2. függelék: A Szervezet információbiztonsági gyakorlati intézkedései

1 Beépített és alapértelmezett adatvédelem

A **KKM Magyar Diplomáciai Akadémia Kft.** mint adatgazda (a továbbiakban: Szervezet) a technológiai képesség és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a munkavállalók és felhasználók jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a vonatkozó jogszabályokban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

A Szervezet megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a kezelt személyes és üzleti adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt biztosítják, hogy a személyes és üzleti adatok kompromittálódásának kockázati szintjét minimálisan tartsa.

2 Specifikus intézkedések és előírások

2.1 Adatbiztonságra törekvő magatartás a Szervezet székhelyén és telephelyein

- Személyes és üzleti adatokat tartalmazó dokumentumok, iratok nem hagyhatók felügyelet nélkül az asztalon;
- Munkavégzés során (lehetőleg) csak azok az iratok, illetve dokumentumok lehetnek elöl az asztalon, amelyek az adott munka végzéséhez akkor szükségesek;
- Munkavégzés után minden személyes adatot tartalmazó dokumentumot, iratot és elektronikus adathordozót el kell tenni az asztalokról és zárható irodabútorban, illetve biztonsági tárolóban kell tárolni;
- Megbeszélések után a tárgyalóból minden dokumentumot, különösen a személyes és üzleti adatokat tartalmazó iratokat, papírokat, jegyzeteket el kell távolítani. (Ide beleértendők a használt flip-chart papírok eltávolítása, táblák letörlése, stb.);
- Személyes és üzleti adatokat tartalmazó dokumentumok, iratok másolásakor sem eredeti példány, sem másolat nem maradhat a fénymásoló készülékben;
- Személyes és üzleti adatokat tartalmazó dokumentumok, iratok csak olyan felhasználóknak adhatók át, akik munkaköri feladatuknál fogva vagy jogszabályi előírásnak megfelelve jogosultak azoknak az információnak a megismerésére vagy használatára, és az átadó személy erről meggyőződött;
- Elektronikus átviteli út (pl. telefon, e-mail) esetén a védendő információkat ajánlott védett kommunikációs csatornán továbbítani;
- Amennyiben a személyes és üzleti adatokat tartalmazó dokumentumok, iratok őrzésére, tárolása már nincs szükség, azokat iratmegsemmisítővel azonnal, vagy biztonságos tárolás után kell megsemmisíteni;

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- A személyes és üzleti adatokat tartalmazó kézi feljegyzéseket, munkapéldányokat, másolati példányokat ugyanolyan biztonsági előírások alapján kell kezelni, mint az eredeti példányokat.

2.2 Az asztali számítógépek biztonságos használatának feltételei, üres asztal - üres képernyő szabály

- A munkaállomáshoz, valamint az elektronikus formában tárolt adatokhoz, információkhoz való illetéktelen hozzáférés megakadályozása és azok jogosulatlan eltulajdonításának elkerülése érdekében minden dolgozónak ismernie és alkalmaznia kell a jelen bekezdésben leírtakat;
- a felhasználó a számítógépbe/hálózati szolgáltatások eléréséhez személyre szóló azonosítót és jelszót kap, mely a belépéshez szükséges nem nyilvános információkat tartalmaz;
- az azonosító és a megfelelő erősségű jelszó használatával a felhasználó védelemmel rendelkezik a nevében történő visszaélések ellen, ezért a személyre szóló azonosítót és jelszót szigorúan védeni kell és a kezdeti jelszót első bejelentkezéskor meg kell változtatni;
- a felhasználó semmilyen infokommunikációs eszközt nem csatlakoztathat és telepíthet a Szervezet informatikai rendszerébe, illetve azok elhelyezését, telepítési módját nem változtathatja meg. Semmilyen szoftvert nem telepíthet, nem törölhet és nem módosíthat;
- az internet használata kizárólag a Szervezet tevékenységéhez köthető feladatokkal kapcsolatban engedélyezett. Tilos fájlletöltő szolgáltatások használata. Tilos a munkaköri leírásban foglalt feladatkörrel nem azonosítható tartalom letöltése és tárolása;
- a felhasználónak infokommunikációs eszköz, illetve szoftver telepítési igényét a Szervezet IT üzemeltetésért felelős vezető engedélyezi;
- a monitorok elhelyezésekor törekedni kell az azokra való minél kisebb rálátás biztosítására, hogy a képernyők tartalma ne legyen olvasható az alkalmilag arra haladó személyek számára és semmiképpen se legyen látható az épületen kívülről (árnyékoló függöny szükség esetén alkalmazható);
- a felhasználó a munkaállomását zárolni köteles (a Ctrl +Alt +Del billentyűk, majd Zárolás), ha ideiglenesen felfüggeszti azon a munkavégzést;
- az automatikus zárolás maximum 5 perc várakozást követően zárolja a munkaállomást;
- a munkafázis végeztével ki kell jelentkezni az alkalmazásokból, majd zárolni – az IT üzemeltetésért felelős vezető felhívására leállítani – a munkaállomást;
- vendéget irodában felügyelet nélkül hagyni tilos;
- kizárólag a munkavégzéshez szükséges adathordozók használata engedélyezett.

2.3 A hordozható munkaállomás (laptopok) biztonságos használatának feltételei

- A hordozható munkaállomás extrém hőmérséklet, mágneses tér, magas páratartalom vagy erős füstképződés hatásának kitenni TILOS;

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- A munkaállomásokat bekapcsolt állapotban szállítani nem szabad (ez nem vonatkozik az utazás közbeni munkavégzésre),

2.4 Adatbiztonsági szabályok:

- Személyes adatok csak titkosítva tárolhatók a hordozható munkaállomáson;
- A hordozható munkaállomáson lokálisan tárolt adatok rendszeres mentéséről a felhasználó maga köteles gondoskodni. A mentéseket az adathordozón titkosítva kell tárolni és az adathordozókat biztonságosan szükséges elzárni;
- A külső munkahelyen történő feladat elvégzése után a hordozható munkaállomáson keletkezett vagy tárolt adatokat a kijelölt a hálózati fájlszerverekre kell menteni és ezt követően a hordozható munkaállomásról le kell őket törölni.

2.5 Jogosulatlanok általi információhoz való hozzáférések megakadályozása

- Bel- és külföldi kiküldetésre (munkahelyi és otthoni használaton kívül) utazó kollégák hordozható munkaállomásainak a titkosítását el kell végezni, ennek végrehajtásáért z az IT üzemeltetésért felelős vezető a felelős;
- A hordozható munkaállomást csak annak a rendszergazda által beállított felhasználója, a saját bejelentkezésével és jelszavával, a munkavégzés céljára használhatja;
- TILOS a hordozható munkaállomást más célra használni, illetve másoknak (pl. családtagoknak, barátoknak, ügyfeleknek) használatra átengedni;
- Nyilvános helyeken történő használatnál ügyelni kell arra, hogy illetéktelenek ne olvashassák el a képernyő tartalmát;
- A hordozható munkaállomás rövid idejű elhagyásakor is azonnal zárolni kell az eszközt, ezzel megakadályozva az esetleges kompromittálódást;
- A rendszergazda által beállított biztonsági beállítások megváltoztatása TILOS.

2.6 Hordozható munkaállomások fokozott vírusveszélye kockázatainak csökkentése

- A rendszergazda által telepített központi vírusvédelmi rendszer használata kötelező;
- Az idegen külső adathordozók (pl.: optikai adathordozók, külső merevlemezek, memória alapú adathordozók, stb.) vírusmentességét felhasználásuk előtt kötelező megvizsgálni;
- A hordozható munkaállomás külső hálózatra kapcsolódását (pl.: szállodákban, rendezvényeken, beszállítóknál, otthon, stb.) követő használata előtt soron kívüli, teljes gépre vonatkozó vírusellenőrzést kötelező végrehajtani.

2.7 Intézkedések, ha a hordozható számítógépet már eltulajdonították vagy elveszítették

- Az eltulajdonítás, elveszítés tényét a lehető leggyorsabban jelenteni kell az IT üzemeltetésért felelős vezetőnek és az IBF-nek;
- Tájékoztatni kell a közvetlen felettes vezetőt arról (előzetesen szóban, majd ahogyan lehetőség adódik erre, írásban is megerősítve), hogy az eszköz tartalmaz-e bármilyen személyes vagy üzleti adatot;
- Ha kiküldetés során a munkaállomást a szállodai szobából vagy a szálloda ingatlanján álló gépjárműből lopták el, értesíteni kell a szálloda vezetését;

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- Rendőrségi jegyzőkönyvet kell felvetetni eltulajdonítás esetén;
- Hordozható munkaállomás eltulajdonítása esetén az személyes és üzleti adatot is tartalmazott, azt adatvédelmi incidensnek kell tekinteni és az annak megfelelő eljárást kell kezdeményezni.

2.8 Adathordozók biztonságos használata

- Munkavégzés céljaira csak a rendszergazda által átadott, a Szervezet tulajdonában lévő adathordozó használható;
- Az adathordozókat azok feldolgozása és tárolása alatt úgy kell kezelni, hogy biztosítva legyenek elvesztés, megsemmisülés, megsérülés és elcserélés, valamint jogosulatlan hozzáférés ellen;
- Gondosan és elzárva kell a használaton kívüli adathordozókat tárolni.

2.9 A Szervezet informatikai hálózatának biztonságos használata

- A hálózaton csak a rendszergazda által biztosított és üzemeltetett informatikai eszközök üzemeltethetők az eredeti telepítési környezet megtartása mellett;
- A hálózatba a felhasználók csak a saját belépési azonosítójukat használva jelentkezhetnek be;
- TILOS a saját azonosító és jelszó megosztása;
- A rendszergazda által biztosított eszközöket a szervezeti hálózatra csatlakoztatás során egy másik, lokális (vezetékes vagy vezeték nélküli) hálózatra kötve megosztani SZIGORÚAN TILOS!
- Az informatikai rendszer használata otthonról csak korlátozottan, ügyvezetői engedéllyel, biztonságos VPN csatornán keresztüli bejelentkezéssel engedélyezhető;
- Az informatika rendszerek távoli eléréssel történő használata során a rendszergazda által beállított biztonsági eljárások, eszközök és beállítások (pl. titkosított csatorna, VPN, stb.) használata kötelező.

2.10 Bejelentkezési adatok védelme

1. Egy adott jelszót csak egy platformon szabad alkalmazni;
2. A jelszót nem szabad képernyőre, más nyilvános helyre, online tárhelyre elmenteni, illetve a fájlszerverre rögzíteni;
3. Amennyiben egy munkavállalónak megszűnik a munkaviszonya, akkor a felhasználói fiókját zárolni kell;
4. A jelszó legalább 14 karakter hosszúságú, tartalmaz legalább 1 darab számot, illetve kis és nagy betűket;
5. Online jelszógenerátort TILOS szabad használni;
6. A jelszavak élettartama maximum 90nap;
7. Jelszavakat nem szabad lementeni;
8. Az elektronikus információs rendszereket kétfaktoros belépési kötelezettséggel kell védeni.

Főv.Törv.szék Cégb.Cg.: 01 09 203215

2.11 Fájlszerver (NAS) védelme

1. A fájlszerveren található adatokat titkosított partíciókon kell elhelyezni;
2. Minden felhasználó egyedi azonosítóval és jelszóval csatlakozhat a fájlszerverre;
3. A NAS telepítési helyére csak az arra feljogosított munkavállalók léphetnek be önállóan, más személyek pedig csak kísérettel;
4. A NAS telepítési helyét zárni kell és a belépést rögzíteni szükséges.

2.12 Belső meghajtók, fájlmegosztó rendszerek használata

- A belső hálózaton adattartalmat kizárólag az ügyvezető engedélyével a rendszergazda törölhet;
- A munkatársak kizárólag a saját feladatuk ellátásához szükséges könyvtárakat használhatják;
- A megosztott tárhelyen magánjellegű információkat, fényképeket SZIGORÚAN TILOS tárolni;
- Az otthoni munkavégzés során különös figyelmet kell fordítani arra, hogy a Szervezet adatait senki más ne tekinthesse meg.

2.13 A munkahelyi elektronikus levelezés biztonsági előírásai

- A Szervezet az elektronikus levelezési szolgáltatást (e-mailt) csak és kizárólag munkavégzés céljából, a munkaköri feladatok hatékonyabb ellátásának érdekében biztosítja. A szolgáltatást magán célra és egyéb, a munkavégzéssel nem összefüggő célokra használni TILOS;
- Az elektronikus levelezés használati engedélye személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe;
- A felhasználó saját azonosítójának és jelszavának átadása más felhasználók részére TILOS;
- Helyettesítés és távollét esetén a levelezés továbbításának szabálya beállítható;
- TILOS a munkahelyi e-mail címmel magánjellegű regisztrációt elvégezni (pl.: közösségi oldalak);
- Az ingyenes levelezőrendszerek (pl.: gmail.com, freemail.hu) munkahelyi célú használata TILOS;
- Az elektronikus levelek és csatolmányok védelmi előírásai megegyeznek az egyéb dokumentumok védelmének előírásaival.

2.14 Az e-mailek küldésére vonatkozó irányelvek

- A feladó, mint felhasználó felelős az e-mail tartalmáért;
- TILOS más nevében e-mailt küldeni, kivéve a meghatalmazottak (pl.: titkársági feladatok) esetében;
- A leveleket mindig célzottan kell kiküldeni, sosem szükségtelenül nagy címzetti kör számára;
- Nagy adatmennyiségeket lehetőleg csak tömörített és védett formátumú csatolmányként szabad küldeni;

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- Személyes és üzleti adatokat tartalmazó dokumentumok e-mail-en keresztül csak titkosított formában küldhetők;
- Zavaró, megtévesztő és lánclevelek levelek küldése, jogtalan megrendelések elindítása TILOS és eljárást vonhat maga után.

2.15 Az e-mailek fogadására vonatkozó irányelvek

- A címzett felelős az e-mail tovább-feldolgozásáért és továbbításáért;
- Védendő információk (pl. különlegesen személyes adatok) továbbítását kérő elektronikus levelek esetében mindig meg kell győződni az információkérés hitelességéről;
- Ismeretlen helyről származó e-mail érkezése esetén (pl. a feladó ismeretlen vagy a feladó e-mail gyanús) megnyitás nélkül értesíteni kell a rendszergazdát;
- Külső vagy belső e-mail címről érkező, félrevezető tartalmú e-mail-ek esetén azonnal értesíteni kell a rendszergazdát;
- A beérkező e-mail mellékleteket megnyitás előtt víruskeresővel kell átvizsgálni.

2.16 Mobiltelefonok, mobileszközök védelme

- Védelem nélküli kommunikációs csatornával rendelkező WIFI-hez csatlakozni tilos;
- Az eszközöket PIN kóddal vagy jelszóval kell védeni;
- Az eszközök zárolt képernyőjéről a tartalmakat el kell rejteni;
- Amennyiben az eszköz lehetővé teszi, a szenzitív adatokat tartalmazó elektronikus információs rendszereket PIN kóddal vagy jelszóval kell védeni.

3 Vírusvédelemhez kapcsolódó szabályok

3.1 A központi vírusvédelmi szoftver alkalmazására vonatkozó szabályok

- A rendszergazda által telepített vírusvédelem nélkül sem hálózati, sem önálló munkaállomás nem használható;
- A felhasználó nem akadályozhatja a vírusvédelmi program és részeinek folyamatos működését;
- A felhasználónak kötelessége jelenteni a rendszergazda részére, ha észleli, hogy a gépén a vírusvédelmi szoftver nem működése hibát jelez;
- A hordozható munkaállomások esetében a vírusadatbázis sikeres rendszeres frissítése a felhasználó kötelessége;
- A számítógépen idegen adathordozót csak vírusvizsgálat után lehet használatba venni;
- A dokumentumok esetében kerülni kell a makrók és aktív tartalmak megnyitását, külső forrásból érkező dokumentum esetében pedig tilos engedélyezni a makrókat.

3.2 Teendők vírusfertőzés gyanúja vagy biztos felismerése esetén

Ha a felhasználó gépén vírus jelenlétére utaló működési zavarok jelentkeznek – ezt a vírusvédelmi program akár jelzi, akár nem – a következő lépéseket kell tenni:

- Ne használja tovább vírusos vagy vírusgyanús rendszert!
- Ne változtassa meg a rendszer-állapotot!

Főv.Törv.szék Cégb.Cg.: 01 09 203215

- Azonnal jelentse az esetet a rendszergazdának!

4 A területek fizikai biztonsági követelményei

4.1 Fizikai biztonság védősávja

A védett helyiségeket, illetve területeket a fenyegetettség és kockázat mértéke szerint biztonsági zónákba kell besorolni. Héjszerű, többlépcsős fizikai védelmet kell kialakítani. A Szervezet székhelyének telephelyeinek területeit az alábbi kategóriák egyikébe kell besorolni:

a) belső terület;
b) védett terület;
c) érzékeny terület.

4.2 Belső terület

Belső területnek tekintendők a Szervezet bejárata utáni közös használatú helyiségei és folyosói és a tárgyalók, oktatótermek. A belső terekben infokommunikációs eszközök nem telepíthetők, a kivételek jóváhagyása az IT üzemeltetésért felelős vezető feladata.

4.3 Védett terület

Védett terület valamennyi irodahelyiség.

A védett területeket zárva kell tartani. A védett területek bejárati ajtajában a kulcsokat nem szabad a zárban hagyni, illetve, ha az ajtó nyitva van, a helyiséget nem szabad őrizetlenül hagyni.

4.4 Érzékeny terület

- Érzékeny terület a Szervezet informatikai rendszerének központi elemeit tároló helyisége;
- Látogatók belépése az érzékeny területre csak hivatali célból, ellenőrzötten és kísérővel történhet;
- Az érzékeny területeken a jogosulatlan belépések kizárása, a belépések engedélyezése, figyelése, dokumentálása és ellenőrzése érdekében belépési naplót kell vezetni;
- A belépési naplót az Ügyvezetői Titkárságon kell tárolni;
- Az érzékeny területek elérésére az IT üzemeltetésért felelős vezető, a rendszergazda és az ügyvezető jogosultak. Minden más személy részére az ügyvezető csak esetileg engedélyezheti a belépést.

4.5 Fizikai belépési engedélyek

- A Szervezet összeállítja azon személyek listáját, akik jogosultak a védett területre önállóan belépni. A listát az ügyvezető hagyja jóvá.
- Az IT üzemeltetésért felelős vezető 3 havonta felülvizsgálja a belépésre jogosult személyek listáját és eltávolítja a belépésre jogosult személyek listájáról azokat, akiknek a belépése már nem indokolt.

Főv.Törv.szék Cégb.Cg.: 01 09 203215