3. Správca IT je povinný zabezpečiť bezpečný šifrovaný prístup zamestnanca tretej strany.
4. Zamestnanci externej organizácie sú povinní pred prihlásením sa do informačného systému školy o tejto skutočnosti oboznámiť Správcu IT, a to buď prostredníctvom mailu, alebo telefónom. Na základe tohto oznámenia im Správca IT povolí pripojenie. Po skončení údržby alebo inej činnosti zamestnancom externej organizácie, Správca IT zruší možnosť pripojenia.
5. Poverená osoba je povinná poučiť zamestnancov externej organizácie o ochrane a mlčanlivosti ohľadom osobných a citlivých údajov. Táto skutočnosť by mala byť zakomponovaná do zmluvy s externou organizáciou.

Článok 8
Prístup do siete internet a mailová komunikácia

1. Každý zamestnanec, ktorému bol umožnený prístup do siete internet, je povinný rešpektovať nasledovné zásady:
   a. Prístup do siete internet využívať predovšetkým v súlade so svojou pracovnou náplňou.
   b. Dodržiavať etické zásady a zdržiavať sa činností, ktoré by mohli viesť k poškodeniu dobrého mena pracoviska alebo k iným škodám.
   c. Komunikácia v internete spravidla nie je chránená pred "odpočúvaním". V prípade potreby prenosu osobných údajov je nevyhnutné ich pred prenosom zabezpečiť šifrovaním. Ak nie je zamestnanec schopný prenos takto zabezpečiť, nie je prípustné ho uskutočniť.
   d. Je zakázané zo siete internet preberať nelegálny obsah (softvér, súbory chránené autorskými právami a pod.).
2. Výber blokovaných stránok je v kompetencii prevádzkovateľa. V prípade veľkého prenosu objemu dát nesúvisiacich s pracovnou činnosťou zamestnanca vyplývajúceho z výsledkov webovej analýzy, má právo prevádzkovateľ zakázať a znemožniť užívateľovi prístup do internetu.
3. Zamestnanec je povinný zabezpečiť správne adresovanie príjemcu mailovej správy a na prenos správ používať všeobecne dané dátové štandardy.
4. V prípade posielania citlivých a osobných údajov, zamestnanec je povinný použiť kryptovanú komunikáciu za použitia kryptovacieho kľúča.
5. Používať elektronickú poštu len na legálne účely. Obsah dát odosielaných v rámci siete školy a cez internet nesmie byť v rozpore s dobrými mravmi.
6. Je zakázané používanie pracovnej elektronickej pošty na súkromné účely.
7. Rešpektovať zákaz posielať reťazové a hromadné e-maily, reklamné správy a pod..
8. Vedenie školy môže zamestnancovi kontrolovať obsah odosielaných a prijímaných mailových správ.

Článok 9
Antivírová ochrana

1. Správca IT je zodpovedný za zabezpečenie antivírovej ochrany a za inštaláciu a pravidelnú aktualizáciu softvéru potrebného na zabezpečenie tejto ochrany.
2. V prípade, že sa na pracovnej stanici zamestnanca zobrazí varovanie, že sa na disku alebo prenosnom médiu nachádza vírus alebo iný škodlivý kód, zamestnanec nesmie toto varovanie ignorovať. V prípade, že zavírené prenosné médium patrí inému subjektu, zamestnanec ho označí ako zavírené a vráti majiteľovi. V prípade zavírenia vlastného pevného disku alebo prenosného média, zamestnanec túto skutočnosť bezodkladne oznámi Správcovi IT.
3. V prípade objavenia vírusu v prijatej elektronickej pošte, zamestnanec bezodkladne o tejto udalosti upovedomí Správcu IT. V žiadnom prípade zavírenú elektronickú poštu neposiela inému adresátovi a na svojej pracovnej stanici ju uschová len dočasne a len na žiadosť Správcu IT (na účely ďalšej analýzy prieniku vírusu do systémov pracoviska.).