Článok 4
Zálohovanie a archivovanie údajov

1. Zamestnanci sú povinní zabezpečiť zálohovanie aplikácií nainštalovaných na im zverenom počítači minimálne raz za týždeň.
2. Médiá so záložnými údajmi musia byť uložené v inej miestnosti, než sa nachádza počítač, z ktorého boli záložné údaje vyhotovené.

Článok 5
Prístupové práva

1. Zamestnanci nesmú mať heslá kratšie ako 8 znakov. Zamestnanec nesmie ako heslo použiť takú kombináciu znakov, ktorú by bolo možné priradiť k jeho osobe, akými sú napríklad meno používateľa a jeho rodinných príslušníkov napísané spredu či odzadu, telefónne číslo domov alebo na pracovisko a podobne. Heslo musí obsahovať minimálne jedno veľké písmeno, jedno číslo alebo špeciálny znak.
2. Zamestnancom sa zakazuje zverejňovať alebo vyzradiť prihlasovacie údaje (heslá) inej osobe. Taktiež sa zakazuje držanie záznamu hesiel (napr. na papieri, v softvérovom súbore alebo prenosnom zariadení), ak takýto záznam nemôže byť bezpečne uložený.
3. Používateľ sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený.
4. Po skončení pracovného pomeru je poverená osoba povinná odobrať odchádzajúcemu zamestnancovi jeho prihlasovacie údaje a zmeniť ich tak, aby sa mu znemožnil ďalší prístup.

Článok 6
Pracovné stanice

1. Zamestnanec je povinný používať zverené pracovné stanice len na pracovné účely. Porušenie tohto ustanovenia sa považuje za bezpečnostný incident.
2. Zamestnanec môže na pracovných staniciach používať výlučne len programové vybavenie nainštalované Správcom IT, resp. nainštalované s jeho preukázateľným súhlasom. Zamestnanec nemôže na pracovnej stanici meniť žiadne programové vybavenie, a tiež nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými sa mení vzhľad pracovného prostredia.
3. Zamestnanec je zodpovedný za dodržiavanie autorských práv a licenčných podmienok, ktoré sa vzťahujú k programom, súborom, grafike, dokumentom, správam a ostatným materiálom, ktoré má v úmysle inštalovať, sťahovať, zverejňovať alebo kopírovať.
4. Zamestnanec nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici.
5. Zamestnanec je pred opustením pracoviska povinný ukončiť prácu s aplikačným programovým vybavením, odhlásiť sa zo siete a operačného systému a dohliadnuť na vypnutie pracovnej stanice.
6. Pri krátkodobej neprítomnosti môže zamestnanec nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky s heslom, resp. jej uzamknutím.
7. Zamestnanec je povinný po inštalácii novej verzie programového vybavenia po dobu minimálne jedného týždňa venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadné odchýlky od požadovaného stavu je povinný čo najúplnejšie zdokumentovať a bezodkladne ohlásiť Správcovi IT.
8. Zakazuje sa pripájať do siete školy vlastné zariadenia (napr. notebooky, PDA, tlačiarne a pod.), a taktiež povoliť pripojenie cudzej osoby do siete školy bez vedomia správcu. Taktiež sa zamestnancom zakazuje používať vlastné USB kľúče na archiváciu osobných údajov, alebo databáz osobných údajov, alebo akýchkoľvek súborov s osobnými údajmi. Porušenie tohto bodu sa považuje za bezpečnostný incident.

Článok 7
Zamestnanci externej organizácie

1. Prístup zamestnancov externej organizácie do informačných systémov zriaďuje Správca IT.
2. Správca vydá zamestnancovi externej organizácie prístupové heslo a práva.