PROSPERIS ALBA
KUTATÓKÖZPONT

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Hatályos: 2021.04.01.

Csanády László

ügyvezető

Prosperis Alba Kutatóközpont Nonprofit Kft.

8000 Székesfehérvár, Oskola utca 2-4.
www.prosperisalba.hu
iroda@prosperisalba.hu
+36 22 202 028

Az IBSZ célja:

Jelen informatikai biztonsági szabályzat (a továbbiakban IBSZ) célja, hogy a Prosperis Alba Kutatóközpont Kft. (a továbbiakban társaság) informatikai rendszerének használatát szabályozza.

A szabályzat felülvizsgálatának rendje, hatálya:

1. § Jelen szabályzat felülvizsgálatát a működés rendjében bekövetkezett változást követő 15 napon belül az ügyvezető végzi el.

Az IBSZ hatálya:

2. § Az IBSZ rendelkezéseinek hatálya a társaság informatikai eszközeire, az azokon tárolt adatokra, futtatott alkalmazásokra, a társaság munkavállalóira és a társasággal megbízásos jogviszonyban álló személyekre terjed ki.

Eszközökkel kapcsolatos szabályok:

3.§ A társaság a munkavégzéshez megfelelő számítástechnikai hátteret biztosít, a biztosított eszközöket azonban munkaidőben kizárólag munkavégzés céljára lehet használni.

4. § Ha a felhasználó bármilyen biztonsági problémát vagy hibát észlel, azonnal köteles értesíteni az irodavezetőt.

5. § Tilos az eszközöket és azok részeit áthelyezni, burkolatukat megbontani. (Az áthelyezés tilalma értelemszerűen nem vonatkozik a mobil eszközökre - pl. laptop, tablet, "okostelefon.)

6. § Tilos az eszközök közvetlen közelében enni, inni, dohányozni.

Jelszókezeléssel kapcsolatos szabályok:

7. § (1) A felhasználók a társaság által biztosított eszközön használt jelszavukat 3 havonta kötelesek cserélni.
   (2) A jelszónak minden felhasználó által bármikor megváltoztathatónak kell lennie. A kezdetben generált jelszót az első bejelentkezés alkalmával meg kell változtatni.
   (3) A jelszó minimum 8 karakter hosszú legyen, és tartalmazzon (kicsi és nagy) betűket és számjegyeket is. További feltétel, hogy nem tartalmazhatja a felhasználó nevét még részleteiben sem.

8. § (1) A jelszó nem írható fel semmilyen jól látható vagy könnyen hozzáférhető helyre. A jelszavakat nem szabad felírni, papíron tárolni, amennyiben az elkerülhetetlen (pl. kezdetben generált jelszó esetén) gondoskodni kell a jelszó biztonságos helyen, zárt borítékban történő tárolásáról.
   (2) A jelszó és a hozzátartozó azonosító soha nem kerülhet egy postai küldeménybe, még elektronikus levelezés során sem.

9. § Ha a felhasználó azt gyanítja, hogy jelszavát valaki megismerte, azonnal le kell azt cserélnie.

Szoftverekkel kapcsolatos szabályok:

10. § A társaság kizárólag jogtiszta szoftverekkel dolgozik.

11. § Tilos bármilyen terjesztési engedéllyel (freeware, shareware, stb.) rendelkező szoftvert a társaság tulajdonát képező informatikai eszközökre feltelepíteni.

Adatvédelmi szabályok:

12. § A felhasználók a társaság által biztosított informatikai eszközökről vagy a társaság szervereiről külső adathordozóra (pendrive, CD/DVD stb.) adatokat, fájlokat csak az ügyvezető engedélyével menthetnek le.

13. § A munkahely elhagyása esetén a számítógépet zárolni kell a "Windows" + "L" billentyűk egyidejű lenyomásával, és olyan képernyővédőt kell beállítani, mely csak jelszóval engedi a gép feloldását.
14. § A számítógépen tilos mappamegosztást definiálni, működtetni. Kivétel ez alól a minden számítógépen létrehozott osztott (Shared) mappa. Utóbbi használata kizárólag arra az esetre vonatkozik, amikor a számítástechnikai eszközök között – a társaság működését szolgáló céllal - adatállomány-mozgatás történik. Ezen mappákban tilos az állományokat tartósan – egy munkanapon túl - tárolni!

Internethasználattal kapcsolatos szabályok:

15. § (1) Tilos a munkahelyen bármely, harmadik személynek távoli elérést engedő program használata.
    (2) Tilos a munkahelyi internet kapcsolaton keresztül olyan program és egyéb fájl letöltése, ami nem a munkavégzéshez szükséges.
    (3) Fájlok külső szerverekre való feltöltése minden esetben tiltott. Kivételt képez ez alól a társaság által bérelt ftp szerverekre való feltöltés és az ügyvezető által engedélyezett, kijelölt "felhőalapú" mappákba feltöltés.
    (4) Tilos minden internetes "online" sugárzott műsor (ide tartoznak a rádió, televízió műsorok) hallgatása, megtekintése.
    (5) Nem üzleti célú levelezés nem engedélyezett munkaidőn belül a munkahelyi számítógépeken.
    (6) Mindenféle fájlmegosztó alkalmazás használata a társaság számítástechnikai eszközein tiltott.

Vírusvédelmi szabályok:

16. § (1) A számítógépeken vírusellenőrző program fut, mely a gép működése közben automatikusan figyeli a rendszert. A vírusellenőrző programot leállítani és annak működésébe beavatkozni szigorúan tilos.
    (2) Minden fájlművelet előtt ez a program ellenőrzi a megnyitott fájlokat. Bármilyen, adatbiztonságot veszélyeztető eseményre figyelmeztetés jelenik meg a felhasználó monitorán, azonnal értesítenie kell az irodavezetőt, hogy a megfelelő lépésekkel megakadályozhassák a kártékony programok további fertőzéseit.
    (3) Vírusfertőzés gyanúja esetén a munkát azonnali hatállyal fel kell függeszteni, a számítógépet az adathálózatról le kell választani és meg kell kezdeni az okok feltárását és a helyreállítást.

Berendezések karbantartása, selejtezése:

17. § A berendezéseket előírásszerűen karban kell tartani folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében.
18. § Selejtezésekor valamennyi olyan berendezést, amely tárolóeszközt foglal magában, ellenőrizni kell, hogy az adatokat és szoftvereket helyreállíthatatlanul eltávolították-e róluk.

Információbiztonsági incidensek kezelése

19. § INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK ÉS GYENGESÉGEK JELENTÉSE
    A munkáltató minden alkalmazottjának és partnerének kötelessége az általa tapasztalt biztonsági eseményt vagy általa feltárt biztonsági sebezhetőséget haladéktalanul jelenteni az ügyvezetőnek.

20. § ESEMÉNYEK, GYENGESÉGEK KIÉRTÉKELÉSE, INCIDENSEK KEZELÉSE
    Információbiztonsági incidensnek minősül az informatikai eszközök elvesztése, eltulajdonítása vagy jogosulatlan hozzáférése is. A biztonsági események

kiértékelése, incidensek kezelése elsődlegesen az ügyvezető feladata. Az ügyvezető kötelessége a bejelentés dokumentálása, valamint a kiértékelés elvégzése. Az ismertté vált gyengeség, sebezhetőség kezelését a lehető legrövidebb időn belül, de legkésőbb a bejelentést, ismertté válást követő 2 munkanapon belül meg kell kezdeni. Az incidensek kezelését a bejelentést, ismertté válást követően haladéktalanul meg kell kezdeni.

21. § INCIDENSEK KIÉRTÉKELÉSE

A biztonsági esemény kiértékelése az ügyvezető feladata, melynek során meg kell határoznia, hogy a biztonsági esemény:

- az informatikai rendszer kiesésével, vagy meghibásodásával;
- a szolgáltatás megtagadásával;
- az adatok megsérülésével, pontatlanságával;
- biztonságsértéssel kapcsolatos;
- meg kell határoznia a biztonsági esemény okát;
- meg kell határoznia a javító intézkedést az előzetesen gyűjtött adatok felhasználásával;
- meg kell határoznia a biztonsági esemény elhárításának végső határidejét.

22. § INCIDENSEK ÖSSZEGZÉSE

Az ügyvezető köteles évente:

- a beérkező biztonsági eseményekről statisztikát készíteni,
- a biztonsági eseményekből közvetlenül származtatott kárt megbecsülni,
- a jellemző információbiztonsági sérüléseket azonosítani, dokumentálni

Jelen szabályzat 2021. április 1. napjától visszavonásig alkalmazandó.

Csanády László
ügyvezető