AKADEMICKÉ GYMNÁZIUM

škola hlavního města Prahy

Štěpánská 22, 110 00, Praha 1

tel.: +420 221 421 931, fax :+420 221 421 957 e-mail: agstepanska@agstepanska.cz http://www.agstepanska.cz

Směrnice pro zajištění ochrany osobních údajů při práci s ICT

1. Pravidla práce s výpočetní technikou

1.1 Členění uživatelů sítě, zabezpečení uživatelských účtů

Uživatelé počítačové sítě jsou členěni s ohledem na své pracovní zařazení, pracovní náplň a také na zastávanou pozici v organizační struktuře školy. Na základě tohoto rozčlenění získávají jednotliví zaměstnanci/uživatelé přístup do jednotlivých informačních systémů a příslušných pracovních adresářů na síťových discích. Povinností každého uživatele je mazat takové soubory, které vytvořil, ale již je nepotřebuje a nepoužívá.

1.2 Pravidla pro uživatelská jména a přístupová hesla

Všichni uživatelé sítě LAN mají přiděleno uživatelské jméno a musí dodržovat následující pravidla pro uživatelské heslo:

- Nikomu jej nesdělovat a udržovat jej v tajnosti;
- Nikam ho nezaznamenávat (vyjma bezpečného způsobu – šifrování);
- Měnit jej kdykoliv dojde k jeho kompromitaci;
- Nesmí být založeno na skutečnosti, kterou může někdo snadno odhadnout nebo ji získat z osobních údajů (jména, data narození, rodné číslo, telefonní číslo apod.);
- Hesla nezačleňovat do jakýchkoliv automatizovaných přihlášení;
- Nesdílet hesla, která byla individuálně přidělena konkrétnímu uživateli;
- Pravidla pro sestavení hesla stanovuje správce sítě, heslo by mělo mít alespoň 8 znaků, obsahovat malá i velká písmena, číslice, případně také speciální znaky;
- heslo pravidelně měnit.

V případě, že uživatel své heslo ztratí nebo získá podezření, že by mohlo být zneužito, je povinen tuto skutečnost neprodleně ohlásit správci IT a požádat jej o zablokování daného hesla. Prozrazení hesla představuje bezpečnostní incident.

1.3 Administrátorský účet

Administrátorský účet nesmí být využíván pro běžnou pracovní činnost, heslo pro tento účet musí být stanoveno podle pravidel uvedených výše.

1.4 Bezpečné přihlašovací procedury

Při bezpečném přihlašovacím postupu je zajištěno:

- Ochrana autentizačních údajů (hesla), heslo není zobrazováno přímo, ale pomocí zástupných znaků;
- Přihlašovací informace je předávána mezi stanicí a serverem pomocí šifrované komunikace;
- Informační systém nepodává uživateli žádné informace o průběhu přihlašování, dokud není uživatel bezpečně a úspěšně přihlášen.

2. Přístupová práva k souborům a adresářům na síťových discích

2.1 Zřízení přístupových oprávnění

Při zřizování přístupových oprávnění vždy o vytvoření uživatelského přístupu do počítačové sítě, informačních systémů a na datová úložiště žádá ředitel školy správce IT. Přístup je zřizován vždy pro konkrétního podřízeného pracovníka s ohledem na jeho pracovní zařazení a pozici v organizační struktuře. Ředitel školy zodpovídá za to, aby byl rozsah poskytnutého oprávnění v souladu s pracovním zařazením konkrétního zaměstnance. Správce IT následně na základě žádosti zajistí zřízení přístupů a předání uživatelských oprávnění konkrétnímu uživateli. Pokyny ke zřízení přístupových oprávnění musí být archivovány.

2.2 Změny v přístupových právech

Požadavky na změny v přístupových oprávněních k adresářům, souborům nebo aplikacím opět schvaluje ředitel školy, obvykle na základě žádosti uživatele. Schválené požadavky (písemná podoba, změny se evidují a archivují) následně k realizaci obdrží správce IT.

2.3 Odebrání přístupových práv

Při změně pracovního zařazení, ukončení pracovního poměru apod. jsou všechna přístupová oprávnění a uživatelské účty zablokovány. O provedení blokace se provádí záznam. Při zablokování účtů z důvodu ukončení pracovního poměru jsou účty zachovány po dobu 2 měsíců, následně jsou správcem IT ze serveru zcela odstraněny.

2.4 Pravidla elektronické výměny dat a informací

Jsou zavedeny procedury pro ochranu výměny informací (elektronická komunikace, použití hlasových, faxových a video komunikačních zařízení, případně též FTP) při splnění následujících bezpečnostních požadavků:

- Každý uživatel je poučen o možnostech kopírování, modifikací a zničení sdílených informací, případně o možnosti odposlechu neveřejných informací;
- Každý uživatel je obeznámen s postupy a nástroji pro detekci a ochranu před škodlivými kódy, které mohou být přenášeny elektronickou komunikací (antivirové programy);
- Uživatelé, osoby smluvních a třetích stran mají zodpovědnost (často smluvně garantovanou), že nezneužijí data, která si se školou vyměňují například zasíláním reklamních sdělení, řetězovým zasíláním e-mailových zpráv apod.;
- Dokumenty, které obsahují osobní údaje, musí být bezprostředně po tisku odebírány z tiskárny či kopírky;
- Uživatelé jsou poučeni, aby v nezabezpečených webech nezadávali žádné osobní údaje, neveřejné informace a podobně.

2.5 Pravidla pro používání e-mailové komunikace

Přidělené schránky elektronické pošty (e-mailové schránky) s doménovým jménem školy smí být používány výhradně pro emailovou komunikaci související s výkonem práce.

Uvedené e-mailové schránky nesmí být používány pro odesílání nebezpečně (nešifrovaně) zabezpečených citlivých informací. Dále nesmí být služební e-mail využíván pro odesílání nelegálního obsahu (videa, hudba apod.) a soukromou korespondenci.

2.6 Pravidla pro používání informačních systémů

Práce s informačními systémy školy a v nich obsaženými osobními údaji se řídí zejména pokyny a nařízeními ředitele/ředitelky školy, případně správce IT. Uživatelé těchto informačních systémů a aplikací musí dbát především na dodržování následujících pravidel:

- Používat informační systémy výhradně k pracovním účelům;
- Používat přístupová hesla do informačních systémů a aplikací používaných ve škole v souladu s pokyny pro používání hesel (viz výše);

2.7 Pravidla pro využívání Internetu

Veřejnou celosvětovou síť Internet lze používat pouze k plnění pracovních úkolů, je třeba dbát zvýšené obezřetnosti (výskyt škodlivých programů). Je zakázáno stahování a instalace jakéhokoliv SW přístupného z internetu na pracovní stanici, toto může výhradně v odůvodněných případech provést správce IT nebo jím pověřený pracovník.

3. Bezpečnost práce v síti

Cílem a smyslem níže uvedených opatření je zamezit neúmyslnému i úmyslnému poškození dat, jejich zničení či odcizení nebo vyzrazení neoprávněným osobám. Z pohledu uživatele se tato opatření projevují žádostí o zadání uživatelského jména a hesla při přihlašování a také omezeným přístupem do příslušných adresářů.

Bezpečnostní opatření:

- Uživatelské jméno a heslo;
- Data uložená na síťových discích není povoleno poskytovat osobám, které nejsou k organizaci v pracovním či jiném právním vztahu;
- Data v jakékoliv formě a podobě nesmí být vynášeny z prostor školy bez souhlasu nadřízeného;
- Veškerá data z cizích zdrojů a vyměnitelná záznamová média (především přepisovatelná: CD, DVD, flash disk, externí HDD) musí být před použitím prověřena antivirovým programem, zda neobsahují viry.

3.1 Antivirová ochrana, ochrana před škodlivými programy

Ochrana před počítačovými viry a škodlivými programy je v zařízeních realizována prostřednictvím antivirového programu (AVG Bussines by Avast), který je nastaven tak, že probíhá automatická aktualizace.

Uživatelům PC stanic a dalších prostředků IT je zakázáno jakkoliv měnit chod a nastavení antivirového programu. Pokud je nalezen vir, který není možné pomocí instalovaného antivirového programu běžně odstranit, je uživatel zařízení povinen na tuto skutečnost bezprostředně po zjištění upozornit správce IT.

Všichni uživatelé PC jsou povinni při používání přenosných přepisovatelných médií před tím, než otevřou soubor uložený na takovém médiu, spustit antivirovou kontrolu daného média.

4. Bezpečnost dat sítě LAN

Přístup k datům v prostředí sítě LAN je zajištěn prostřednictvím přístupových práv přiřazených jednotlivým uživatelským účtům.

4.1 Zabezpečení rozhraní sítě internetu

Síť LAN je před hrozícím externím nebezpečím chráněna prostřednictvím instalace bezpečnostní brány na rozhraní internetu a vnitřní PC sítě. Smysl bezpečnostní brány spočívá v tom, že umožní přístup pouze bezpečných a podporovaných komunikačních protokolů.

4.2 Zabezpečení neobsluhovaných stanic

Každý uživatel počítačové stanice je povinen, se při jejím opouštění, byť jen na krátký časový úsek, odhlásit nebo stanici uzamknout, aby bylo zamezeno neoprávněnému přístupu k datům.

Externí přístupy do počítačové sítě

Přístupy ke zdrojům a systémům uvnitř PC sítě musí být zabezpečeny prostřednictvím VPN připojení, to je realizováno prostřednictvím IPSec, SSL VPN apod. Externí přístupy lze zřídit vybraným uživatelům či dodavatelům pouze na základě schválení ředitelem školy.

Zřízení přístupu probíhá na základě formálního schválení. Přístupy jsou přidělovány vždy na základě žádosti příslušného vedoucího pracovníka po schválení ředitelem školy. Odpovědnost za zřízení a přidělení přístupu nese správce IT.

5. Pravidla používání přenosných prostředků mimo prostory školy

Pokud je uživateli z řad zaměstnanců školy přidělen přenosný prostředek (flash disk, notebook, paměťová karta apod.), který plánuje používat mimo školu, je povinen dodržovat následující pravidla:

- Prostředek nesmí předat třetí osobě, pokud to nevyplývá z pracovní povinnosti;
- Pracovat tak, aby bylo zabráněno případné možnosti odezírat informace z displeje notebooku/PC neoprávněnými osobami;
- Provést všechna opatření, která povedou k zabránění případné ztráty či odcizení daného prostředku (nenechat bez dozoru, zabezpečení v dopravních prostředcích, hotelech apod.);
- Hlásit okamžitě nadřízenému případnou ztrátu či odcizení prostředku;

Datové nosiče přenosných prostředků, které obsahují osobní údaje, musí využívat šifrovací SW (např. komprimovaný soubor, zip či rar s ochranou pomocí hesla), za dodržování tohoto pravidla je zodpovědný uživatel prostředku.

6. Správa, obnova a údržba výpočetní techniky

Smyslem údržby a obnovy výpočetní techniky je uchovat ji v bezproblémovém a bezporuchovém chodu a také zajištění dostatečného výkonu prostředků výpočetní techniky ve vztahu k počtu používaných aplikací.

6.1 Záznamy o činnostech a zásazích na serveru

Musí být založen a veden provozní deník, který slouží k zaznamenávání všech zásahů a změn ke kterým na serveru dochází. Provozní deník lze vést také v elektronické podobě. Auditní záznamy o činnosti serveru musí být zálohovány a archivovány.

6.2 Hlášení chyb a požadavků, záznamy

Požadavky na prostředky výpočetní techniky (poruchy, závady, nefunkčnost apod.) sdělují jednotliví uživatelé přímo správci IT (písemně v elektronickém deníku závad výpočetní techniky, e-mailem). Nesnese-li odstranění problému odkladu, nebo nelze-li e-mail odeslat, lze správce IT kontaktovat také telefonicky.

6.3 Údržba osobních PC

Správce IT zodpovídá za plánování a provádění údržby hardware osobních PC, dojde-li k nekorektnímu chování počítače, je uživatel povinen o tom informovat správce IT.

6.4 Údržba LAN sítě

Údržbu počítačové sítě (HW i SW) zajišťuje správce IT dle pokynů, které pro jednotlivé produkty (síťové komponenty) dodávají jejich výrobci či dodavatelé.

6.5 Zálohování dat na serverech

Data uložená na síťových úložištích jsou zabezpečena před jejich ztrátou prostřednictvím zálohování na záložní média, zálohování dat provádí správce IT (inkrementální a plné zálohování ve stanoveném časovém intervalu), proto se na něj také obracejí uživatelé v případě, že potřebují, aby byla určitá data obnovena.

6.6 Správa a údržba PC stanic v síti

Všechny PC stanice jsou zařazeny do domény školy a není povoleno jejich svévolné vyřazování z domény, to lze pouze po předchozím schválení. Uživatelé jsou povinni se k síti hlásit prostřednictvím svého doménového účtu.

Pro možnost dálkových i lokálních zásahů do sítě je pro každou stanici povoleno přihlášení administrátora (lokální skupina Administrators). Je zakázáno odebírat tuto skupinu a jakkoliv omezovat její práva ve stanici.

6.7 Likvidace datových nosičů, bezpečné mazání dat

Datové nosiče, které obsahují informace s osobními údaji a jiné neveřejné informace školy (diskety, CD-ROM, flash disky, HDD apod.) určené k vyřazení musí být odevzdány správci IT, který zajistí jejich bezpečné smazání či fyzickou likvidaci nosiče, aby byla minimalizována možnost obnovy dat z takového nosiče. Bezpečné smazání/fyzická likvidace je prováděna následujícím způsobem:

- CD-ROM, DVD-ROM: rozřezáno pomocí skartovacího stroje;
- CD-RW, DVD-RW: rozřezáno pomocí skartovacího stroje nebo smazáno pomocí SW pro bezpečné mazání dat;
- Flash disky: funkční disky budou smazány pomocí SW pro bezpečné mazání dat, u nefunkčních bude fyzicky zlikvidován paměťový čip;
- HDD, SSD: funkční disky budou smazány pomocí SW pro bezpečné mazání dat, u nefunkčních proběhne provrtání v oblasti ploten disků, nebo rozebrání a fyzická likvidace;
- Zálohovací kazety: funkční kazety budou smazány pomocí SW pro bezpečné mazání dat, u nefunkčních kazet proběhne rozebrání a páska bude rozstříhána.

O likvidaci dat bude sepsán příslušný záznam/protokol.

6.8 Sledování událostí a audit síťových služeb a serverů

Na řadiči domény bude provedeno nastavení logování následujících událostí:

- Přihlášení do domény – úspěšné/neúspěšné;
- Lokální přihlášení - úspěšné/neúspěšné;
- Management uživatelských skupin a účtů - úspěšné/neúspěšné;
- Změny lokálních a doménových politik - úspěšné/neúspěšné;
- Privilegované operace - úspěšné/neúspěšné;

- Systémové události - úspěšné/neúspěšné;

Na dalších serverech je prováděno auditování stejných událostí jako na doméně, s výjimkou přihlášení do domény. Dále je logován přístup k informačním systémům, souborům a adresářům obsahujícím osobní údaje.

Závěr: *Touto směrnicí jsou povinni se řídit v rámci svých pracovních povinností všichni zaměstnanci školy a rovněž další osoby, které jsou k organizaci v obdobném právním vztahu (zaměstnanci pracující formou dohody o práci konané mimo pracovní poměr, osoby spolupracující na základě smlouvy apod.).*

Materiál je závazný pro:	všechny zaměstnance a žáky školy
Platnost:	od 1. 3. 2019
Aktualizace:	průběžně
Kontrola:	1x ročně
Zpracoval:	Mgr. Tomáš Raja, Ph.D.
Kontakt:	221 421 936
Připomínkovali:	vedení školy
Schválil:	PaedDr. Milan Štěrba

V Praze dne 28. 2. 2019

PaedDr. Milan Štěrba
ředitel AG