1. számú melléklet

KKM Magyar Diplomáciai Akadémia Korlátolt Felelősségű Társaság

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Hatályos: 2026. év április 1. napjától

jóváhagyta:

Horváth Csilla
ügyvezető

KKM Magyar Diplomáciai Akadémia
Korlátolt Felelősségű Társaság
1107 Budapest, Ceglédi utca 2.
Cégjegyzékszám: 01-09-203215
Adószám: 14163241-2-42
Banksz.: 10300002-13530333-00014905

2/2026. (IV. 1.) számú ügyvezetői utasítás

az Informatikai Biztonsági Szabályzat kiadásáról

Horváth Csilla, a KKM Magyar Diplomáciai Akadémia Kft. (a továbbiakban: Szervezet) ügyvezetőjeként a Szervezet mindenkor hatályos Szervezeti és Működési Szabályzata alapján, a munka törvénykönyvéről szóló 2012. évi I. törvény 17. §-ára is tekintettel a következő utasítást adom ki.

1. A Szervezet Informatikai Biztonsági szabályzatát az 1. számú mellékletben foglaltak szerint határozom meg.

2. Az Informatikai Biztonsági Szabályzatot minden munkavállalónak kötelező megismernie, az abban foglaltak be nem tartása a Szervezet belső szabályainak megsértésének minősül, amely fegyelmi vétségnek is minősíthető.

3. Az Információ Biztonsági Szabályzat felülvizsgálata a Szervezet információbiztonsági felelőse hatáskörébe tartozik.

4. A jelen utasítás a kihirdetése napján lép hatályba, és hatálybalépésével egyidejűleg hatályát veszti az adatvédelmi és adatbiztonsági szabályzat kiadásáról szóló 3/2025. (III. 24.) ügyvezetői utasítás 1 függeléke („a Társaságnál alkalmazott információbiztonsági intézkedések, megoldások").

Budapest, 2026. április 1.

KKM Magyar Diplomáciai Akadémia
Korlátolt Felelősségű Társaság
1107 Budapest, Ceglédi utca 2.
Cégjegyzékszám: 01-09-203215
Adószám: 14163241-2-42
Bankszámlaszám: 10300002-13530333-00014905

Horváth Csilla
ügyvezető
KKM Magyar Diplomáciai Akadémia Kft.
Munkáltató

Melléklet:

1. számú melléklet: A Szervezet Informatikai Biztonsági Szabályzata

1. Általános rendelkezések

1.1 A szabályzat célja

Jelen Informatikai Biztonsági Szabályzat (a továbbiakban: **IBSZ** vagy **Szabályzat**) célja a **KKM Magyar Diplomáciai Akadémia Korlátolt Felelősségű Társaság** (továbbiakban: **Szervezet**) által vagy érdekében létrehozott, illetve üzemeltetett IT infrastruktúra sértetlenségének és rendelkezésre állásának, továbbá a Szervezet által létrehozott, kezelt és minden egyéb formában ismert adat, információ bizalmasságának, sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos biztosítása. A Szervezet célja továbbá, hogy tevékenységéből adódóan az üzletmenet-folytonosság állandó, kiemelt figyelmet kapjon az esetlegesen bekövetkező károk minimalizálása érdekében, továbbá megfelelő preventív intézkedésekkel alátámasztott felkészültséggel rendelkezzen, amely csökkenti vagy kizárja a bekövetkezhető károkat és azok mértékét, illetve elősegíti a Szervezet rövid időn belül történő reagálási képességét.
Az IBSZ kizárólag a hozzá tartozó függelékekkel együtt tekinthető teljes értékű és alkalmazható dokumentumnak. A függelékek tartalmazzák az egyes biztonsági osztályokhoz kapcsolódó specifikus követelményeket.
A Szabályzat és annak kiegészítő dokumentumai együttesen biztosítják a Szervezet információbiztonsági megfelelőségét a hatályos jogszabályokkal, különösen a **Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvénnyel, a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII. 23.) Korm. rendelettel**, valamint **a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. (VI. 24.) MK rendelettel** összhangban.
A Szabályzat az információbiztonsággal kapcsolatos jogszabályi előírások figyelembevételével, továbbá a NIST SP 800-53 Rev. 5 irányelv alapján került összeállításra.

1.2 A szabályzat hatálya

1.2.1 Személyi hatály

Jelen Szabályzat személyi hatálya kiterjed a Szervezet teljes személyi állományára, illetve a Szervezet minden, informatikai rendszereit használó, informatikai vonatkozású feladatot végző külső partnerére.
A Szabályzat rendelkezéseit alkalmazni kell a Szervezettel közvetlen vagy közvetett szerződéses kapcsolatban álló magánszemélyekre, jogi személyekre, valamint jogi személyiséggel nem rendelkező szervezetekre is úgy, hogy a polgári jogi szerződés erre utalást tartalmazzon.
A Szabályzat meg nem ismerése nem mentesít a felelősség és jogkövetkezmények alól.

1.2.2 Tárgyi hatály

A Szabályzat tárgyi hatálya kiterjed a Szervezet által üzemeltetett vagy használt informatikai eszközökre, azok elhelyezésére szolgáló létesítményekre, valamint az általuk kezelt, tárolt, továbbított adatokra.
A Szervezet kiszervezési tevékenység keretében partnerei információs vagyonát is kezelheti; ez esetben a szolgáltatási szerződés további biztonsági követelményeket írhat elő.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

1.2.3 Időbeli hatály

Jelen dokumentum **2026. április 1.** napján lép hatályba azzal, hogy annak rendelkezéseit a kihirdetés naptól kell alkalmazni, és visszavonásáig hatályos.

1.3 A szabályzat felülvizsgálata

A Szabályzatot minden új, releváns jogszabály hatálybalépése után, illetve jelentős architektúraváltozás vagy új fenyegetettség megjelenésekor haladéktalanul, de legalább **18 (tizennyolc) havi** gyakorisággal felül kell vizsgálni.
A felülvizsgálat elrendelésére a Szervezet ügyvezetője jogosult.
Rendkívüli felülvizsgálat szükséges különösen az alábbi esetekben:

- új informatikai technológiák bevezetése vagy megszűnése,
- lényeges új kockázatok azonosítása,
- a Szervezet igényeinek, céljainak megváltozása,
- a Szabályzat működésképtelenségének vagy elégtelenségének megállapítása.

2. Információbiztonsági irányelvek és kapcsolódó dokumentumok

2.1 Információbiztonsági Politika (IBP)

A Szervezet vezetősége világos iránymutatással, elkötelezettségének kinyilvánításával, az informatikai biztonsággal összefüggő felelősségi körök kijelölésével és elismertetésével aktívan támogatja az informatikai biztonságot a szervezetben.
Az IBP az információbiztonsági irányítási rendszer alapját képezi. Az IBP meghatározza a Szervezet információbiztonsági alapelveit, célkitűzéseit és elkötelezettségét az információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítására.
Az IBP kiterjed minden munkavállalóra, illetve alvállalkozóra, akik kötelesek megismerni és magukra nézve kötelezőnek elismerni.
Az IBP jelen dokumentummal koherens biztonsági szabályzat.

2.2 Információbiztonsági Irányítási Rendszer (IBIR)

A Szervezet munkavállalói, valamint vállalkozói számára rövid összegzést tartalmaz a Szervezet által támasztott követelményekről, azok betartásának elismeréséről.
Minden munkavállaló és alvállalkozó köteles megismerni és magára nézve kötelezőnek tekinteni.

2.3 Informatikai Biztonsági Szabályzat (IBSZ)

Az IBSZ az információbiztonsági szabályozás második szintű dokumentuma, jelen dokumentum és függelékei együttesen értelmezendők.
Minden munkavállaló, illetve vállalkozó számára kötelező az abban foglaltak betartása. A szabályok megsértése jogi kötelezettségszegésnek minősül, és azonnali felelősségre vonást vonhat maga után.

Fővárosi Törvényszék Cégbíróság Cg.: 01 09 203215

2.4 Egyéb, információbiztonságot érintő szabályozás

A harmadik szintű dokumentumok az információbiztonsági munkautasítások, amelyek a rendszerszintű beállításokat, adatvédelemmel kapcsolatos előírásokat, végrehajtandó folyamatokat és az azokhoz tartozó követelményeket tartalmazzák.
Az itt foglaltak minden érintett munkavállalóra, valamint vállalkozóra nézve kötelezőek, azok megismerése a munkavégzés feltétele.

3. Információbiztonság szervezete

3.1 Információbiztonsági szerepek és felelősségek

Az információbiztonsági tevékenységeket a Szervezet kijelölt munkatársainak részvételével kell koordinálni.

3.1.1 Szerepkörök és feladatok

A Szervezet az információbiztonság biztosítása érdekében az alábbi szerepköröket határozta meg:

- Ügyvezető,
- Információbiztonsági Felelős (IBF),
- Fizikai biztonsági vezető,
- Jogi Irodavezető,
- Megfelelési tanácsadó,
- IT üzemeltetési vezető,
- Adatvédelmi tisztviselő (DPO),
- IT üzemeltetés,
- Alkalmazásgazda,
- Adatgazda,
- Felhasználó,

A felhasználók információbiztonsági felelősségét a munkaköri leírások tartalmazzák.

3.2 Információbiztonsági szerepkörök

A Szervezet munkaköri leírásokban rögzíti a feladatokat és felelősségeket. Az alábbiakban az egyes szerepkörökhöz tartozó részletek szerepelnek.

3.2.1 Ügyvezető

Az ügyvezető a Szervezet legfelső szintű operatív vezetője, felelős a Szervezet biztonságos működéséért, így az információbiztonságért is.
Feladatai többek között:

- Az információbiztonsági stratégia és szabályozási környezet biztosítása.
- Irányelvek, szabályzatok jóváhagyása.
- Információbiztonság összhangjának biztosítása az üzleti célokkal.
- IBF és DPO kijelölése.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- Kockázatértékelések és intézkedések jóváhagyása.
- Erőforrások biztosítása.
- Kritikus incidensek kezelésének irányítása.

3.2.2 Információbiztonsági Felelős (IBF)

Az IBF felelős:

- Az IBIR kialakításáért, működtetéséért és fejlesztéséért a NIST 800-53 Rev5 és NIS2 követelmények alapján.
- A kockázatkezelésért: kockázatok azonosítása, értékelése, kezelése.
- Biztonsági szabályzatok és eljárások frissítéséért.
- Információbiztonsági tudatosság növeléséért, oktatásokért.
- Incidenskezelés irányításáért.
- Auditok szervezéséért.
- Hatósági kapcsolattartásért.

Hatáskörei:

- Döntéshozatal az információbiztonság területein.
- Jogosultságkezelés ellenőrzése.
- Auditok kezdeményezése.
- Jelentések készítése a vezetőség számára.

3.2.3 Fizikai biztonsági vezető

Felelős a szervezet fizikai területeinek védelméért, beleértve:

- Jogszabályoknak való megfelelés biztosítása.
- Fizikai biztonsági szabályok készítése, felülvizsgálata.
- Beléptetési rendszerek működtetése.
- Kamerarendszerek és riasztórendszerek kezelése.
- Oktatások szervezése.
- Tűzvédelem, vészhelyzeti tervezés.

Hatáskörei:

- Javaslattétel biztonsági módosításokra.
- Külső biztonsági szolgáltatók értékelése.
- Jelentések készítése fizikai kockázatokról.

3.2.4 Jogi irodavezető

Feladata:

- Munkavállalók információbiztonsági és adatvédelmi tudatosságának növelése.
- Beléptetési és kiléptetési folyamatok kezelése.
- Képzések szervezése és dokumentálása.
- Munkaköri leírások összehangolása biztonsági előírásokkal.
- Kapcsolattartás a DPO-val.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

3.2.5 Megfelelési tanácsadó

Felelős a beszállítók biztonsági megfelelőségéért:

- Beszállítói kockázatok értékelése.
- Szerződéses biztonsági követelmények biztosítása.
- Teljesítmény és incidensek felügyelete.
- Folyamatos kapcsolattartás beszállítókkal.

3.2.6 IT üzemeltetési vezető

Felelős:

- Informatikai rendszerek üzemeltetéséért és fejlesztéséért.
- Biztonsági intézkedések bevezetéséért.
- Kockázatok azonosításában való részvételért.
- Jogosultságkezelési szabályok betartatásáért.
- Incidenskezelés koordinálásáért.

Jogosult informatikai szabályzatok készítésére és intézkedések kezdeményezésére.

3.2.7 Adatvédelmi tisztviselő (DPO)

Feladata:

- Személyes adatok kezelésének felügyelete.
- Jogszabályoknak való megfelelés biztosítása.
- Hatásvizsgálatok támogatása.
- Adatvédelmi incidensek kezelése.
- Kapcsolattartás a NAIH felé.
- Oktatások szervezése.
- Nyilvántartások naprakészen tartása.

3.2.8 IT üzemeltetés

Feladatai:

- Hibabejelentések fogadása, kezelése.
- Incidensek nyomon követése.
- Felhasználói fiókok kezelése.
- Eszközök kiadása, nyilvántartása.
- Biztonsági események jelentése az IBF felé.

3.2.9 Adatgazda

Jogszabályi vagy műszaki alapon rendelkezik az adatok felett.
Feladatai:

- Adatok osztályozása.
- Adatvédelmi és használati szabályok meghatározása.
- Jogosultságok meghatározása.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- Védelmi intézkedések támogatása.

3.2.10 Felhasználó

Felhasználó minden munkavállaló, valamint vállalkozó.
Felelőssége:

- Rendszerek rendeltetésszerű használata.
- Előírások betartása, különösen adatvédelmi területen.
- Hibák jelentése.
- Oktatásokon való részvétel.
- Információbiztonsági előírások betartása.

3.3 Feladatkörök szétválasztása

A Szervezetnél el kell különíteni:

- fejlesztői és üzemeltetői,
- üzemeltetői és információbiztonsági,
- végrehajtói és jóváhagyói feladatokat.

A hozzáféréskezelésben a kérelmező, jóváhagyó és jogosultságot kiosztó szerepkörök is elválnak.

3.4 Kapcsolat a hatóságokkal

A hatóságokkal (pl.: NBSZ Nemzeti Kiberbiztonsági Intézet) az IBF tart kapcsolatot, távollétében vagy akadályoztatása esetén az ügyvezető. Adatvédelmi ügyekben a DPO bevonása kötelező. Az ügyvezető tájékoztatása minden esetben kötelező.

3.5 Kapcsolat a szakmai csoportokkal

Az IBF, illetve távollétében az IT üzemeltetési vezető:

- figyeli a fenyegetettségekkel kapcsolatos szakmai csatornákat,
- konferenciákon vesz részt,
- gondoskodik a biztonsági előírások naprakészen tartásáról.

4. Megfelelés

4.1 Biztonsági osztályba sorolás

A biztonsági osztályba sorolás célja, hogy a Szervezet által kezelt információs erőforrásokat — adatokat, rendszereket, alkalmazásokat — értékelje a bizalmasság, sértetlenség és rendelkezésre állás szempontjából, majd ezek alapján megfelelő védelmi intézkedéseket rendeljen hozzájuk.
A biztonsági osztályba sorolás kiterjed minden olyan elektronikus információs rendszerre (a továbbiakban: **EIR**), amelyre a Szervezet jogi, szerződéses vagy üzleti kötelezettséget vállalt.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

A Szervezet az alábbi alapelvek szerint végzi a biztonsági osztályba sorolást:

- Bizalmasság, azaz jogosulatlan hozzáférés elleni védelem,
- Sértetlenség, azaz jogosulatlan módosítás elleni védelem,
- Rendelkezésre állás, azaz időben történő hozzáférés biztosítása.

Az osztályozást évente, illetve minden, az adott EIR biztonságát, sértetlenségét vagy rendelkezésre állását befolyásoló körülmény felmerülése esetén el kell végezni.

A biztonsági osztályba sorolásáért az IBF felelős. Eredményeit az ügyvezető hagyja jóvá.

Osztályozási folyamat:

1. **Értékelés**: az alkalmazásgazda, IT üzemeltetési vezető vagy az IBF végzi.
2. **Kockázatelemzés**: a Szervezet kockázatmenedzsment keretrendszere alapján.
3. **Osztályba sorolás**: a három alapelv szerinti legmagasabb érték alapján.
4. **Dokumentálás:** az EIR biztonsági dokumentációjának elkészítése.
5. **Felülvizsgálat**: legalább évente vagy jelentős változás esetén.

4.2 Megfelelés a jogi és szerződéses követelményeknek

A Szervezet folyamatosan követi a működésére vonatkozó:

- jogszabályi,
- szabályozói,
- szerződéses

információbiztonsági követelményeket, és gondoskodik azok betartásáról.

Cél: a jogi és szerződéses megfelelés fenntartása, valamint a szabályszegések elkerülése.

4.3 Vonatkozó jogszabályi és szerződéses követelmények azonosítása

- Az információbiztonságot érintő jogszabályok követése az **IBF**, távollétében az **IT üzemeltetési vezető** feladata.
- A személyes adatok védelmére vonatkozó jogszabályok követése a **DPO** felelőssége.

Jogszabályváltozás esetén az IBF és/vagy a DPO:

- intézkedési javaslatot tesz,
- szükség esetén szabályzat-, folyamat-, vagy eljárásmódosítást kezdeményez.

Fővárosi Törvényszék Cégbíróság: 01 09 203215

4.4 Szellemi tulajdonjogok

A Szervezet elkötelezett a szellemi tulajdon védelme mellett.

Fő elvek:

- A Szervezet által létrehozott szellemi termék a Szervezet tulajdona.
- Engedély nélküli továbbítás vagy megosztás tilos.
- Csak jogtiszta szoftverek és digitális tartalmak használhatók.
- Licencfeltételek betartása kötelező.
- A Szervezet licencnyilvántartást vezet.
- Az IBF évente ellenőrzi az installált szoftvereket.
- A munkavállalók rendszeres tájékoztatást kapnak a követelményekről.

4.5 A feljegyzések védelme

A Szervezet az informatikai biztonsági rendszerdokumentációkat és feljegyzéseket csak az arra jogosultak számára teszi elérhetővé.

Papíralapú dokumentumok:

- Bizalmas vagy fokozottan bizalmas dokumentumok: zárt, kulccsal védett tárolás.
- Feleslegessé vált dokumentumok: iratmegsemmisítő használata kötelező.

Elektronikus dokumentumok:

- Jogosultsági rendszeren alapuló hozzáférés.
- Törlés esetén: fizikai törlés kötelező.
- Adathordozók kezelése külön szabályzat alapján.

Dokumentumok továbbítása:

Ismeretlen vagy gyanús címzettnek történő bármilyen adattovábbítás csak **IBF** vagy **IT üzemeltetési vezető** írásos (e-mailben történő) engedélyével végezhető.

4.6 A magántitok és a személyhez köthető információk védelme

Az elektronikus információs rendszerekhez és adatvagyonhoz való hozzáférés:

- a **legkisebb jogosultság elvén** történik,
- megfelelő tájékoztatást követően engedélyezhető.

A jelen IBSZ hatálya alá tartozó minden személy köteles:

- a belső titoktartási szabályokat betartani,
- a szerződéses és munkajogi előírásokat követni.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

Jogosulatlan adattovábbítás vagy információmegosztás azonnali jogi következményekkel jár.

5. Információbiztonsági irányítási rendszer

A Szervezet átfogó információbiztonsági irányítási rendszert (ISMS / IBIR) működtet annak érdekében, hogy biztosítsa az adatok bizalmasságát, sértetlenségét és rendelkezésre állását. A Szabályzat főként a védelmi és irányítási területeket foglalja össze, míg részletes szabályozások a függelékekben találhatók.

5.1 Adminisztratív védelmi intézkedések

A Szervezet az információbiztonság szervezeti alapjainak kialakításához adminisztratív intézkedéseket alkalmaz.

Fő elemei:

- Belső szabályzatok, folyamatleírások és utasítások kialakítása,
- Munkavállalók és partnerek oktatása, tájékoztatása,
- Titoktartási és biztonsági nyilatkozatok alkalmazása,
- Dokumentumkezelési és verziókövetési rend,
- Információbiztonsági szerepkörök és felelősségi körök meghatározása.

Cél: minden érintett ismerje és alkalmazza a rá vonatkozó biztonsági elvárásokat.

5.2 Kockázatmenedzsment keretrendszer

A Szervezet a fenyegetettségeket és kockázatokat formalizált rendszer keretében kezeli.

A kockázatmenedzsment fő elemei:

- Éves rendszeres kockázatelemzés,
- Kockázati szintek és egyértelmű értékelési módszerek,
- Kontrollok hozzárendelése a kockázatok csökkentése érdekében,
- Maradványkockázatok dokumentálása és eszkalálása,
- Intézkedések folyamatos nyomon követése.

A keretrendszer támogatja a vezetői döntéshozatalt.

5.3 Logikai védelmi intézkedések

A logikai védelem magában foglal minden szoftveres és rendszerszintű biztonsági megoldást, amely az információs rendszerek működésének, elérésének és használatának szabályozását szolgálja.

5.3.1 Üzemeltetési szabályok

A Szervezet célja, hogy informatikai rendszerei biztonságosan, megbízhatóan és zavartalanul működjenek. Az ehhez kapcsolódó üzemeltetési szabályok az IT infrastruktúra mindennapi működését szabályozzák.

Fő elvek:

- Rendszeres frissítések és hibajavítások alkalmazása,
- Mentési és helyreállítási eljárások dokumentálása és tesztelése,
- Változáskezelés minden módosítás esetén,
- Monitoring és teljesítményfigyelés,
- Jogosultságok és szolgáltatások rendszeres felülvizsgálata.

A szabályok célja az incidensek megelőzése, bekövetkezésük esetén gyors és hatékony kezelése. A részletes üzemeltetési szabályozás a függelékben található.

5.3.2 Fejlesztési irányelvek

A Szervezet az alkalmazásfejlesztéseket információbiztonsági elvek mentén, a „security by design" megközelítéssel végzi. Cél, hogy már a tervezési szakaszban megelőzhetők legyenek a biztonsági kockázatok.

A fejlesztési biztonsági alapelvek:

- Fejlesztési és tesztkörnyezetek elkülönítése az éles rendszerektől;
- Verziókezelés és forráskód-naplózás alkalmazása;
- Kódellenőrzés, biztonsági tesztek és auditok végzése;
- Adatvédelmi megfelelőség biztosítása (pl. DPIA, adatminimalizálás);
- Dokumentáció és visszavonási terv minden kiadáshoz.

A szabályozás a fejlesztők, tesztelők és üzemeltetők együttműködését segíti. A részletes fejlesztési követelmények a függelékben találhatók.

5.3.3 Hozzáférés-menedzsment

A hozzáférés-menedzsment célja annak biztosítása, hogy csak az arra jogosult személyek férhessenek hozzá az információkhoz és rendszerekhez és csak a szükséges mértékben.

A hozzáférés-szabályozás fő elemei:

- Szerepkör-alapú jogosultságkezelés (RBAC) alkalmazása;
- Belépési és kilépési folyamatok dokumentált kezelése;
- Jogosultságok rendszeres felülvizsgálata és visszavonása;
- Admin jogosultságok szétválasztása és naplózása;
- Hozzáférések nyilvántartása, indokolása és jóváhagyása.

A jogosultságkezelés belső munkatársakra, partnerekre és rendszerek közti kapcsolatokra is kiterjed. A részletek a Szabályzat függelékében szerepelnek.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

5.3.4 Azonosítás és hitelesítés

A Szervezet minden informatikai rendszerében biztosítania kell a felhasználók egyértelmű azonosítását és hitelesítését, az illetéktelen hozzáférések kizárása érdekében. Az azonosítási és hitelesítési eljárások célja, hogy minden felhasználó csak a számára kijelölt adatokhoz és funkciókhoz férhessen hozzá.

Az alkalmazott védelmi mechanizmusok elvei:

- Egyedi, személyhez kötött felhasználói fiókok kötelező használata;
- Erős hitelesítési módszerek alkalmazása (többtényezős azonosítás – MFA);
- Automatikus zárolás, jelszavak lejárata és komplexitási követelmények előírása;
- Rendszerek közötti szerepkör-alapú jogosultságkezelés integrálása;
- A rendszerekhez való hozzáférés minden esetben naplózásra kerül.

A szabályozás kiterjed a belső felhasználókra, külső partnerekre, szolgáltatókra és alkalmazások közötti technikai hitelesítésekre. A részletes technikai és szervezési előírásokat a szabályzat függeléke tartalmazza.

5.3.5 Naplózási elvárások

A Szervezet köteles biztosítani, hogy minden informatikai rendszer működése során keletkező naplóállományok megfelelően kezelve, védve és ellenőrizve legyenek. A naplózási követelmények célja az események nyomon követhetősége, az incidensek visszakereshetősége, valamint a jogosulatlan tevékenységek észlelhetősége.

A naplózási és naplókezelési elvek:

- A rendszerhasználat, belépések, jogosultságmódosítások, adatelérések és rendszerhibák naplózása kötelező;
- A naplóknak tartalmazniuk kell legalább a következőket: felhasználó azonosító, esemény típusa, időpont, érintett rendszer vagy adat, valamint a végrehajtott művelet leírása;
- A naplófájlokat védett módon, manipulálás ellen biztosított tárolással kell kezelni (pl. írásvédelem, titkosítás, időbélyeg alkalmazása);
- A naplóadatokhoz való hozzáférés korlátozott és naplózott, kizárólag adminisztratív vagy biztonsági célból engedélyezett;
- A naplók megőrzési idejét információbiztonsági és jogszabályi előírások szerint kell meghatározni, és azok rendszeres automatikus archiválását biztosítani kell;
- A naplóelemzés-, és monitorozás folyamatait dokumentálni kell, különös figyelemmel az incidensgyanús események azonosítására.
- A naplózás a biztonságtudatos rendszerüzemeltetés és hatósági megfelelés alapvető eszköze. A részletes naplózási struktúrákat, formátumokat és elemzési eljárásokat a szabályzat függeléke tartalmazza.

5.3.6 Adathordozókra vonatkozó követelmények

A Szervezet elkötelezett az információk teljes életcikluson át tartó védelme mellett, beleértve a fizikai és digitális adathordozókat is. Az adathordozók biztonságos kezelése különösen fontos az adatszivárgások, illetéktelen hozzáférések és adatvesztések megelőzése érdekében.

A keretrendszer fő elvei:

- Adathordozók nyilvántartása és azonosíthatóság biztosítása;
- Hozzáférés korlátozása és jogosultság alapú használat;
- Titkosítási eljárások alkalmazása minden hordozható, külső vagy eltávolítható eszközön (pl. USB, külső HDD, mobil eszközök);
- Szállítás és tárolás szabályozása, különös tekintettel a fizikai védelemre és csomagolásra;
- Adathordozók selejtezése és megsemmisítése helyreállíthatatlan módon, tanúsított eszközökkel vagy szolgáltatóval.

A szabályozás kiterjed a belső és külső (pl. felhő, szolgáltatói) adattárolásra, és az alkalmazandó adatvédelmi és biztonsági előírások betartását írja elő minden életciklus-fázisban. A részletes előírásokat, eljárásokat és eszközökre vonatkozó szabályokat a szabályzat függeléke tartalmazza.

5.3.7 Rendszer és kommunikációvédelem

A Szervezet célja, hogy minden informatikai rendszer és azok közötti kommunikáció védelmét biztosítsa a jogosulatlan hozzáférés, lehallgatás, manipuláció vagy adatvesztés ellen. A védelemnek ki kell terjednie a hálózati kapcsolatokra, alkalmazásrétegű adatcserére, valamint a rendszerösszetevők közötti interfészekre is.

A rendszer- és kommunikációvédelmi követelmények fő elvei:

- Az adatátvitel során titkosítás alkalmazása minden olyan csatornán, ahol érzékeny vagy személyes adat halad át (pl. TLS, VPN);
- Tűzfalak, hálózati szegmentáció és IDS/IPS rendszerek használata a belső és külső forgalom szabályozására;
- A kommunikációs protokollok és interfészek engedélyezési listák alapján történő szabályozása;
- Portok és szolgáltatások rendszeres felülvizsgálata és korlátozása a szükséges minimumra;
- Mobil és távoli elérés védelme (pl. VPN, multifaktoros hitelesítés, eszközregisztráció).

A Szervezet minden hálózati és rendszerkommunikációs tevékenységet naplóz és monitoroz, külön figyelemmel a jogosulatlan forgalmi mintákra. A részletes védelmi intézkedések a szabályzat függelékében találhatók.

5.3.8 Rendszer és információsértetlenség

A Szervezet köteles biztosítani, hogy minden informatikai rendszer által kezelt adat teljes, pontos, hiteles és jogos eredetű legyen. A rendszer-, és adatérintetlenség (integritás) védelme kiterjed az adatok előállítására, tárolására, továbbítására és feldolgozására.

Az információsértetlenség biztosításának alapvető intézkedései:

Fővárosi Törvényszék Cégbíróság Cégjegyzékszám: 01 09 203215

- Hash-alapú ellenőrzések és digitális aláírások alkalmazása az adatok változatlanságának igazolására;
- Integritás-ellenőrző kontrollok beépítése a fejlesztett rendszerekbe (pl. adatbevitel-ellenőrzés, duplikációk kiszűrése);
- Naplóállományok védelme és a kompromittálódás lehetőségének kizárása;
- Rendszerkonfigurációk és szoftverkiadások verziókövetése;
- Automatizált ellenőrzések és értesítések indítása integritás-sértés gyanúja esetén.

Az integritási védelem célja, hogy a rendszerhasználók, partnerek és hatóságok számára is igazolható legyen az adatok és működési folyamatok hitelessége. A részletes szabályozást és ellenőrzési eljárásokat a szabályzat függeléke tartalmazza.

6. Biztonsági eseménykezelés

A Szervezet célja, hogy minden információbiztonsági eseményre és incidensre gyorsan, szabályozott módon és megfelelően dokumentált eljárásokkal reagáljon. Az eseménykezelés célja a károk minimalizálása, a rendszer helyreállítása és a tanulságok visszacsatolása.

A biztonsági eseménykezelés fő elemei:

- Események osztályozása és súlyosság szerinti kategorizálása;
- Bejelentési és eszkalációs folyamatok meghatározása;
- Incidensnapló vezetése, utólagos elemzés és tanulságdokumentálás;
- Helyreállítási lépések és érintett rendszerek nyomon követése;
- Jogszabályi bejelentési kötelezettségek (pl. NIS2, GDPR) teljesítése.

Az eseménykezelési folyamatban a felhasználók, rendszergazdák és az információbiztonsági szervezet közösen vesznek részt. A részletes eljárásrend a szabályzat függelékében található.

6.1 Fizikai biztonsági elvárások

Az információs rendszerek és adathordozók védelme fizikai szinten is elengedhetetlen a bizalmas információk integritásának és rendelkezésre állásának megőrzése érdekében. A fizikai biztonság célja, hogy csak jogosult személyek férhessenek hozzá kritikus eszközökhöz és helyiségekhez.

A fizikai védelem kulcselemei:

- Beléptető rendszerek és zárt hozzáférésű helyiségek alkalmazása;
- Felügyeleti és riasztórendszerek (pl. kamerás megfigyelés, belső érzékelők);
- Szervertermek, adatarchívumok és éles rendszerek fokozott védelme;
- Vendégek és külső partnerek belépésének szabályozása;
- Fizikai eszközmozgás nyomon követése, ki- és bejelentés.

A szabályozás célja a fizikai behatolás, lopás, illetéktelen megfigyelés és rongálás megelőzése. A részletes intézkedések a Szabályzat függelékében találhatók.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

6.2 Humánbiztonsági, személyi biztonsági elvárások

A Szervezet számára kiemelten fontos, hogy munkavállalói és harmadik felei tudatosan és felelősségteljesen viszonyuljanak az információbiztonsághoz. A humánbiztonsági intézkedések célja a biztonsági kockázatok csökkentése az emberi tényezők figyelembevételével.

A személyi biztonság fő elemei:

- Előzetes ellenőrzés a foglalkoztatás vagy megbízás megkezdése előtt (referenciák, nyilatkozatok);
- Titoktartási nyilatkozatok aláíratása minden érintettel;
- Belépési és kilépési folyamatok kezelése, jogosultságok visszavonása;
- Kötelező IT-biztonsági és adatvédelmi oktatások lebonyolítása;
- Szankcionálási rend kialakítása információbiztonsági szabályszegések esetére.

A humánbiztonság az információbiztonsági kultúra alapja. A kapcsolódó eljárások és követelmények a szabályzat függelékében találhatók.

6.3 Beszerzés

A Szervezet az informatikai rendszerek, szolgáltatások és eszközök beszerzése során is érvényesíti információbiztonsági követelményeit. A cél, hogy már a beszerzés megkezdése előtt meghatározásra kerüljenek a szükséges biztonsági szintek.

A beszerzésekhez kapcsolódó információbiztonsági elvek:

- A beszerzendő eszköz vagy szolgáltatás kockázati szintjének előzetes értékelése;
- Biztonsági és adatvédelmi elvárások rögzítése – a hatályos jogszabályok alapján – a műszaki specifikációban és a szerződésben vagy annak mellékleteként;
- Szállítók és szolgáltatók kötelezése titoktartásra és megfelelőségre;
- Átvételkor technikai és dokumentációs megfelelőség ellenőrzése;
- A beszerzések kapcsolódása a beszállítói minősítési folyamatokhoz.

A beszerzési biztonsági szempontokat minden projektben kötelező figyelembe venni. A részletes előírásokat a szabályzat függeléke tartalmazza.

6.3.1 Beszállítói minősítés

A külső beszállítók, partnerek és szolgáltatók biztonsági kockázatot jelenthetnek a Szervezet információs rendszereire. A beszállítói minősítés célja e kockázatok előzetes és rendszeres értékelése.

A beszállítói minősítés fő elemei:

- Kockázatalapú előminősítés új beszállítók szerződéskötése előtt;
- Biztonsági követelmények beépítése a szerződésekbe (pl. titoktartás, auditálhatóság);
- Szállítók értékelése teljesítmény, incidensmúlt és megfelelőség alapján;
- Rendszeres újraminősítés, különösen hosszú távú vagy kritikus beszállítók esetén;
- A minősítések eredményeinek dokumentálása és utókövetése.

A beszállítók megfelelősége az ellátási lánc biztonságának alapfeltétele. A részletes értékelési szempontokat és eljárásokat a Szabályzat függeléke tartalmazza.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

6.4 Információosztályozás

A Szervezet az információs rendszereiben feldolgozott, továbbított és tárolt adatok védelmét a kockázatokkal arányosan biztosítja, ezért az adatokat biztonsági kategóriákba sorolja. Az adatok osztályozását az Adatgazda végzi, és rendszeres időközönként – legalább évente – felülvizsgálja, szükség esetén pedig soron kívül is aktualizálja.

Elektronikus információs rendszerek esetén az azonos informatikai környezetben (pl. közös adatbázisban vagy könyvtárban) tárolt adatok egységes biztonsági kategóriába kerülnek besorolásra. A besorolás során a legérzékenyebb adat védelmi szintje határozza meg az egész adathalmaz kategóriáját.

Az adatosztályozási rendszer kialakítása, karbantartása, valamint a vonatkozó jogszabályi követelmények érvényesítése az IBF feladata.

Az Adatgazdák felelősek annak biztosításáért, hogy minden olyan személy, aki az adott információhoz hozzáfér, tisztában legyen annak biztonsági besorolásával és az ebből fakadó kötelezettségekkel.

Az osztályozás megfelelőségéért – ideértve a jogszabályi és kockázati szempontokat, valamint az adatok teljességét és naprakészségét – szintén az Adatgazdák felelnek. Soron kívüli felülvizsgálatot kell végezni:

- ha új informatikai rendszer kerül bevezetésre;
- ha jogszabályi változás érinti az adatbiztonságot;
- vagy ha a Szervezet működésében, illetve az általa kezelt adatok körében jelentős változás történik.

7. Információbiztonsági vizsgálatok

7.1 Megfelelés a biztonsági irányelveknek és szabványoknak

A Szervezet célja, hogy minden információbiztonsági tevékenysége megfeleljen a belső biztonsági irányelveknek, valamint a nemzetközi szabványoknak és legjobb gyakorlatoknak, különös tekintettel az ISO 27001-re, valamint a NIST 800-53 Rev. 5-re. A vezetők feladata továbbá a területükön alkalmazott információbiztonsági követelmények, eljárások működésének betartatása és ellenőrzése.
Az IT üzemeltetésért felelős vezető, valamint az IBF feladata, hogy az általa meghatározott gyakorisággal (legalább évente) egy belső audit keretében ellenőrizze az információbiztonsági szabályoknak való megfelelés állapotát és erről jelentést készítsen, amelyet megküld az ügyvezető részére.
A felülvizsgálatok során feltárt eltérésekre, a kockázatokkal arányos helyesbítő és megelőző intézkedéseket szükséges megfogalmazni, amelyekhez határidő rendelése minden esetben kötelező. Az intézkedések eredményességéről az intézkedések felelősei legalább évente beszámolnak.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

7.2 Műszaki megfelelés vizsgálata

A technikai megfelelőségi ellenőrzés, azaz a műszaki megfelelés vizsgálat magában foglalja a jelen dokumentum „Logikai biztonsági szabályzat", valamint „Fizikai és környezeti biztonság, üzemeltetési szabályzat" függelékeiben rögzített feltételek szerinti működést.
Az ellenőrzés során szükség esetén az adott területen dolgozó speciális helyismerettel rendelkező munkatárs bevonható. Az ellenőrzés végezhető manuálisan (ha szükséges, szoftver eszközt igénybe véve) vagy automatikusan megfelelő szoftvercsomaggal. Ennek módjáról előzetesen az IT üzemeltetésért felelős vezető, valamint az IBF tájékoztatása szükséges.
A megfelelőségi vizsgálat része lehet a sérülékenységi (behatolási) vizsgálat is, amelyhez az IT üzemeltetésért felelős vezető, valamint az IBF előzetes jóváhagyása szükséges. A Szervezet valamennyi informatikai rendszerében technikai ellenőrzést csak az IT üzemeltetésért felelős vezető, valamint az IBF által felhatalmazott személy vagy külsős szervezet végezhet, továbbá kiszervezett tevékenység esetén, annak érzékenysége okán, kizárólag az IT üzemeltetésért felelős vezető felügyelete alatt végezhető.
Az ellenőrzési célkitűzések ismeretében meg kell jelölni az ellenőrzés eszközeit és annak határait. A vizsgálat eredményéről jelentés készül, abban a javasolt intézkedések és azok priorizálásának megjelölésével, majd ezekről tájékoztatják az ügyvezetőt.

7.3 Kockázatmenedzsment keretrendszer

A kockázatmenedzsment keretrendszer olyan strukturált, ugyanakkor rugalmas megközelítés és szervezeti folyamatok összessége, amely integrálja a kiberbiztonsággal kapcsolatos kockázatkezelési tevékenységeket a rendszerfejlesztési életciklusban a kockázatokkal arányos védelmi intézkedések azonosításán, bevezetésén, értékelésén, működtetésén és nyomon követésén keresztül az új és már használatban lévő rendszerek fenyegetettségeinek folyamatos felderítése, és kockázatainak hatékony kezelése érdekében.

A kockázatmenedzsment keretrendszer része a kockázatelemzés és kockázatkezelés. A Szervezet a keretrendszer alapján először kockázatelemzés segítségével azonosítja a kockázatokat, majd azt követően kockázatkezelést valósít meg.

A Szervezet a fenyegetéseket káros hatásainak és azok bekövetkezésének valószínűsége alapján azonosítja az abból eredő kockázatokat egy **négy fokozatú skálán**:

- alacsony;
- közepes;
- magas;
- kritikus;

mint kockázati kategória.
A Szervezet dokumentálja és az ügyvezető számára kommunikálja a kockázatelemzés eredményét a kockázatkezelési válaszlépések támogatása érdekében, valamint biztosítja a kockázatelemzési folyamat során keletkezett információk megosztását az arra jogosultakkal.

A Szervezet az azonosított kockázatokról eldönti és dokumentumban rögzíti, hogy az egyes kockázatok kezelése érdekében az alábbiak közül egyenként mely intézkedést alkalmazza:

- kockázat elkerülése,
- kockázat csökkentése védelmi intézkedések kialakításával és működtetésével,

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- kockázat áthárítása vagy megosztása harmadik felekkel,
- kockázat felvállalása.

7.4 Helyesbítő intézkedések rendszere

Annak érdekében, hogy az információbiztonság folyamatosan, minden területen a kívánt biztonsági szinten működjön, az alábbi irányelvek érvényesítése szükséges a napi munka során:

- A biztonsági eseményeket és incidenseket azok bekövetkezésekor vagy észlelésekor a lehető legrövidebb időn belül jelenteni, majd dokumentálni szükséges a jelen IBSZ-nek megfelelően:
- A rögzített incidensekből statisztikai adatként ki lehessen nyerni az egyes fenyegetettségek bekövetkezési valószínűségét.
- A rögzített incidenseket később fel lehessen használni oktatási anyagként az információbiztonsági tudatosság növelése érdekében.
- A felhasználói incidensekből statisztikailag ki lehessen nyerni az elkövetési magatartást.
- Az IT üzemeltetési incidensek esetén statisztikailag ki lehessen nyerni az egyes szolgáltatásokra vonatkozó incidensek számosságát.
- A biztonsági eseményekből és incidensekből levont tapasztalatokat be kell építeni a kockázatmenedzsment folyamataiba, ezzel elősegítve egy kiberbiztonsági jó gyakorlat kialakulását, valamint a védelmi rendszer tervezése és szervezése érdekében.
- Amennyiben szükséges, a meglévő kontrollok konszolidációját végre kell hajtani.
- A védelmi intézkedések átalakítását indokolttá tehetik a belső ellenőrzések eredményei, felügyeleti szervek, külső szakértők által lefolytatott ellenőrzések, illetve a jogszabályoknak való megfelelés.
- A védelmi intézkedések fejlesztése során az alábbi követelményeket kell betartani:
    - Törekedni kell a nemzetközileg elfogadott szabványokon, ajánlásokon, jó gyakorlatokon nyugvó védelmi intézkedések alkalmazására.
    - Figyelembe kell venni a tervezett védelmi intézkedés várható egyszeri és folyamatos költségeit, igazolva annak kockázatarányosságát.
    - Figyelembe kell venni a tervezett biztonsági intézkedésnek Szervezetünk
    - működésére gyakorolt hatását, szükség esetén egyeztetni kell a felhasználói szervezeti egységek vezetőivel.
    - Az információbiztonsági védelmi intézkedések bevezetését az IT üzemeltetésért felelős vezető, valamint az IBF javaslatait és véleményét figyelembe véve, a Szervezet ügyvezetője hagyja jóvá.

8. Függelékek

1. számú függelék: A Szervezet rendszereinek biztonsági osztályba sorolása
2. számú függelék: A Szervezet információbiztonsági gyakorlati intézkedései
3. számú függelék: Fogalomtár

Főv.Törv.szék Cégb.Cg.: 01 09 203215

9. Záró rendelkezések

A függelékek vagy mellékletek módosítására az IBF előterjesztése alapján az ügyvezető jogosult abban az esetben, ha a módosítani kívánt függelék vagy melléklet nem generálja jelen Szabályzat törzsszövegének módosítását. A módosítandó mellékletet vagy függeléket az IBF felterjeszti jóváhagyásra az ügyvezető elé. A módosított függelék vagy melléklet az ügyvezető jóváhagyásának, illetőleg a Szabályzatok SharePoint linken való közzétételének napján lép hatályba, mely dátummal a korábbi melléklet vagy függelék hatályát veszti, és ettől a naptól kezdve jelen Szabályzat érvényes és hatályos függelékévé vagy mellékletévé válik.

Fővárosi Törvényszék Cégbíróság Cégjegyzékszám: 01 09 203215