Dél-Kom
Nonprofit Kft.

DK-27-11-4-4/B-1/2025 Ikt. szám

SZ-16/1

INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT – Felhasználói kivonat

Tartalomjegyzék

1. A szabályzat általános rendelkezései *3*
1.1. Célja 3
1.2. Az informatikai biztonsági szabályozó környezet kialakítása 3
1.4. Az IBSZ hatálya 4
1.5. Az IBSZ felhasználói kivonatának elérhetősége, hozzáférés szabályozása 4
2. Az Informatika biztonság szervezete *4*
2.1 Szerepkörök, tevékenységek, felelősségek 5
2.1.8. Felhasználók 5
4. Jogosultság kezelés *6*
4.1 Szerepkörök meghatározása 6
4.2 Jogosultságok biztosítása és visszavonása 6
4.4 Adatkezelési, adatvédelmi besorolás 7
6. Rendszerek és szolgáltatások akvizíciója, igénybevétele, beszerzése *8*
6.1 Külső rendszerek szolgáltatásainak igénybevétele 8
7. Biztonságtervezési alapelvek *8*
7.1 Folyamatos felügyelet és monitorozás 8
8. Hozzáférések kezelése *9*
8.1 Sikertelen bejelentkezések kezelése 9
8.2 Tájékoztatás a rendszerek használata előtt 9
8.3 Azonosítás, hitelesítés nélkül igénybe vehető informatikai szolgáltatások, rendszerek 9
8.4 Távoli hozzáférés biztosítása 9
8.5 Vezeték nélküli hozzáférés 9
8.5.1 Belső hálózat 9
8.5.2 Vendég hálózat 10
9. Oktatás, képzés *10*
9.1 Oktatások rendje, hatóköre 10
11.Konfiguráció kezelés *10*
11.5 Szoftverhasználat szabályozása 10
13. Azonosítás és hitelesítés *11*
13.1 Névkonvenció 11
13.2 Hitelesítésre szolgáló eszközök kezelése 12
13.3 Azonosítók újbóli felhasználása, változtatása 12
15. Karbantartás, frissítés *12*
16. Adathordozók védelme *12*
18. Tervezés, biztonsági követelmények meghatározása *13*
18.1 Viselkedési szabályok és normák külső webhelyek és közösségi média használata során 13
22. Mellékletek *13*

1. A szabályzat általános rendelkezései

1.1. Célja

Az Informatikai Biztonsági Szabályzat (továbbiakban IBSZ) szabályozza és meghatározza a Dél-Kom Nonprofit Kft. (továbbiakban Társaság) valamennyi:

- informatikai eszközére,
- az igénybe vett és nyújtott informatikai szolgáltatásokra,
- az informatikai eszközöket igénybe vevő és használó külső és belső felhasználókra,
- az informatikai rendszerekben és eszközökben kezelt adatokra,
- az eszközök, rendszerek, szolgáltatások tervezésére, beszerzésére, előfizetésére,
- az eszközök, szolgáltatások nyilvántartására,
- Az eszközök, rendszerek, szolgáltatások üzemeltetésére,
- az eszközök, szolgáltatások, folyamatok fizikai és logikai védelmére,
- a kockázatok kezelésére,
- az incidensek, nem várt események megelőzésére,
- a hozzáférések szabályozására,
- a rendszerek és szolgáltatások elemein végzett tevékenységek naplózására, ellenőrzésére,
- a mentések archiválások rendjére, az adatok rendelkezésre állásának biztosítására,
- az üzletmenet folytonosságra,
- fentiekhez tartozó általános és egyedi beállításokra,

vonatkozó - a biztonsággal összefüggő - előírást és követelményt.

1.2. Az informatikai biztonsági szabályozó környezet kialakítása

- az „Irányelv az egész Unióban egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2 irányelv)-ben meghatározott”,

- a 2023. évi 23-ik törvényben (Kibertan törvény) és
- a 7/2024. (VI.24.) MK rendeletben előírtak alapján, valamint a

- NIST SP 800-53 Rev5 és
- ISO 27001:2022 kontrol gyűjtemények figyelembevételével készült.

A Társaság a 7/2024. (VI.24.) MK rendelet 2.2 pontja szerint előírt értékelés alapján „alap” és „jelentős” biztonsági osztályba sorolja EIR rendszerit. A kialakított védelmi megoldások az egyenszilárdság biztosítása érdekében egységesen „jelentős” biztonsági osztály előírásainak teljesítésére törekszik.
A biztonsági szintbe sorolást minden, az informatikai rendszereket, vagy a kezelt adatokat érintő lényeges változást követően ismételten el kell végezni!

1.4. Az IBSZ hatálya

Jelen IBSZ személyi hatálya kiterjed a Társaság valamennyi dolgozójára, belső és külső felhasználóira, a Társasággal informatikai vonatkozásban kapcsolatba kerülő szervezetekre és személyekre, akik kötelesek az IBSZ-ben leírtakat betartani.

Az IBSZ tárgyi hatálya kiterjed minden olyan informatikai eszközre és szolgáltatásra, amely fizikailag a Társaság telephely(ei)én az informatikai hálózatba csatlakozik, vagy csatlakozhat, illetve azzal adatküldés és/vagy információt cserél, számára szolgáltatást biztosít, vagy szolgáltatást vesz tőle igénybe, információ és adatkezelést vagy adatfeldolgozást valósít meg.

A személyi és tárgyi hatálytól történő eltéréseket tételesen meg kell határozni, azokat egyedileg kell vizsgálni és engedélyezni.

A biztonsági megoldások esetében az előírtnál szigorúbb beállításokat külön engedély nélkül i s lehet alkalmazni.

1.5. Az IBSZ felhasználói kivonatának elérhetősége, hozzáférés szabályozása

Az IBSZ felhasználói kivonatának adatvédelmi besorolása: **„Bizalmas információ”**.
Az IBSZ megismerése a hatókörben meghatározottak számára differenciáltan biztosított a betartáshoz, végrehajtáshoz szükséges mértékben. A Társaság a könnyebb kezelhetőség és a védett információk bizalmasságának megőrzése érdekében kivonatokat készít az IBSZ-ből, melynek elérhetősége:

IBSZ Felhasználói kivonata: Delkom:/Informatika/IBSZ/Felhasználói kivonat/ adatvédelmi besorolása: „Bizalmas információ”.

Az IBSZ felhasználói kivonatának és vonatkozó mellékleteinek megismerése és betartása a felhasználók munkába állásának feltétele.

2. Az Informatika biztonság szervezete

A Társaság a tulajdonosi szerkezetéből, az igénybe vett informatikai szolgáltatások köréből, Társaság méretéből, valamint az üzemeltetett rendszerek számából levezetve külön informatikai biztonsági szervezetet nem hoz létre. Az ezzel összefüggő feladatokat az Informatikai csoporthoz rendeli, koordinálására Informatikai Biztonsági Felelőst nevez ki.
Az Informatikai Biztonsági Felelős (IBF)

- neve: Tardik Tamás Gábor
- elérhetőségei: E-mail: tardik.tamas@delkom.hu Tel.: +3620/952-9355
- távollétében helyettesítését ellátja: Juhász Zoltán
- elérhetőségei: E-mail: juhasz.zoltan@delkom.hu Tel.: +3630/410-9785

2.1 Szerepkörök, tevékenységek, felelősségek

Az informatikai biztonsággal kapcsolatos feladatok szerepkörökhöz rendeltek. A szerepkörök szerinti felelősök kijelölése elsősorban a munkaköri leírásokban történik. Az informatikai infrastruktúra biztonságos működtetésében, illetve az informatikai rendszerekben kezelt adatok védelmének tárgykörében az alábbi szerepkörök kerülnek meghatározásra:

2.1.8. Felhasználók

A Társaság felhasználói, korlátozás nélkül a belső és külső felhasználókra.

- Ismerniük kell az IBSZ-ben szereplő előírásokat, illetve azokat maradéktalanul be kell tartaniuk, továbbá ezek betartásában az informatikai rendszer használatát irányító személyekkel együtt kell működniük.
- Ismerniük kell a felhasználói leírásokat, utasításokat, illetve azokat maradéktalanul be kell tartaniuk.
- Rendelkezniük kell az általuk üzemeltetett berendezésekre és szoftverekre vonatkozó előírásokkal, illetve ismerniük kell azok tartalmát.
- Tevékenységük megkezdésekor ellenőrizniük kell, hogy az általuk használt eszközök üzemképesek-e és azok beállítása az előírásoknak megfelelő-e.
- Kötelesek figyelemmel kísérni az általuk használt berendezések és szoftverek állapotát és az esetleges meghibásodást vagy helytelen működést azonnal jelezni kell a közvetlen vezetőnek.
- Munkájuk során figyelniük kell arra, hogy illetéktelen személyek lehetőleg ne tartózkodjanak az adat/információ feldolgozása során a helyiségben.
- Tevékenységük befejezésekor a használt programokból szabályszerűen ki kell lépni.
- Hálózati információ igénybevételét követően a hálózatból szabályosan ki kell lépni.
- Az általuk üzemeltetett berendezést szükség esetén az előírásoknak megfelelően le kell állítani, illetve áramellátását meg kell szüntetni.
- A munkahelyen a helyiségből utolsóként való távozáskor meg kell győződni a helyiség biztonságos lezárásáról.
- Felelősek a részükre munkavégzésre biztosított, de a Társaság tulajdonát képező informatikai eszközök (például notebook, okostelefon) rendeltetésszerű és az engedélyeknek megfelelő használatáért.
- Felelősek az általuk elkövetett informatikai vonatkozású szabálytalanságokért, valamint a keletkező károkért és hátrányokért.
- Kötelesek a Társaságnál szervezett informatikai biztonsági oktatásokon részt venni, az ismeretanyagok elsajátításáról számot adni.
- Amennyiben a munkát bármilyen okból is megszakítják, vagy befejezik, kötelesek a számítógépet kikapcsolni vagy zárolni, a papír alapú dokumentációkat, iratokat és mobil adathordozókat elzárni.
- Az általuk használt Informatikai eszközök, adathordozók elvesztését, ellopását, megrongálódását haladéktalanul jelenteni kell az informatikai csoportnak.
- A munkahelyükön rendet kell tartaniuk a munkavégzéssel kapcsolatos iratokat, dokumentumokat, adathordozókat nem hagyhatják felügyelet nélkül.

- Az IBSZ és rendelkezései ismeretének hiánya nem mentesíti a felhasználót annak megsértése esetén foganatosítható szankcióktól, illetve az esetleges anyagi kártérítési felelősség és büntetőjogi következmények alól.

4. Jogosultság kezelés

A Társaság szerepkör alapú jogosultság kezelést valósít meg. A felhasználói jogosultságok mindig az adott szerep- és feladatkör szerint kerülnek meghatározásra. A kezelt adatokra, információkra a Társaság adatvédelmi besorolást hoz létre.

4.1 Szerepkörök meghatározása

Valamennyi, az informatikai rendszerekben előforduló hozzáférést, jogosultságot meg kell határozni és dokumentálni kell.

A jogosultságok biztosítása során csak felhasználó → szerepkör (csoportjog) összerendelés a megengedett.

Minden felhasználó egyedi azonosítóval kell, hogy rendelkezzen, kivéve a technikai és adminisztrátori jogosultságokat (pl.: DB admin, DB user, local admin, kamerarendszer admin, ip telefon admin, nyomtató admin, router admin, telefonközpont, kiszolgálószerver admin, hálózati kiszolgáló eszköz admin stb.)

Az elsődleges authentikáció és authorizáció elsődlegesen Windows Active Directory alapú SingleSignOn megoldás.
A hozzáférések kizárólag szerepkör-csoporttagság, munkakör-csoporttagság és felhasználó-csoporttagság alapján valósíthatók meg.

A Társaság a szerepkörök és csoporttagságok között az összeférhetetlenségi mátrixban meghatározottak szerint állapít meg összeférhetetlensége(ke)t.

A jogosultságokat legalább évente felül kell vizsgálni, ennek meghatározott módja: az adott terület, szolgáltatás adatgazdája, és/vagy a munkahelyi vezető számára meg kell küldeni a hozzá tartozó felhasználók jogosultságait, szerepköreit, melyről **14 napon belül visszajelzést köteles** küldeni (jóváhagyás, elutasítás, bővítés) az Informatikai csoportrészére.

4.2 Jogosultságok biztosítása és visszavonása

Jogosultság biztosítása minden esetben **az igénylő, jóváhagyó, végrehajtó funkciók** szétválasztásával valósítandó meg. Eltérés csak a technikai, adminisztrátori jogosultságok létrehozásánál megengedett, amennyiben azt a telepítési dokumentáció tartalmazza.

- Igénylő: az a személy vagy szervezet, aki a hozzáférést igényli.
- Jóváhagyó: az a személy vagy szervezet, aki az adatgazdai jogokat gyakorolja.
- Végrehajtó: az a személy vagy szervezet, aki informatikai rendszeren a szükséges jogosultságokat létrehozza, a beállításokat elvégzi.

- Ellenőrző: az a személy vagy szervezet, aki a beállítások megfelelőségét ellenőrzi. A társaság véletlen időpillanatokban szúrópróba-szerű és évenként teljeskörű ellenőrzéseket ír elő.

A jogosultságok, szerepkörök biztosítása során törekedni kell arra, hogy mindenki csak a feladathoz **szükséges és elégséges minimális jogosultságok**kal és információkkal rendelkezzen!

A szerepkörök létrehozása során az egyes szerepkörök metszeteit minimalizálni kell, szükség esetén az adott felhasználóhoz több szerepkört (csoportjogot) kell hozzárendelni.

A jogosultság igénylésének folyamatát belépő és kilépő dolgozók esetén, illetve munkakör, feladatkör változása esetén a ***2. számú melléklet*** tartalmazza. (Kilépéskor, munkaviszony megszűnésekor rendelkezik az adatok, jogosultságok és feladatok helyettesítő személyhez rendeléséről, az érintett szervezeti egység és külső partnerek tájékoztatásáról, gondoskodik az esetleges jogsértő magatartás megelőzéséről, nyilatkoztatja kilépő felhasználót, hogy személyes adatokat nem tartalmaznak a hozzáférésével elérhető felhasználói fiókok, azok munkahely vezetőjének, vagy a helyettesítő személynek átadhatók.)

A Társaság fenntartja a jogot, hogy a távozó felhasználó által létrehozott vagy kezelt információkat, adatállományokat, file-okat, üzeneteket megtartsa, azokhoz további felhasználás céljából hozzáférést biztosítson más felhasználók számára, vagy a meglévő hozzáféréseket korlátozza.

A Bér-és Munkaügyi csoport (HR) feladata kilépéskor nyilatkoztatni a távozó dolgozót az általa kezelt és tudomására jutott bizalmas és titkos információkkal kapcsolatos titoktartási kötelezettségről (titoktartási nyilatkozat).

A Társaság a munkakör vagy feladatkör változásából adódó jogosultságok változását a korábbi jogosultságok és szerepkörök teljes visszavonásával – kivéve a felhasználó egyedi azonosítóját és postafiókját - és az új feladatokhoz illeszkedő jogosultságok hozzárendelésével valósítja meg. Munkakör, vagy feladatkör bővülésekor, csökkenésekor nem kell alkalmazni a teljes körű visszavonásokat.

A Társaság informatikai munkatársai a megszűnő jogosultságokat az előírt idő intervallumban vonják vissza.

4.4 Adatkezelési, adatvédelmi besorolás

A Társaság a kezelt adatok, információk tekintetében három adatkezelési, adatvédelmi szintet határoz meg:

1. Nyilvános adat: minden olyan információ és adat, amit a
   a. Társaság magáról közzétesz, sajtóban közösségi médiában megjelentet,
   b. nyilatkozik,
   c. jogszabályi kötelezettségének eleget téve nyilvánosságra hoz,
   d. bárki számára akadálytalanul megismerhetővé tesz.

2. Bizalmas adat: Minden olyan információ és adat, amely
   a. kezelését jogszabály szabályozza,
   b. a Társaság üzletmenetére, működésére hatással van vagy lehet,
   c. megismerése csak a Társaság által kijelölt személyek és szervezetek számára hozzáférhető.

3. Titkos adat: Minden olyan információ és adat, amely
   a. a Társaság működését és üzletmenetét, üzleti céljainak elérését jelentősen befolyásolja.

Minden, külön minősítéssel el nem látott dokumentum, adat és információ és azt ezt kezelő, biztosító, vagy tároló rendszerek automatikusan a „Bizalmas adat" kategóriába sorolandók.

Amennyiben egy rendszerben, eszközön, szolgáltatásban több adatvédelmi besorolás alá tartozó információt kezelnek, úgy a rendszerre a benne előforduló minősítések közül a legszigorúbb besorolás fog vonatkozni.

6. Rendszerek és szolgáltatások akvizíciója, igénybevétele, beszerzése

6.1 Külső rendszerek szolgáltatásainak igénybevétele

Bármely külső szolgáltatást annak igénybevétele előtt átfogó vizsgálatnak kell alávetni. Amennyiben a megfelelőségi vizsgálathoz az adatkérés nem követelhető meg a szolgáltatótól, azonban a termék/szolgáltatás használata indokolt (pl: Microsoft termékek, AWS szolgáltatások, Google-Cloud, Azure Cloud, eszköz vagy alkalmazás gyártója, stb.) akkor a rendelkezésre álló információk alapján elsősorban harmadik fél által kiállított megfelelőségi jelentések (ISO tanúsítvány, SOC-1/2/3 riport, SOX kontrolok megléte, közzétett sérülékenységi vizsgálati eredmény, stb) alapján, másodsorban a Társaság maga által elvégzett és a kockázatkezelésben feltüntetett vizsgálata alapján kell kezelnie.
A Társaság a **külső szolgáltatásokról nyilvántartást** vezet, feltüntetve az ott megvalósuló és használt szerep- és feladatköröket, összerendelve a társaság aktuális munkaköreivel és feladataival – ***6. számú melléklet.***

7. Biztonságtervezési alapelvek

7.1 Folyamatos felügyelet és monitorozás

A Társaság valamennyi rendszerén és szolgáltatásán folyamatos felügyeletet és monitorozást valósít meg a

- keletkező naplóállományok munkakörhöz kötött ellenőrzésével,
- az informatikai biztonságot szolgáló céleszközök üzemeltetésével,
- a rendelkezésre álló frissítések, javítócsomagok alkalmazásával,

valamint külső, független auditok és szakértők igénybevételével.

8. Hozzáférések kezelése

8.1 Sikertelen bejelentkezések kezelése

A felhasználói fiókok védelme érdekében – amennyiben azt a rendszerek lehetővé teszik - a sikertelen bejelentkezéseket naplózni kell, valamint meg kell határozni azok maximális számát, ezt elérve pedig korlátozni kell a hozzáférést. A sikertelen bejelentkezések számát időintervallumra vetítve is vizsgálni szükséges, amennyiben az adott rendszerek lehetővé teszik – figyelembe véve a minden rendelkezésre álló biztonsági elem használatára vonatkozó elvet:

Sikertelen bejelentkezések maximális száma: 5

Felhasználói fiók zárolása: 30 percre

8.2 Tájékoztatás a rendszerek használata előtt

A Társaság belső rendszereihez történő hozzáférés előtt egységes bejelentkezési képernyőt határoz meg AD csoportházirenddel, melyen a rendszerekbe történő bejelentkezés előtt megjeleníti a következőket:

- Felhasználó tájékoztatása, hogy a Társaság rendszerét használja.
- Felhasználó tájékoztatása a jogosulatlan használat bűntetőjogi következményeiről.
- Felhasználó tájékoztatása, hogy tevékenységét megfigyelhetik, naplózhatják, monitorozhatják.
- Felhasználó tájékoztatása, hogy rendszerbe történő belépéssel elfogadja és tudomásul veszi, magára nézve kötelezőnek ismeri el a használati feltételeket.

8.3 Azonosítás, hitelesítés nélkül igénybe vehető informatikai szolgáltatások, rendszerek

A Társaság a nyilvánosan elérhető Weblapján kívül nem határoz meg más, azonosítás nélkül hozzáférhető rendszert.

8.4 Távoli hozzáférés biztosítása

A távoli hozzáférés kizárólag megfelelő azonosítást követően, engedélyezett felhasználók számára, védett csatornán keresztül történhet. A Társaság a határvédelmi eszközökön VPN hozzáférést biztosít.

8.5 Vezeték nélküli hozzáférés

8.5.1 Belső hálózat

A Társaság informatikai rendszereihez történő vezeték nélküli hozzáférés nem biztosított.

8.5.2 Vendég hálózat

A nyilvános (vendég) WiFi hálózatot szeparálni kell az egyéb hálózatoktól, azon csak internet elérést szabad biztosítani. A hálózat legalább WPA2 szintű titkosítást kell alkalmazni, lehetőség szerint MAC cím szűréssel, és engedélyezéssel.

9. Oktatás, képzés

A Társaság informatikai rendszereihez csak olyan személynek adható hozzáférés, aki
- megfelelő (bizonyított) képzettséggel rendelkezik az adott rendszer használatához;
- ismeri annak az adott feladat elvégzéséhez szükséges funkcionalitásait;
- tisztában van az adott rendszer használatából eredő biztonsági kockázatokkal és hatásokkal;
- megfelelő, felelős viselkedéssel képes a rendszer használatára;
- ismeri és betartja a jelen szabályzatban és vonatkozó mellékleteiben foglalt előírásokat.

9.1 Oktatások rendje, hatóköre

A Társaság minden felhasználó számára (belső és külső egyaránt) kötelező informatikai biztonsági – biztonságtudatossági oktatást ír elő, **legalább évente egy alkalommal**, melyhez a cégvezetés biztosítja a szükséges erőforrásokat. Az oktatás elmulasztása esetén a felhasználó 60 nap haladékot kap annak pótlására, ezt túllépve a felhasználói jogosultságokat fel kell függeszteni.

Az új felhasználók esetében a munkavégzés feltétele biztonsági-biztonságtudatossági oktatás teljesítése.
A Társaság törekszik valamennyi felhasználója számára a legteljesebb, legmagasabb szintű oktatást biztosítani, egyes esetekben azonban differenciál a speciális ismereteket igénylő területeken (pl: rendszer üzemeltetői, adminisztrátorok).

Az oktatás célja a rendszerek használata során
- a felmerülő kockázatok azonosítása, csökkentése, elkerülése,
- felkészítés az ismertté vált támadási módszerek felismerésére, elhárítására,
- az elmúlt időszakban bekövetkezett és tapasztalt események, incidensek tanulságainak levonása, megelőző magatartás kialakítása,
- általános biztonsági szemlélet kialakítása és erősítése,
- az informatikai rendszerekben bekövetkezett változások tételes ismertetése, amennyiben azok érintik az informatikai biztonságot.

11.Konfiguráció kezelés

11.5 Szoftverhasználat szabályozása

A Társaság meghatározza az engedélyezett szoftverek körét, melyről nyilvántartást vezet, feltűntetve a felhasználó összes engedélyezett, egyidejű engedélyezett, különféle jogosultságokkal előfizetett/megvásárolt és engedélyezett számát.

Az engedélyezett szoftverek listáját az Informatikai csoport tartja nyilván, frissíti és szükség esetén bővíti, szűkíti.

13. Azonosítás és hitelesítés

Azonosításra és hitelesítésre a következő metódusokat alkalmazza:

- Felhasználónév és jelszó párosa, ahol a jelszavak vagy központi (AD) bejelentkezéshez kötött, vagy helyi (lokális) nyilvántartásúak.
- Felhasználónév, jelszó és többfaktoros azonosításra szolgáló eljárás, ahol a fentieken túl az azonosításhoz és hitelesítéshez további – egyszer használatos jelszó generátor, vagy internetes kapcsolattal rendelkező, értesítési üzenet alapú (push notification) másodlagos azonosítást is megkíván a rendszer.
- Kulcs, kulcspár, vagy tanúsítvány alapú azonosítás, ahol a felsoroltak birtokában történik a felhasználó vagy rendszer azonosítása, hitelesítése.

A Társaság törekszik megvalósítani a többfaktoros azonosítást minden szükséges esetben, ahol az informatikai rendszerek erre lehetőséget adnak.

Közös használatú azonosítók és jelszavak használata esetén a felhasználók köréből kikerülő személy esetén a jelszót haladéktalanul meg kell változtatni, kivéve, ha a hozzáférést egyéb módon korlátozni lehet (fizikai hozzáférés kilépett dolgozó esetén, zárt hálózathoz történő hozzáférés visszavonása, stb). A jelszavak cseréje ezekben az esetekben is javasolt 30 napon belül.

13.1 Névkonvenció

A Társaság által generált azonosítók az alábbi névkonvenciók követik:

a) Felhasználói azonosítók képzésének módja:
vezetéknév.keresztnév@delkom.local
vezetéknév.keresztnév@delkom.hu
a személyazonosító okmányban megadott név, vagy a felhasználó által kért név alapján
Névazonosság esetén a tévesztés elkerülése érdekben: elsősorban kerülni kell a hasonló azonosítók létrehozását, ha ez elkerülhetetlen, akkor sorszámozni kell a felhasználói azonosítókat.
Ügyviteli rendszerek esetében lehetőség szerint kerülni kell a más rendszerekben használt felhasználói azonosítók és jelszavak használatát.
A privilegizált felhasználók esetében a felhasználói szerepkörre utaló (pl admin, security, network, stb) utalást kell feltüntetni az elnevezésben.
A nem saját állományú felhasználók esetén szerepeltetni kell a felhasználói azonosítóban azok státuszát „ext" (external, külsős) kiegészítéssel.

13.2 Hitelesítésre szolgáló eszközök kezelése

A Társaság a hitelesítésre szolgáló jelszavak kezelését és kiadását a Jelszókezelési szabályzatban határozza meg, amelyet a ***11. számú melléklet tartalmaz***.
A Társaság a hitelesítésre szolgáló, többfaktoros azonosításra szolgáló eszközként hard tokent illetve a mobiltelefonokra telepíthető authenticator programokat használja. A telepítést és beállítást kizárólag az Informatikai csoport végezheti.

A Társaság biometrikus azonosítást a
- mobiltelefonokon engedélyezi,
- egyéb számítástechnikai eszközön az IBF külön engedélyéhez köti. Az engedély kiadása mellett a felhasználót külön tájékoztatni kell az azonosítás korlátairól és veszélyeiről.

13.3 Azonosítók újbóli felhasználása, változtatása

A Társaság a visszavont, érvénytelenített, felfüggesztett azonosítókat kötött időn belül nem használja fel újra. Azonosítót leghamarabb 1 év türelmi idő múlva lehet újra használni, amennyiben ez nem elkerülhető.

15. Karbantartás, frissítés

A Társaság törekszik arra, hogy informatikai eszközei, szolgáltatásai beszerzésekor vagy előfizetésekor gyártói támogatással, és kiterjesztett garancia feltételekkel vásárolja, vagy fizesse elő. Az üzembe helyezés során az eszközök gyártói támogatási idejére legalább 3 évet ír elő. Amennyiben műszaki, gazdasági indokok miatt ettől el kell térni, úgy azt a kockázatkezelésben szerepeltetni kell.

Általános felhasználói környezetben mind a munkaállomások, mind a mobil eszközök esetében kötelezően előírja, hogy csak gyártói támogatással rendelkező eszközöket és szoftver elemeket lehet használni.

A rendszerek, rendszerelemek karbantartása kizárólag ütemezetten és tervezetten történhet, ez alól kivételt képeznek a
- hiba elhárítási,
- esemény kezelési eljárások.

16. Adathordozók védelme

A Társaság informatikai eszközeinek megbontása, az adathordozók kiszerelése kizárólag az Informatikai csoport, vagy megbízottjai, partnerei számára engedélyezett.

A Társaság hordozható adathordozók használatát a következőképpen írja elő:

- Csak az egyedileg, az engedélyezett felhasználók számára megengedett külső adathordozó csatlakoztatása a munkaállomásokhoz (csoportházirend alapján, AVP).

- Csak és kizárólag a társaság tulajdonát képező hordozható adathordozók csatlakoztathatók az Társaság informatika eszközeihez.
- Idegen adathordozó használata Tilos, kivétel képeznek a gyártói eszközök, melyeket használat előtt minden esetben vírusvédelmi vizsgálatnak kell alávetni.
- Tilos a Társaság mobil adathordozóit más rendszerekhez csatlakoztatni.
- A kiadott, eszközöket személyhez kell rendelni (nyilvántartása az AVP rendszerben történik.)
- A Társaság rendszeresen ellenőrzi a kiadott adathordozók tartalmát, az ellenőrzéseket az IBF szervezi és hajtja végre. Az adathordozókat minden felhasználó köteles átadni ellenőrzés céljából.

18. Tervezés, biztonsági követelmények meghatározása

18.1 Viselkedési szabályok és normák külső webhelyek és közösségi média használata során

A Társaság a külső webhelyek, közösségi és szórakoztató médiák elérését biztonsági megfontolásból korlátozhatja. A munkahelyen kívüli kommunikáció során előírja a felhasználóknak, hogy sem a Társaságról, sem tevékenységéről, sem a használt informatikai rendszerekről, szolgáltatásról, műszaki és védelmi megoldásokról nem adható ki információ harmadik félnek, csak az IBF írásos engedélyével. Egyebekben a Társaság **informatikai etikai kódex**e alkalmazandó. (lásd ***14. számú melléklet***) Kivételt képeznek azon felhasználók és/vagy szerződött partnerek, akik munkakörükből adódóan a közösségi médiában, interneten, webportálon és egyéb felületeken hivatottak információt közzé tenni.
Partnerrel, harmadik féllel egyaránt csak titoktartási megállapodás aláírása után osztható meg „Bizalmas", vagy „Titkos" információ. A titoktartási megállapodás tartalmi ellenőrzése a jogi koordinációs vezető feladata.

22. Mellékletek

- **2. számú melléklet**: A jogosultság igénylésének folyamata belépő és kilépő dolgozók esetén, illetve munkakör, feladatkör változása esetén
- **11. számú melléklet**: Jelszókezelési szabályzat
- **14. számú melléklet**: Informatikai etikai kódex

Pécs, 2024. október 15.

Jelen szabályzat kiadásával a korábban kiadott DK-27-11-4-10/B-1/2018 iktatószámú szabályzat hatályát veszti.

Érvényes: 2024. október 18-tól visszavonásig.

Kapják: minden szervezeti egység

Dél-Kom
Nonprofit Kft.

IBSZ 2 sz. melléklet

Jogosultság igénylés, módosítás és visszavonás folyamata

A jogosultság igénylését, módosítását vagy visszavonását a levelező rendszerben (informatika@delkom.hu) indított folyamattal indítja a felhasználó felettes vezetője.

A folyamat:

- a felhasználó felettes vezetője, mint igénylő, a folyamat indítója
- a szakági vezető, mint engedélyező (helyettesítés esetén tájékoztatás a szakági vezető részére)
- az informatikai csoport, mint végrehajtó
- az ellenőr, aki esetenként szúrópróba-szerűen, évente legalább egyszer teljes körűen ellenőrzi a jogosultságokat és szerepköröket (IBF)

Az igényt lehetőség szerint a tervezett hatálybalépési idő előtt 5 nappal szükséges elindítani. A szakági vezetők, mint engedélyezők a következő személyek lehetnek, jogosultságot kizárólag ők engedélyezhetnek, módosíthatnak vagy vonhatnak vissza:

- Gazdálkodás és számvitel: Paizs József (gazdasági vezető)
- Jog: Dr. Miklósa Mária (jogi koordinációs vezető)
- Igazgatás, Adminisztráció: Lévayné Hajdics Katalin (adminisztrációs koordinációs vezető)
- Szolgáltatás: Gálfi Andrea (szolgáltatási koordinációs vezető)
- Szállítás: Hoffmann Bálint (szállítási koordinációs vezető)
- Környezetvédelem: Farkas Patrícia (környezetvédelmi csoportvezető)
- Létesítményfenntartás: Rónai Norbert (létesítményfenntartási vezető)

A közvetlenül az ügyvezető irányítása alatt álló felhasználóknál engedélyező az ügyvezető vagy az általa megjelölt szakági vezető lehet. Ebben az esetben a folyamat indítója maga a felhasználó.

Amennyiben az adott szakág vezetője akadályoztatva van, más szakági vezető az engedélyezési jogkört átveheti, ebben az esetben mellékútvonalba be kell vonni az adott terület szakági vezetőjét tájékoztatásra.

Kilépéskor a felettes vezető részéről szükséges különös intézkedések:

Kilépéskor, munkaviszony megszűnésekor rendelkezik az adatok, jogosultságok és feladatok helyettesítő személyhez rendeléséről, az érintett szervezeti egység és külső partnerek tájékoztatásáról, gondoskodik az esetleges jogsértő magatartás megelőzéséről, nyilatkoztatja kilépő felhasználót, hogy személyes adatokat nem tartalmaznak a hozzáférésével elérhető felhasználói fiókok, azok munkahely vezetőjének, vagy a helyettesítő személynek átadhatók. Kilépéskor ennek hiányában a kiléptetési folyamat nem folytatható.

Dél-Kom
Nonprofit Kft.

11. sz. melléklet

Jelszó szabályzat

A Társaság az informatikai rendszerekhez történő hozzáférések, a felhasználók azonosítása során eltérő erősségű jelszavakat és azonosítási módokat határoz meg. A jelszóhasználat során törekedni kell a minél nehezebben kitalálható, a felhasználóhoz nem köthető kódok kialakítására. A jelszóhasználat során az egy rendszer – egy jelszó elvet kell alkalmazni. A központi azonosítást biztosító rendszerek esetében az azonosítást végző megoldás (pl.: AD authentikáció) tekintendő egy rendszernek.

A rendszerek használói számára kifejezetten TILOS:

- Máshol, más rendszerekben használt jelszavak alkalmazása, különös tekintettel a közösségi felületekre!
- A jelszavak megjegyeztetése, tárolása a böngészőkben!
- A személyhez rendelt, egyedi azonosításra szolgáló felhasználói jelszavak megosztása másokkal!
- Könnyen kitalálható, személyhez, vagy a Társasághoz köthető jelszavak használata!
- Jelszavak hozzáférhető helyen történő tárolása, munkakörnyezetben papírra, cetlire felírva, számítógépen dokumentumokban, védelem nélküli állományokban tárolva!

Jelszóképzés példák:

Kifejezetten kerülendő, **rossz** jelszavak például: jelszó123, asdf1234, qwertz, 12345, andi123 (főképp andi nevű felhasználóknál), Delkom123, Születési dátum, családtag és háziállat neve, telephelyre, szervezeti egységre utaló jelszó, gmail-en, facebook-on, magánszférában, stb. használt jelszavak.

Néhány példa a fenti kritériumoknak megfelelő jelszóképzésre:

- **É**n **2**005 **m**ájusában **k**ezdtem **a Dél-Kom**nál, **m**int **f**őportás **é**jjeli **m**űszakban**!**
  - Az ebből létrehozott jelszó: **É2mkaD,mfém!**
- **A** **L**idlben **30%-**os **l**eértékelés **v**olt **m**inden **b**arkács **e**szközre
  - Az ebből létrehozott jelszó: **AL30%-lvmbe**
- **Ej, mi a kő! tyúkanyó, kend**
- **A** szobában **l**akik **i**tt **b**ent**?**
  - Az ebből létrehozott jelszó: **E,mak!t,kAslib?**

Minden eljárás csak addig jó, amíg titokban marad!

Kategóriák:

- Általános célú, felhasználói azonosítók, egyedi azonosításhoz.
- Általános célú, közösen használt felhasználói azonosítók.
- Privilegizált, rendszergazdai jogosultságok, egyedi azonosításhoz.
- Privilegizált, rendszergazdai jogosultságok, közös felhasználáshoz.
- Technikai azonosítók, rendszerek, rendszer komponensek azonosítására.
- A karbantartási célú és ideiglenes azonosítók - felhasználási céljuktól függően – a fenti kategóriákkal azonosak.

Dél-Kom
Nonprofit Kft.

11. sz. melléklet

Rendszer megnevezése	Felhasználói kategória	Jelszó hossza	Jelszó komplexitás elvárások	Jelszó érvényessége	Többfaktoros azonosítás	Kezdeti jelszó
delkom.local AD	felhasználói, egyedi	12	kisbetű, nagybetű, szám, speciális karakter, utolsó 10 jelszó újbóli használat tiltása	3 hónap	nem	igen
	privilegizált, egyedi	20	kisbetű, nagybetű, szám, speciális karakter, utolsó 10 jelszó újbóli használat tiltása	1 hónap	igen	nem
	technikai azonosító	20	kisbetű, nagybetű, szám, speciális karakter, utolsó 10 jelszó újbóli használat tiltása	korlátlan	nem	nem
	privilegizált, vészhelyzeti	20	kisbetű, nagybetű, szám, speciális karakter, utolsó 10 jelszó újbóli használat tiltása	korlátlan	nem	nem
Ügyviteli rendszerek	felhasználói	8	nincs	korlátlan	nem	nem
	privilegizált	8	nincs	korlátlan	nem	nem
...						
MS Authenticator	általános	6	6 számjegyű PIN kód, és vagy biometrikus azonosítás	korlátlan	nem	nem
...						
Hálózati eszközök	privilegizált, közös	20	nincs	korlátlan	nem	nem

14. sz. melléklet

Etikai kódex

Az etikai kódex célja

Jelen etikai kódex célja a Társaság működésének, az ott kezelt adatok kiemelt bizalmassággal történő kezelésének biztosítása, az érzékeny adatok védelme érdekében kötelezően betartandó viselkedési normák meghatározása a dolgozók részére.

A dolgozók munkavégzésük során speciális információkhoz férhetnek hozzá, melynek során törekedniük kell azok bizalmasságának megőrzésére, mind az üzleti titkok, mind a személyes adatok, mind a partnerekkel, beszállítókkal kapcsolatos információk, mind pedig az esetleges működési rendellenességek vonatkozásában. Ezen információk illetéktelen felhasználása veszélyeztethetik az adott a Társaság és rendszereinek működését, visszaélésekre, károkozásra adhat lehetőséget.

A munkavégzés során továbbá fennállhat a veszélye mind a social engineering támadásnak, mind egyéb – személy elleni - célzott adatszerzésnek, provokációnak. Az etikai kódex további célja ezen kitettség csökkentése.

Munkavégzéssel, adatkezeléssel kapcsolatos elvárások

- A Társaság adatkezelői és/vagy adatfeldolgozói minőségben és szerepkörben jár el saját dolgozói és ügyfelei, beszállítói személyes adatainak kezelése során. Kiemelt cél a Társaság és dolgozói által megismert és kezelt adatok védelme, azok bizalmasságának megőrzése.
- A dolgozók semmilyen más módon nem használhatják fel a birtokukba jutott információt, ismeretanyagot, adatokat, folyamatokat, eljárásokat, azokat nem adhatják át jogosulatlan harmadik félnek.
- A dolgozóknak kerülniük kell minden olyan utalást mind a munkavégzés során, **mind a magánéletben**, mely információt közöl a Társaság rendszereiről, az ott végzett munka természetéről, az ott birtokába került információkra, az ügyfelek és beszállítók beazonosítására, a használt eszközökre, a Társaságra és munkatársakra vonatkozóan is – különösen családban, baráti összejöveteleken, közösségi hálón, szakmai fórumokon. A munkahely csak általános téma legyen, napi történések, események mesélése nélkül.
- A dolgozóknak az információ kiáramlást zéró közeli értéken kell tartaniuk, a lehető legkisebb támadási vektort biztosítva személyük és a Társaság ellen.
- A közösségi portálokon, hálózatokon, fórumokon, stb. közzétett és megosztott információk nem tartalmazhatnak utalást a Társaságra, az ott végzett munkára.
- A dolgozóknak kerülniük kell az on-line kapcsolati háló kiterjesztését munkatársaikra, ügyfeleikre.
- Kifejezetten tiltott a közösségi hálózatokon folytatott egymás közti üzleti kommunikáció (pl: messenger, zoom, google drive, stb), üzleti célra a Társaság által biztosított platformokat kell használni.

- A dolgozóknak tudatosan kerülniük kell a szakmai vitáknak álcázott, provokatív, adatszerzésre irányuló szakmainak *tűnő* vitákat.
- Nyilatkozat, interjú kérésekre, megkeresésekre csak az arra felhatalmazott dolgozó válaszolhat érdemben, kizárólag a Társaság engedélyével.
- Készenlét, ügyelet, távoli munkavégzés ellátása során különösen ügyelni kell az adatok és rendszerek betekintés, meghallás elleni védelmére. Törekedni kell arra, hogy a dolgozó egyedül legyen ilyenkor. A felhasználóknak tudatosítani kell magukban, hogy nem védett környezetből folyik a rendszerek használata, így fokozottan kell ügyelnie a biztonsági előírások betartására.
- A munkahelyi eszközöket csak és kizárólag a munkahelyi feladat elvégzése érdekében szabad és megengedett használni.
- Az internet használata során különös figyelmet kell fordítani annak biztonságára! Kerülni kell a védelem nélküli nyílt hálózatokat! A Társaság informatikai hálózatán kívül történő eszköz és szolgáltatás használat közben kiemelt gondossággal kell eljárni és védeni a felhasználói jogosultságokat, hozzáféréseket és az elért szolgáltatásokat, valamint a használt eszközöket!
- A magán és céges eszközök közötti adatcsere nem megengedett, különös tekintettel a mobiltelefonokra.
- A dolgozóknak el kell választaniuk a magáncélú használatot az üzleti felhasználástól.
- A céges e-mail fiók használata magán célra nem megengedett, azzal regisztrálni magán célból tilos (pl.: Ügyfélkapu, Kréta, Neptun, Webshopok, közösségi hálózatok és platformok, stb. - valamint ezek hírlevelei, értesítései.)
- Kifejezetten tiltott a céges eszközökön más, magáncélú külső erőforrások, postafiókok, meghajtók csatlakoztatása (privát postafiók, OneDrive, dropbox, googledrive, stb.)
- A személyi használatra kapott mobiltelefonok egyedi, a gyártó által biztosított backup funkcióihoz, készülék védelmi és követési megoldásaihoz csak céges postafiókkal megengedett regisztrálni és azokat használni a visszaállíthatóság érdekében.
- A számítástechnikai berendezésekhez idegen, nem ellenőrzött más eszközt, adathordozót, telefont, perifériát, stb. csatlakoztatni még töltés céljából sem megengedett!
- A felhasználók kötelessége betartani valamennyi Informatikai biztonsági előírást és alkalmazni valamennyi rendelkezésre álló informatikai védelmi megoldást.
- A Társaság által biztosított, vagy a Társaság érdekében üzleti célból igénybe vett külső erőforrásokhoz és szolgáltatásokhoz történő csatlakozáshoz csak a Társaság eszközeit lehet használni.

Viselkedési normák

- A dolgozó viselkedésével, megjelenésével, kommunikációjával a Társaságot képviseli, minden esetben elvárt ezek kulturált teljesítése.
- Elvárt az összeszedett, átgondolt, részletes tájékoztatás és a precíz kommunikáció. A türelmes és megnyugtató hangvétel a megkívánt - mind a belső, mind a külső ügyfelekkel szemben.

„Üres íróasztal" szabály

Az irodahelyiségekben az íróasztalokon rendet kell tartani. Csak a munkához felhasznált iratok, adathordozók lehetnek az asztalokon munkaidőben. Munkavégzés után, vagy ha nem tartózkodik senki a helyiségben, az íróasztalokról az adathordozókat, munkához felhasznált iratokat zárható szekrénybe el kell zárni az illetéktelen hozzáférés megelőzése érdekében.

„Sötét képernyő" szabály

A felhasználók kötelesek a munkájuk megszakítása vagy befejezése után a számítógépet zárolni vagy kikapcsolni. A munkaállomásokat úgy kell beállítani, hogy ha azokat hosszabb időre (több mint 5 perc) felügyelet nélkül hagynák, akkor a képernyővédő automatikusan induljon el és csak a felhasználó újbóli azonosítását követően lehessen azt használni.

Tárgyaló rendje

A tárgyalókkal kapcsolatosan az alábbi szabályokat kell betartani:

- Tilos a tárgyalóban felügyelet nélkül hagyni számítógépet.
- Bizalmas információ kivetítése, vagy táblán, bemutatása esetén az illetéktelenek betekintését meg kell akadályozni.
- A táblákon, hagyott információkat a tárgyalóterem elhagyása előtt törölni kell.
- A tárgyalóban is alkalmazni kell az "Üres asztal" szabályt.

Jelszóhasználat

Mindenki köteles a számára kiadott hozzáféréseket, jelszavakat bizalmasan kezelni. A felhasználóknak minőségi jelszavakat kell használniuk és azokat rendszeresen cserélniük kell. A jelszavak nem tartalmazhatnak könnyen kitalálható, személyhez vagy a Társasághoz köthető, ismétlődő, billentyűzeten egymást követő karakter sorozatokat.

A **Társaság** javasolja a jelszóhasználat szigorúságának és védelmének kiterjesztését a privát használatra is.

Szoftverhasználat

A felhasználók előretelepített szoftverekkel veszik használatba a számítógépet. Telepítésre- és törlésre csak az üzemeltetési vezető, vagy a rendszermérnök jogosult. A Társaság rendelkezik engedélyezett szoftverlistával („szoftver leltár"). A munkatársaknak lehetőségük van szoftver igénylésre.

A munkaállomásokon található szoftverek éves jelleggel felülvizsgálatra kerülnek.

A munkatársak **nem telepíthetnek** szoftvert a számítógépre, és nem használhatnak portable alkalmazást sem jóváhagyás nélkül.

Vagyontárgyak védelme

A vagyontárgyak védelmére vonatkozó általános szabályok

- Az informatikai berendezések használata közben és azok közelében étkezni, dohányozni tilos.
- A használati utasításokban a gyártó által megadott szabályokat mindig be kell tartani.
- Munkaidő befejezésekor a munkaállomást ki kell kapcsolni. Tilos a munkaállomást bekapcsolva hagyni magáncélú internetes letöltés vagy távoli használat céljából.

- A helyi számítógépen vagy mobil eszközön történő munka során létrehozott dokumentumokat a lehető legrövidebb időn belül a megfelelő központi szervereken kell elhelyezni.
- Informatikai eszközök, adathordozók elvesztését, ellopását, megrongálódását haladéktalanul jelenteni kell az üzemeltetési vezetőnek.
- Informatikai eszközöket, adathordozókat TILOS nyilvános helyen őrizetlenül hagyni!
- Az informatikai eszközöket úgy kell elhelyezni, hogy a véletlenszerű rongálás (leesés, leverés, csepegő, fröccsenő folyadék) ellen minél védettebb legyen.
- A notebook számítógépeket a munkahely elhagyásakor haza kell szállítani, vagy zárható irodában és/vagy zárható szekrényben tárolni a következő felhasználásig.

Mobil eszközök védelme szállítás közben

- A notebook-ot táskában, védett körülmények között kell szállítani! Szállítás közben óvni kell a nagy melegtől, közvetlen napsugárzástól, nagy hidegtől, portól, nedvességtől.
- A notebook-ot és adathordozókat TILOS (még rövid időre is) az autóban hagyni!
- Repülőgépen a kézipoggyászban kell szállítani.
- Szállítás közben a számítógépnek teljesen kikapcsolt, vagy hibernált állapotban kell lennie, gondoskodva a véletlen bekapcsolás elleni védelemről.
- Gépkocsival történő szállítás esetén a zárt/fedett csomagtartóban kell elhelyezni, a jármű elhagyásakor magával kell vinnie, a közlekedés során az csomagtér/ajtónyitásos, ablakon benyúlva elkövetett lopást/rablást meg kell akadályozni (pl központi zár használatával, ablakok részleges nyitásával, körültekintő közlekedéssel).
- Szállítás előtt mindig meg kell bizonyosodni róla, hogy minden szükséges külső tartozékkal együtt került elcsomagolásra, (pl. tápegység, egér, dokkoló, adathodotó, mobil stick, stb.)

Mobil eszközök védelme a telephelyen kívüli használat közben

- Ha a készülék a szállítás során túlzottan lehűlt, vagy felforrósodott, használat előtt meg kell várni amíg hőmérséklete felveszi a környezeti hőmérsékletet.
- Használat közben óvni kell az erős napsugárzástól, portól, nedvességtől, erős rázkódástól.
- Különösen külföldön az elektromos hálózatra történő csatlakozás előtt meg kell győződni arról, hogy a hálózat megfelel a készülékére megengedett értékhatároknak.
- Telephelyen kívül lehetőleg soha ne hagyja felügyelet nélkül a mobil eszközöket.
- Tilos a mobil eszközök használatát harmadik félnek átengedni, sem idegenek, sem családtagok, rokonok, ismerősök nem használhatják ezeket.
- Tilos idegen eszközt adatátvitelre alkalmas kábellel csatlakoztatni az eszközökhöz, még **töltés céljából sem!**

Információbiztonsági Továbbképzés

A Társaság legalább éves jelleggel továbbképzést tart a munkavállalói számára, melynek célja az információbiztonsággal kapcsolatos tudás frissítése, bővítése, így a humánkockázat csökkentése. A továbbképzésen a munkavállalónak jelenlétiív aláírásával és írásbeli teszttel kell igazolnia a részvételét. A képzés elmulasztása esetén a Társaság korlátozza az informatika rendszerekhez történő hozzáférést.