto dokumentu a podle potřeby se základními pravidly při práci s ICT.

2.6. Zaměstnavatel poskytne zaměstnanci specifikační list počítače, aby byl zaměstnanec seznámen s tím, které programové produkty je oprávněn používat.

## 3. Práva a povinnosti zaměstnance

3.1. Zaměstnanec je povinen používat prostředky ICT (počítač, tiskárny, kopírky, telefony, přístup na Internet apod.) pouze k plnění svých pracovních povinností a v souladu s účelem, ke kterému byly ICT určeny.

3.2. Zaměstnanec není oprávněn provádět instalace, opravy či jiné formy nakládání s počítačovými programy (včetně případných instalací počítačových programů vlastněných uživatelem nebo instalace počítačových programů získaných prostřednictvím Internetu). Tyto úkony může provádět jen pověřený pracovník, který vždy také zajistí příslušnou aktualizaci specifikačního listu. Zaměstnanec musí oznámit požadavek na některý z požadovaných úkonů pověřené osobě, popřípadě svému bezprostřednímu nadřízenému.

3.3. Zaměstnanec nesmí používat programové vybavení, které není uvedeno ve specifikačním listě počítače. Zjistí-li, že kromě počítačových programů, uvedených ve specifikačním listu, se v počítači nachází i jiný počítačový program, je zaměstnanec povinen bezodkladně tuto skutečnost oznámit pověřené osobě nebo svému přímému nadřízenému. Zaměstnanec potvrdí svým podpisem na specifikačním listu počítače, který využívá, že byl seznámen s tím, které programové produkty je oprávněn používat.

3.4. Pokud zaměstnanec potřebuje pro svou práci používat software, který není uvedený ve specifikačním listě, musí požádat o jeho používání a instalaci pověřenou osobu, popřípadě svého bezprostředního nadřízeného.

3.5. Zaměstnanec nesmí jakýmkoliv způsobem dále šířit (a to ani bezúplatně) jakýkoliv počítačový program, který je součástí ICT. Počítačové programy se mohou používat pouze v souladu s licenčními podmínkami pro daný typ počítačových programů.

3.6. Zaměstnanec nesmí používat, či poskytnout jiným uživatelům, jakékoliv neoprávněně získané klíče, dekodéry či jiné technické prostředky sloužící k zajištění informační bezpečnosti a ochraně počítačových programů.

3.7. Zaměstnanci nesmí odstranit jakékoliv informace, označení či zařízení identifikující nositele či vykonavatele autorských práv k počítačovým programům, autora či jinou oprávněnou osobu.

3.8. Zaměstnanec nese plnou odpovědnost za obsah dat, která uložil nebo využívá v rámci svého oprávnění (přístupových práv) nebo jejichž uložení či využití umožnil. Zaměstnanec bere na vědomí své povinnosti vyplývající z obecně závazných právních předpisů vztahujících se k autorským a jiným příbuzným právům třetích osob. Toto platí pro data i software zmiňovaných subjektů.

3.9. Zaměstnanec není oprávněn ukládat, instalovat a hrát jakékoli počítačové hry.

3.10. Zaměstnanci nesmí vytvářet nebo pozměňovat data s cílem ovlivnit (mást) kontrolu oprávněnosti použití počítačových programů.

3.11. Zaměstnanec je povinen absolvovat základní proškolení, na kterém se seznámí s ustanoveními vycházejícími z tohoto dokumentu a podle potřeby se základními pravidly při práci s ICT.

3.12. Každé podezření na výskyt škodlivého software musí zaměstnanec neprodleně oznámit pověřené osobě nebo přímému nadřízenému. Stejně tak musí být hlášeno podezření na nesprávnou funkci ochranného programu. Každé obdržené varování před škodlivým software (například elektronickou poštou) musí být předáno pouze správci sítě. Uživatelům není povoleno šířit varování ostatním uživatelům, ať již uvnitř organizace nebo vně. Program chránící před škodlivým software musí být bez výjimek trvale spuštěn na každé pracovní stanici nebo přenosném počítači. Uživatel pracovní stanice má zakázáno pokoušet se o vypnutí nebo znemožnění činnosti programu chránícího před škodlivým software. Uživatelé mají zakázáno poskytovat cizím osobám včetně rodinných příslušníků a zejména sdělovacím prostředkům informace o případném výskytu škodlivého software v organizaci, jeho dopadech a postupech při řešení nákazy. Uživatelé mají přísně zakázáno škodlivý kód aktivně vytvářet nebo šířit. Napomáhání šíření škodlivého software, ať již úmyslně nebo z nedbalosti, bude považováno za porušení pracovní kázně.

## 4. Práva a povinnosti pověřených pracovníků (správce sítě)

4.1. Pověřený pracovník je povinen po každé instalaci, opravě nebo aktualizaci zajistit aktualizaci příslušného specifikačního listu.

4.2. Pověřený pracovník není oprávněn ukládat, instalovat a používat programy v rozporu s jejich licenční smlouvou.

4.3. V případě vzniku požadavku na instalaci počítačového programu, na která nemá organizace licenci, je povinen před instalací zajistit pořízení příslušné licence.

4.4. Pověřený pracovník nese plnou odpovědnost za obsah dat, která uložil nebo využívá v rámci svého oprávnění (přístupových práv) nebo jejichž uložení či využití umožnil. Pověřený pracovník bere na vědomí své povinnosti vyplývající z obecně závazných právních předpisů vztahujících se k autorským a jiným příbuzným právům třetích osob. Toto platí pro data i software zmiňovaných subjektů.

4.5. Pověřený pracovník se s nejvyšší prioritou věnuje každému podezření na výskyt škodlivého software. Je povinen zapsat (nebo zajistit zápis) do zvláštního záznamu a zajistit místo (ICT prostředky), kde k incidentu došlo. Pracovník řídící práce při řešení nákazy se přednostně věnuje identifikaci a určení rozsahu napadení. Je-li to vhodné, vyžádá si podporu externích specialistů. Při tom je oprávněn omezit provoz nebo zastavit subsystémy a zastavit práci uživatelů s cílem omezit šíření nákazy. Jestliže tato opatření přesahují jeho pravomoci, uvědomí o této skutečnosti Manažera bezpečnosti IT, který zajistí prosazení adekvátních opatření. V organizaci, kde je pouze jeden oprávněný správce sítě, vykoná výše uvedené činnosti on sám.

4.6. Pověřený pracovník není oprávněn ukládat, instalovat a hrát jakékoli počítačové hry.

## 5.5. Závěrečná ujednání

5.1. Zaměstnanec je povinen uhradit zaměstnavateli náhradu škody vzniklé v souvislosti s porušením jeho povinností plynoucích z tohoto dodatku.

5.2. Pokud je zaměstnavatel podle tohoto dodatku oprávněn stanovit, měnit či omezit práva zaměstnance, je povinen to zaměstnanci včas oznámit.

5.3. Zaměstnavatel je oprávněn změnit či omezit práva zaměstnance plynoucí z tohoto dodatku v souladu s příslušnými pracovně právními předpisy v případě, že takový postup je nezbytný k zabránění vznikající nebo hrozící škodě a k zajištění řádného plnění pracovních úkolů zaměstnanců nebo z jiných vážných důvodů v souladu s právními předpisy.

5.4. Vnitřní směrnice pro užívání počítačových programů a ostatních prostředků ICT se řadí mezi dokumenty interní legislativy, vstupuje v platnost dnem podpisu a platí do odvolání.

V Jindřichově dne 16.4.2018

-----------------------------------

Vlastimil Adámek, starosta