**BEZPEČNOSTNÁ POLITIKA IT PRE OCHRANU OSOBNÝCH ÚDAJOV – MINIMÁLNE POŽIADAVKY**

Tento dokument obsahuje minimálne požiadavky na ochranu osobných údajov pri ich uchovávaní a spracovávaní pomocou výpočtovej a komunikačnej techniky v rámci spoločností skupiny PPA CONTROLL. Podrobná Bezpečnostná politika IT je dostupná na www.ppa.sk/politiky
V zátvorke sú uvedené čísla bodov v podrobnej Bezpečnostnej politike IT, v ktorých sa ku konkrétnemu bodu z tohto dokumentu nachádzajú podrobnejšie informácie.

**Prístup nepovolaných osôb k údajom**

1. Dokumenty a dáta obsahujúce osobné údaje a ostatné firemné informácie, ktoré nie sú vyslovene označené ako verejné nesmú byť prístupné cudzím osobám bez dozoru kompetentnej osoby našej spoločnosti a cudzie osoby si nesmú z nich robiť kópie. (6.)
2. Neuzamknuté počítače, mobily a tablety a dátové nosiče nesmú byť dostupné cudzím osobám bez dozoru kompetentnej osoby z našej spoločnosti, a ani nesmú byť ponechané bez dozoru na miestach a vozidlách, kde by mohli byť odcudzené (6.)

**Heslá a práva**

3. Prístup k obsahu počítačov, mobilov, tabletov musí byť zabezpečený heslom podľa pravidiel spoločnosti (7.1 – 7.10)
4. Pred odchodom pracovníka z miestnosti musí byť obrazovka počítača uzamknutá (7.36 – 7.41)
5. Pri strate, alebo prezradení hesla musí jeho vlastník zabezpečiť zmenenie hesla buď sám, alebo o to požiada pracovníkov IT (7.7)
6. V prípade odchodu pracovníka zo spoločnosti dá jeho nadriadený podnet pracovníkom IT na zrušenie jeho prístupových práv, v prípade zmeny pracovného zaradenia dá podnet na ich príslušnú úpravu (7.14)

**Práca s počítačom**

7. Každý počítač a mobilné zariadenie pristupujúce do počítačovej siete spoločnosti musí používať aktualizovaný antivírový program (7.42 – 7.47)
8. Pri každom zistení alebo podozrení na stratu osobných dát, alebo iného bezpečnostného problému musí na to pracovník okamžite upozorniť pracovníkov IT (7.20)
9. Používateľ počítača nesmie vykonávať žiadne neoprávnené zásahy do neho a meniť nastavenia a obchádzať akékoľvek bezpečnostné pravidlá ani svojvoľne inštalovať akékoľvek aplikácie (7.16)

**Manipulácia s údajmi**

10. Dáta a dokumenty spoločnosti nesmú byť používané na iný účel, ako boli určené (7.16)
11. Osobné údaje a citlivé údaje spoločnosti sa smú prenášať na dátových nosičoch, len v zašifrovanej forme, alebo musia byť tieto dátové nosiče zašifrované (7.23 – 7.26)
12. Osobné údaje sa majú na prenosných zariadeniach a dátových nosičoch nachádzať len po nevyhnutnú dobu (7.26)
13. Používateľ je povinný ukladať firemné údaje na servery, ktoré sú pravidelne zálohované, alebo ak nemá túto možnosť, zabezpečovať pravidelné zálohovanie údajov na individuálne pridelené zálohovacie médiá (7.51 – 7.53)

**Maily a internet**

14. Osobné údaje sa smú pomocou mailu prenášať len v zašifrovanej forme, hlavne ak sa jedná o prenášanie väčšieho množstvo osobných údajov (7.48 – 7.50)
15. Neotvárať a neklikať na akékoľvek odkazy (tzv. linky) umiestnené v podozrivých mailoch od neznámych alebo akokoľvek inak podozrivých odosielateľov, ani v podozrivej pošte od známych odosielateľov (7.19)
16. Osobné údaje prenášané cez internet musia byť zašifrované (7.20)
17. Z verejného internetu je povolené pristupovať do lokálnej počítačovej siete len s využitím šifrovaného prenosu pomocou VPN (7.21 – 7. 22)

**Vlastné počítače**

18. Vlastné počítače, tablety a mobily pracovníkov spoločnosti, alebo externých spolupracujúcich externých pracovníkov smú byť do lokálnej počítačovej siete pripojené len ak sú o tom informovaní pracovníci IT a tieto zariadenia sú pracovníkmi IT, majú inštalovaný aktualizovaný antivírus a sú pracovníkmi IT otestované na výskyt vírusov (7.27 – 7.32)

Ďakujeme Vám, že budete chrániť svoje dáta