

ADATVÉDELMI- ÉS INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

1. Összefoglaló

Az Adatvédelmi- és Információbiztonsági szabályzat a V-NAGY AUTÓCENTRUM KFT. minden dolgozójára vonatkozó információbiztonsággal kapcsolatos követelményeket és felelősségeket határoz meg, segítséget ad számukra a munkaköri leírásban rögzített feladataiknak az információbiztonsági szabályok szerinti végrehajtásában.

Az Adatvédelmi- és Információbiztonsági szabályzatot minden munkatárs rendelkezésére kell bocsájtani. A szabályzat ismerete és az abban foglaltak betartása a V-NAGY AUTÓCENTRUM KFT. valamennyi alkalmazottjának és a V-NAGY AUTÓCENTRUM KFT. informatikai rendszerével kapcsolatba kerülő, szerződéses viszonyban levő partnere számára kötelező.

2. Az Információbiztonsági szabályzat hatálya

Személyi hatály

Jelen Kézikönyv személyi hatálya kiterjed:

- o a V-NAGY AUTÓCENTRUM KFT.-nél foglalkoztatott munkavállalókra, az adatfeldolgozásban részt vevő külső cégekre, szerződéses jogviszonyban álló, jogi és természetes személyekre, jogi személyiséggel nem rendelkező szervezetekre,
- o a V-NAGY AUTÓCENTRUM KFT.-vel szerződéses kapcsolat keretében adatcserét (küldés és/vagy fogadás, tárolás/továbbítás) folytató szervezetekkel történő kommunikációra, függetlenül a szervezet betöltött szerepétől, szervezeti helyétől, elhelyezésétől és a V-NAGY AUTÓCENTRUM KFT.-hez fűződő kapcsolatától.

Tárgyi hatály

A Szabályzat tárgyi hatálya kiterjed:

- o A V-NAGY AUTÓCENTRUM KFT. minden adatkezeléssel és feldolgozással kapcsolatos folyamatában résztvevő informatikai eszközre, illetve azok elhelyezésére szolgáló létesítményekre,
- o az informatikai eszközök működtetésére szolgáló alap- és rendszerprogramokra, valamint alkalmazási programokra és azok dokumentációira (továbbiakban: program) a tulajdonviszonytól függetlenül,
- o programrendszerek, berendezések beszerzési, fejlesztési, tervezési, kivitelezési munkálataira,
- o a fentiek alapját képező szerződésekre, nyilvántartásokra, dokumentációkra, valamint,
- o a feldolgozás alatt lévő, ott tárolt, illetve a feldolgozás eredményeképpen létrejött adatokra és adathordozókra, függetlenül azok keletkezési helyétől,
- o a V-NAGY AUTÓCENTRUM KFT. tulajdonában vagy használatában lévő informatikai eszközökre és az informatikai eszközök által kezelt, tárolt, továbbított adatokra.

3. Titoktartási megállapodások

Minden alkalmazottnak és a V-NAGY AUTÓCENTRUM KFT.-vel kapcsolatba kerülő külső szervezetnek, személynek (cégnek, egyéni munkavállalónak, stb.) titoktartási nyilatkozatot kell aláírnia, melyben nyilatkoznak arról, hogy a munkájuk során a tudomásukra jutott, nem publikus adatokat sem a munkavégzésük, sem annak vége után nem hozzák harmadik fél tudomására.

4. Vagyontárgyak tulajdonlása

Valamennyi információ és az információfeldolgozással összefüggő vagyontárgy a V-NAGY AUTÓCENTRUM KFT. tulajdona a felhasználók csak használatra kapják meg azokat.

A vagyontárgy használója felelős a következőkért:

- a) Gondoskodik az információ-feldolgozó eszközökkel kezelt adatok besorolásának megfelelő felhasználásáról,
- b) Gondoskodik az eszköz állagának megóvásáról, és rendeltetésszerű használatáról,
- c) Az eszközzel kapcsolatos hibás működést azonnal jelzi szakmai felettesének.

5. Emberi erőforrások

Fegyelmi eljárás

A szabályzat, illetve a biztonsági szabályok be nem tartása jogi következményeket vonhat maga után. A szabályzat ismeretének hiánya nem mentesít a felelősségre vonás alól.

Munkaviszony megszüntetése vagy módosítása

Az alkalmazási jogviszony megszüntetésekor, illetve a munkavállaló feladatkörét érintő megváltoztatásakor a szakmai vezető felelős azért, hogy a munkavállaló jogosultságai visszavonásra, illetve módosításra kerüljenek.

Minden munkavállaló, szerződéses partner, vagy külső fél köteles visszaszolgáltatni V-NAGY AUTÓCENTRUM KFT. számára az összes birtokában lévő vagyontárgyat amennyiben az alkalmazás, szerződés vagy megegyezés megszüntetésre kerül.

6. Hordozható számítógépek fizikai védelme

A munkaállomásokra vonatkozó előírásokon kívül az alábbi fizikai védelmi szabályokat kell betartani:

- A mobilitás és a kis méret miatt a hordozható számítógépek fokozottan ki vannak téve a lopásveszélynek. Gondoljunk erre, és ezeket ne hagyjuk - még rövid időre sem - őrizetlenül autóban (még őrzött parkolóban sem), szállodai szobában, stb. (zárjuk el fizikailag, használjuk az értékmegőrzőt).
- A hordozható számítógép ellopása esetén a lopás tényét a lehető leggyorsabban jelenteni kell a felettes munkahelyi vezetőnek, továbbá:
 - értesíteni kell a rendőrséget,
 - értesíteni kell a szálloda vezetését, ha a számítógépet a szállodai szobából, vagy a szálloda ingatlanján álló kocsiból lopták el,
 - valamennyi rendőrségi és biztosítói jegyzőkönyvet, jelentést meg kell őrizni, és a V-NAGY AUTÓCENTRUM KFT. részére át kell adni.

Adattároló, adatfeldolgozó eszköz elvesztése

Bármely adattároló, adatfeldolgozó eszköz elvesztését a lehető leggyorsabban jelenteni kell a munkahelyi vezetőnek, és tájékoztatni kell őket arról, hogy a berendezés tartalmaz-e bárminemű bizalmas adatot. /Előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban (e-mailben) is megerősítve./

7. Logikai védelmi intézkedések

Hozzáférések védelme és ellenőrzése

A V-NAGY AUTÓCENTRUM KFT. vezetése jogosult a tulajdonában lévő számítógépek és a hálózat használatát, a rajtuk végzett tevékenységeket (pl. céges levelezést, Internet használatot) ellenőrizni.

Felhasználó felelősségi köre

A V-NAGY AUTÓCENTRUM KFT. felhasználói a munkaállomásokon azokat a jogtisztá szoftvereket használhatják, amelyek szükségesek a munkájukhoz, és a számítógépen az erre feljogosított személyek telepítették.

A felhasználó semmilyen IT eszközt nem telepíthet a V-NAGY AUTÓCENTRUM KFT. informatikai hálózatába, azok elhelyezését, telepítési módját nem változtathatja meg. A felhasználó szoftvert csak külön engedéllyel és megfelelő jogosultság birtokában telepíthet, illetve módosíthatja a rendszerszintű beállításokat. Azok a felhasználók, akik adminisztrátori jogot gyakorolnak a gépükön, ők maguk felelnek a gépükre telepített programokért biztonsági és jogtisztasági szempontból egyaránt.

E rendelkezés megszegéséért a felhasználó ellen fegyelmi felelősségre vonás kezdeményezhető.

Az alkalmazottak a saját tulajdonukat képező számítógépeket, szoftvereket és egyéb informatikai eszközeiket csak eseti engedéllyel, bevizsgálás után használhatják a V-NAGY AUTÓCENTRUM KFT. üzleti céljaira.

A V-NAGY AUTÓCENTRUM KFT. tulajdonában lévő adatfeldolgozó eszközeinek hardver-, és szoftver integritásának megőrzése érdekében a felhasználónak tilos a számítógépet fizikailag megbontani, alkatrészeket cserélni, be- és kiszerezni.

A munkaállomás használatát nem szabad senkinek átengedni úgy, hogy a felhasználó saját felhasználói fiókjából nem jelentkezett ki előtte.

A fájlok, állományok elnevezéskor (mentésekor) egyedi, ékezeteket nem tartalmazó, a fájl tartalmára lehetőleg egyértelműen utaló nevet kell adni. A több lépcsőben készített anyagok esetében minden verziót külön verziószámmal kell ellátni.

Munkaállomásokon a fájl / könyvtár megosztás csak külön engedéllyel megengedett.

Hálózati védelem

A V-NAGY AUTÓCENTRUM KFT. hálózatban lévő számítógép egyedi külső hálózati kapcsolattal (pl.: mobil internet, modem, ADSL) csak indokolt esetben, az adott szakterületi vezető engedélyével rendelkezhet. Az ilyen számítógépeken a V-NAGY AUTÓCENTRUM KFT. számítógép-hálózatához való kapcsolódáskor nem engedélyezett a külső kapcsolat és a belső hálózat egyidejű használata.

Jelszókezelési szabályzat

A jelszavak használata az informatikai biztonság egyik meghatározó része. Az informatikai rendszer minden felhasználójának tisztában kell lennie a jelszavak fontosságával és a nem megfelelő jelszókezelés következményeivel, mert például egy rosszul megválasztott, könnyen kitalálható jelszó

nemcsak a jelszó tulajdonosára, hanem a V-NAGY AUTÓCENTRUM KFT. informatikai, telekommunikációs rendszerére is negatív következményekkel járhat.

A kezdeti jelszavak (pl. azok, melyek a felhasználói fiók létrehozásakor vagy jelszó reset esetén állítódnak be) csak az első bejelentkezésig maradhatnak érvényben, a rendszernek ki kell kényszerítenie a jelszó megváltoztatását, amennyiben a rendszer erre nem alkalmas a felhasználó feladata a jelszócsere elvégzése az első belépést követően. A kezdeti és új jelszavakat is a jelszószabályoknak megfelelően kell kialakítani és ezeknek egyedinek kell lennie.

Felhasználói jelszavak kezelése

A felhasználói jelszavak kezelése során az alábbiak betartása szükséges:

- a. A felhasználónak kötelessége a jelszó megváltoztatása a felhasználói fiók létrehozása utáni első belépéskor.
- b. A jelszavakat titokban kell tartani, ennek érdekében:
 - A jelszót tilos másoknak elmondani, a jelszóról mások előtt beszélni.
 - A jelszót se a feletteseknek, se a rendszergazdáknak, adminisztrátoroknak nem szabad elárulni, ha kifejezetten kéri ezt, akkor sem.
 - Tilos közös jelszavakat használni (még családtagokkal, barátokkal sem szabad).
 - A jelszót nem szabad leírni és elérhető helyen tárolni (irodában, táskában...).
 - Ne utaljunk a jelszó tartalmára (pl. „a kedvenc együttesem neve”).
 - Ne használjuk a programok jelszó megjegyző funkcióját.
 - A jelszavunkat ne írjuk be kérdőívekbe, űrlapokba.
 - Ha a belépési nevet és jelszót el kell küldeni, a felhasználó név/jelszó párost egy üzenetben (e-mailben, levélben vagy SMS-ben) nem szabad küldeni. Külön csatornán kell küldeni a nevet és a jelszót (pl. e-mail-ben és SMS-ben), hogy bármelyik lehallgatása, vagy illetéktelen kezekbe kerülése esetén se lehessen visszaélni a megszerzett adattal. A jelszót tartalmazó üzenetből ne lehessen kideríteni, hogy a kapott jelszót milyen felhasználónévvel, milyen rendszerhez lehet használni.
- c. Olyan jelszavakat kell használni, melyek nehezen visszafejthetőek, de könnyen megjegyezhetőek, nem személyes adatokon alapulnak (pl. nem tartalmaz telefonszámot, gyermek nevét, születési dátumot, kedvenc háziállat nevét, cégnevet, rendszámot, stb.) és nem szótári szó.
- d. Minél komplexebb a jelszó, annál kisebb a valószínűsége, hogy a nevünkben visszaélést követnek el, ezért a jelszóképzésnél az alábbi szempontokat kell betartani:
 - A jelszó nem tartalmazhatja az egész vagy egy felismerhető részét a felhasználónévnek; A jelszavaknak minimálisan 8 karakter hosszúnak kell lenniük és tartalmazniuk kell minimum 3 karaktertípust az alábbiakból: nagybetűk, kisbetűk, számok, speciális karakterek;
 - A jelszó az utolsó változtatás után maximum 90 napig maradhat érvényes;
 - Jelszóváltoztatáskor a felhasználó nem használhatja az utolsó 12 jelszavát;
 - Új jelszót csak két nap elteltével lehet megváltoztatni;
 - 5 hibásan megadott jelszó esetén a rendszer letiltja a fiókot.
- e. A felhasználó a jelszavát a legrövidebb időn belül köteles megváltoztatni, amennyiben felmerül a gyanú, hogy a jelszava más tudomására jutott. A jelszó kitudódását vagy annak gyanúját security incidensnek kell tekinteni és jelenteni szükséges.

- f. A felhasználónak tilos más felhasználó jelszavát megkérdeznie és tilos más felhasználó azonosítóját használnia annak belépése után. Hasonlóképpen, a felhasználó nem engedheti meg más felhasználónak az azonosítója használatát és nem engedheti át annak használatát a bejelentkezés után.
- g. A V-NAGY AUTÓCENTRUM KFT. rendszereinek elérésére használt jelszavakat tilos külső rendszerek eléréséhez is használni (pl. gmail-hez, freemail-hez).
- h. Kezdeti jelszavak vagy a jelszó elfelejtése esetén, az ideiglenes jelszó kiadása előtt a felhasználót egyértelműen azonosítani kell.
- i. A felhasználók csak akkor tudják megváltoztatni a jelszavukat, miután a rendszer hitelesíti őket például a jelenlegi jelszót beírva.
- j. Kezdeti vagy ideiglenes jelszavakat a felhasználónak biztonságos csatornán kell eljuttatni.
- k. Kezdeti vagy ideiglenes jelszónak egyedinek kell lennie.
- l. A felhasználónak tilos a jelszavak megfejtésére alkalmas alkalmazást futtatnia.

A jelszószabályok betartása minden felhasználónak jól felfogott érdeke.

A felhasználó felelőssége, ha neki felróható mulasztása miatt a jelszava megismerése révén valaki visszaélést követ el.

Adathordozók megsemmisítése

Adathordozók megsemmisítésére vonatkozó igényt a szakmai felettesnek szükséges jelezni, aki intézkedik a helyes megsemmisítési eljárás lefolytatása kapcsán.

8. Biztonsági mentések, archiválás

Az adatokat nem a lokális gépen, hanem a szerverek megfelelő könyvtáraiban kell tárolni, ahol biztosítható azok rendszeres adatmentése és biztonságos tárolása. A megfelelő könyvtárba való mentés a felhasználó felelőssége.

9. Információbiztonsági hiányosságok és incidensek kezelése

Minden dolgozónak, szerződéses partnernek vagy külső félnek kötelessége a tudomására jutott információbiztonsági hiányosságokról, sérülékenységről, valamint az információbiztonsági szabályok megszegésről azonnal jelentést tenni az információbiztonsági incidensek megakadályozás céljából.

A dolgozók, szerződéses partnernek vagy külső felek a felfedezett biztonsági hiányosságokat semmilyen körülmények között sem jogosultak kihasználni vagy megpróbálni kihasználni azokat, illetve nem jogosultak a felfedezett incidenssel kapcsolatosan intézkedni!

Az információbiztonságot érintő eseményekről, a felfedezésük után, haladéktalanul tájékoztatni kell a felfedező közvetlen munkahelyi vezetőjét.

Az információbiztonságot veszélyeztető események kivizsgálására irányuló vizsgálatokban a dolgozók kötelesek együttműködni a kivizsgálókkal.

Az információbiztonsági hiányosságok megelőzése céljából a munkatársak kötelesek rámutatni az információbiztonsági szint romlására, illetve annak lehetőségére.

Szoftverműködési zavarok

A felhasználó a tárolt adataiban bekövetkező bármely megmagyarázhatatlan változást, az informatikai rendszer szokatlan működését azonnal köteles jelenteni a közvetlen felettesének.

Hiba esetén a felhasználónak rögzíteni kell:

- a hibajelenséget és
- a képernyőn megjelenő hibaüzenetet.

Szükség esetén a munkavégzést azonnal fel kell függeszteni és a számítógépet le kell választani a hálózatról. Amíg nem derítették ki a hiba okát, a számítógépben lévő adathordozókat nem szabad másik számítógépre áttenni.