INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

A GANDHI GIMNÁZIUM, KOLLÉGIUM ÉS ALAPFOKÚ MŰVÉSZETI ISKOLA VALAMINT A GANDHI GIMNÁZIUM KÖZHASZNÚ NONPROFIT KORLÁTOLT FELELŐSSÉGŰ TÁRSASÁG (7629 PÉCS, DOBÓ ISTVÁN U. 93. VALAMINT 7629 PÉCS, KOMJÁT ALADÁR UTCA 5.)

részére

Pécs, 2019.05.10

Készítette:

GDPR Info Kft.

7632 Pécs Olga utca 13. 2.em/6.

E-mail: gilincsek.szabolcs@gdpr.info.hu

Webcím: https://www.gdpr.info.hu/

Tartalomjegyzék

1. BEVEZETÉS

1.1 Szabályzás Célja

A Szabályzás célja az GDPR rendelet alapján elvárható szabályozási célok és intézkedések, a Gandhi Gimnázium, Kollégium és Alapfokú Művészeti Iskola valamint a Gandhi Gimnázium Közhasznú Nonprofit Korlátolt Felelősségű Társaságnál (továbbiakban: Szervezet) történő megvalósulási módjának rögzítése.

Változás követés

Kiadás	Felülvizsgálat	Módosította	Kiadás Dátuma	Jóváhagyta
1.0			2019.05.10	Szommerné Kővári Viola

2. AZ INFORMÁCIÓBIZTONSÁG SZERVEZETE

2.1 Információbiztonsági Szerepek és felelősségek

Az információbiztonsággal kapcsolatos felelősség megoszlik a Szervezet vezetősége, az Informatika, valamint az egyes munkatársak között. A felelősség-megosztás elveit az alábbiakban tárgyaljuk.
A felső szintű felelősség az információbiztonság folyamatos biztosításáért, az információbiztonsággal kapcsolatos szabályozásokért, a Szervezeti információbiztonsági tudatosság megfelelő szintjének biztosításáért, az információbiztonsággal kapcsolatos Szervezeti célkitűzésekért, valamint az információbiztonsági intézkedések bevezetéséért az Informatikánál összpontosul.

Az információbiztonság koordinálásának felső szintű vezetője az Ügyvezető Igazgató.

2.1.1 Feladatkörök szétválasztása

A Szervezetnél a következő Információbiztonsági felelősségi körök definiáltak:

- Ügyvezető Igazgató/Elnök
- Informatika
- Adatvédelemért felelős megbízott

Az Ügyvezető Igazgató főbb feladatai:

- Az Információbiztonsági Rendszerrel kapcsolatos információk egyeztetése az Informatikával,
- Az Információbiztonsági rendszer működéséhez szükséges erőforrások biztosítása,
- Az Információ Biztonsági rendszer belső és külső auditálására megbízás adása.

Informatikai feladatokkal megbízott belső munkavállaó és külső alvállalkozó főbb feladatai (továbbiakban Informatika):

- Az Információbiztonsági rendszer bevezetése, működtetése, a folyamatos fejlesztése, illetve az eredményesség fenntartása
- Jogosultságok kezelése,
- adatmentések felügyelete és naplózása,
- Informatikai rendszer teljesítményének mérése,
- telepített szoftverek átvizsgálása,
- rendszernaplók, víruskeresési naplók, egyéb naplók figyelése,
- az eszközök megfelelő működésének ellenőrzése,
- hálózati működéshez szükséges szoftverek telepítése és beállítása,
- az általános átvizsgálás során észlelt hibák javítása,
- megelőző lépések megtétele,

- munkatársak bejelentései során incidensek monitorozása és javítása,
- a munkatársak igényeinek figyelemmel kísérése,
- javaslatok összeállítása a meglévő szoftverek felhasználására,
- új szoftverek beszerzésére javaslattétel,
- biztonsági beállítások folyamatos felülvizsgálata és szükség esetén korrigálásuk,
- új eszközök vásárlásához javaslatok megtétele,
- A Szervezet információs adatvagyonának felmérése és a nyilvántartás karbantartása
- szerverek, számítógépek telepítése, üzemeltetése.

Adatvédelemért felelős megbízott főbb feladatai:

- adatvédelmi incidensek jelentése
- az Adatvédelemért felelős megbízott részletes feladatait a Szervezet Adatkezelési Szabályzata tartalmazza

2.1.2 Kapcsolat a hatóságokkal és szakmai csoportokkal

Az információbiztonsági (adatvédelmi) incidensek esetén az Informatika kötelessége

- az esemény jelentése az Adatvédelemért felelős megbízott felé
- a kapcsolódó bizonyítékok átadása,
- együttműködés a vizsgálatok lefolytatásában.

A hatóságoknak jelentendő incidenseket az Ügyvezető Igazgató határozza meg. Az Informatika ezt a feladatát a Szervezet jó hírének és érdekeinek védelmének szem előtt tartásával végzi.

Az információbiztonságot érintő ügyekben az Adatvédelemért felelős megbízott köteles kapcsolatot tartani és információt szolgáltatni a következő szervezetek/személyek irányába: Rendőrség, Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH), Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH).

Az Informatika folyamatos kapcsolatot ápol a Szervezet vezetőségével, valamint szükség esetén szakértői információbiztonsági tanácsadást vesz igénybe az információbiztonsági politika, és kapcsolódó szabályozások érvényesítése, az információbiztonság fejlesztésével kapcsolatban és az információbiztonsággal kapcsolatos ismeretek folyamatos frissítése érdekében.

Minden külső IT szolgáltató köteles késedelem nélkül jelezni minden rendellenes vagy annak vélt eseményt az Ügyvezető Igazgató felé.

3. AZ EMBERI ERŐFORRÁSOK BIZTONSÁGA

A Szervezet vezetősége elkötelezett az információbiztonság szervezeten belüli növelése érdekében.
Az információbiztonsági kockázatok között kiemelt helyet foglalnak el a munkavállalókkal kapcsolatos kockázatok, mivel a munkavállalók a munkavégzésük során hozzáférhetnek a Szervezet számára bizalmas és titkos adatokhoz, dokumentumokhoz, amelyekkel esetlegesen visszaélve, vagy akár csak gondatlanul kezelve azokat, súlyos károkat okozhatnak.

Éppen ezért információbiztonsági előírásainak megfelelően a Szervezet különös gondot fordít a munkavállalókkal kapcsolatos kockázatok kezelésére a munkavállalók alkalmazása előtt, alatt, valamint az alkalmazás megszűnése, vagy az alkalmazási feltételekben történő változások eseteiben.

A szabályzat a Szervezet munkavállalóira, különösen az új belépőkre, a csoportot vagy munkakört váltó munkavállalókra alkalmazandó.

3.1 A munkaviszony megkezdése előtt

3.1.1 A munkaviszonnyal kapcsolatos feltételek és kikötések

A Szervezetnél az információbiztonsági vagy azzal összefüggő célok elérése érdekében az új belépőknek az alábbi dokumentumokat kell megismerniük, és az alábbi nyilatkozatokat, megállapodásokat kell aláírásukkal igazoltan elfogadniuk.

Elolvasandó dokumentumok:

- Tűz- és Munkavédelmi szabályzat
- Információbiztonsági szabályzat
- Adatkezelési Szabályzat
- Iratkezelési Szabályzat
- Az adott munkakörre vonatkozó speciális elvárások

Aláírandó nyilatkozatok, megállapodások:

- Titoktartási nyilatkozat
- Nyilatkozat az elolvasott dokumentumokról

3.2 A munkaviszony fennállása során

3.2.1 Vezetői felelősségek és Információbiztonság tudatosítása, oktatása, képzése

A vezetőség egyértelműen rögzítette jelen szabályzatban és a kapcsolódó egyéb szabályozásokban, a munkaszerződésekben, hogy megkövetelik a munkatársaktól az információbiztonsági irányelvek betartását.

A Szervezet az információbiztonsági tudatosság szintjének folyamatos emelése érdekében rendszeres képzésekben részesíti munkatársait évente egy alkalommal. A munkatársak ezen a képzéseken és a hozzájuk kapcsolódó vizsgákon (értékeléseken, teszteken) kötelesek részt venni és legalább megfelelő eredményt elérni.

Aki egy éven belül, az adott időszakra vonatkozó oktatási követelményeket nem teljesíti, az a munkaköre betöltésére alkalmatlanná válik.

A képzéseket a Szervezet vezetője szervezi és tervezi meg. A képzések tárgyköre át kell fogja az alábbiakat.

- információbiztonsági ismeretek
- adatvédelmi ismeretek
- érvényes szabályozások, előírások

Az információbiztonsági tudatosság ellenőrzése a képzésekhez kapcsolódó vizsgákon, és a tervezett felmérések, versenyek, kampányok, valamint az információbiztonsági auditok során valósul meg

3.3 A munkaviszony megszűnése és megváltozása

A foglalkoztatás megszűntetésére vagy megváltoztatására a közvetlen vezető tesz javaslatot. Az alkalmazás megszűntetéséről a munkaviszony létesítéséhez illetve megszüntetéséhez kapcsolódó munkáltatói jogok gyakorlója dönt.

Az alkalmazás megszűnését követő meghatározott időszakig történő titoktartást a munkatársaktól az alkalmazás megkezdésekor kitöltött titoktartási nyilatkozatban kell rögzíteni.

Az alkalmazás megszűnésekor a kilépő munkatársak kötelesek minden, a Szervezet tulajdonát képező vagyontárgyat visszaszolgáltatni. Ennek ellenőrzése érdekében a munkaáltató jogosult a munkavállalóra bízott vagyontárgyakat soron kívül leltározással ellenőrizni. A hiányokat vagy károkat a munkatárs köteles megtéríteni, az adott vagyontárgy könyv szerinti értéke alapján. Meg kell róla győződni, hogy minden a munkatárs nevén szereplő vagyontárgy az eszközgazdálkodás és a konfiguráció kezelés nyilvántartásaiban (cél) visszavételre, vagy új tulajdonoshoz rendelésre kerüljön.

A munkatárs jogosult a visszaszolgáltatott vagyontárgyakról a személyes adatait eltávolítani, de nem jogosult a Szervezet tulajdonát képező információkat törölni.

A kilépő munkatárs köteles a privát eszközeiről (Mobil telefon, laptop, pendrive...stb.) a vezetője vagy a kiléptetést végző személy jelenlétében eltávolítani minden hozzáférést, Szervezeti anyagot különös tekintettel a mobil eszközök által nem fizikai eszközökre szinkronizált dokumentumokat.

Az összes hozzáférési jogot az alkalmazás megszüntetése, változtatása után meg kell szüntetni, mely feladatot az Informatika látja el.

Minden vezető felelős az általa vezetett munkatársak munkaviszonyának megszűnését követően a Szervezeti rendszerekben adott jogosultságok visszavonásáról meggyőződni, hiba esetén intézkedést kezdeményezni.

A távozó munkatárs vezetője felelős a távozással érintett szerepkörök folytonosságát biztosítani, az új munkatársat kijelölni.

Az Ügyvezető évente rendszeresen ellenőrzi a megszűnt munkaviszonyú munkatársak jogosultságainak visszavonását a belső audit keretében a rendelkezésére bocsátott névsor alapján, és a jogosultságokat köteles vezetni a „Jogosultsági mátrixban".

Abban az esetben, ha egy Szervezettől távozó dolgozó jogosultságainak létezését vezetője kockázatosnak ítéli meg a következők szerint kell eljárni:

Mielőtt a dolgozóval vezetője közli az elbocsátást a közvetlen vezetőjét tájékoztatni kell az elbocsátás bejelentésének pontos időpontjáról, a várható visszavonási igényekről, valamint elő kell készíteni a dolgozó céges eszközeinek elvételét.

Az elbocsátás közlésével egy időben azonnal végre kell hajtani a következőket:

- Desktop vagy laptop visszavételezése
- Mobil eszközök visszavétele

Az elbocsátás tényének közlése után a kísérő személy és a dolgozó felettese visszakíséri a dolgozót a munkavégzés helyére, ahol lehetősége van összeszedni a személyes tárgyait majd a céges eszközök átadása után a dolgozót kikísérik az épületből.

Az Informatika köteles a visszavett adathordozókon lévő privát megjelölésű adatokteljes törlésére/formatálására illetve a távozott kolléga postafiókjának megszüntetésére és tartalmának törlésére. A munkatársak számítógépein vagy az online felhő tárhelyen található privát adatok törléséről az Ügyvezető Igazgató illetve az Informatika köteles értesíteni az adat gazdáját majd ezután törölni a privát tartalmú adatokat. Amennyiben a távozó munkatárs kulcsszerepet játszott bizonyos folyamatok kapcsán, az email címe a távozást követő három hónapban megmaradhat és egy automatikus válasszal jelezhető a küldő félnek, hogy a jövőben kinek címezheti a megadott tartalmú emaileket.

4. VAGYONELEMEK KEZELÉSE

4.1 A vagyonelemekért viselt felelősség

A dokumentum célja a Szervezet tárgyi eszközök kezelésével kapcsolatos szabályok és felelősségek meghatározása az egységes és átlátható, valamint eredményes eszközkezelés és eszközgazdálkodás megteremtése érdekében.

4.1.1 A vagyonelemek felelősei

A Szervezet különös figyelmet fordít a Tárgyi Eszközökkel való hatékony gazdálkodásra, ezért a felmerülő igényeket ennek szem előtt tartásával igyekszik kielégíteni, és a használaton kívüli eszközöket felhasználni.

A Szervezet nem támogatja az idegen tulajdonban lévő, felhasználási engedély nélküli tárgyi eszközök munkavégzéshez köthető használatát.

A munkavégzéshez szükséges eszközöket a Szervezet szerzi be és a költségeket is maga fizeti meg.

A Szervezet Pénzügyi Vezetője rendszeres időközönként tárgyi eszköz leltárt készít, hogy alátámassza a mérleg valódiságát.

Felhasználókra vonatkozó általános szabályok:

- A Felhasználó kötelezettsége azon Tárgyi Eszközökkel való elszámolás, melyek a Felhasználó által leadott és a Szervezet részéről engedélyezett igénynek megfelelően megrendelésre, leszállításra, valamint átvételre kerültek.

- A Szervezet valamennyi Felhasználója Tárgyi Eszközt csak a tulajdonában kezelt folyamatokon keresztül vehet birtokba, adhat át és csak az előzetes jóváhagyásokat követően használhat. Valamennyi Tárgyi Eszköz átadása-átvétele a vonatkozó jogszabályok, valamint jelen Szabályzatban rögzített módon történik.

- A Szervezet valamennyi Felhasználója köteles a Tárgyi Eszköz állapotában (mennyiségében vagy minőségében) bekövetkezett változást az Informatikának haladéktalanul jelenteni, és arról a változást megfelelően rögzítő jegyzőkönyvet felvetetni.

- A Tárgyi Eszközökben Felhasználók által okozott károkért (gondatlan, vagy szándékos károkozás) a Felhasználók anyagi felelősséggel tartoznak.

- A Felhasználó a Szervezet által végzett, az eszközgazdálkodási területet érintő ellenőrzések során köteles együttműködni az ellenőrzést végző személyekkel, és minden információt megadni számukra a tárgyi eszközökkel kapcsolatban.

A jelen szabályzatban előírtaktól való eltérés csak ügyvezető igazgatói engedély esetén megengedett.

4.1.2 A vagyonelemek visszaszolgáltatása

Amennyiben a Szervezet munkatársnak nincs szüksége az eszköz további használatára, úgy a Felhasználó írásban kezdeményezi az Informatikának az eszköz átadását.

A Szervezet Eszköz Kiadási Szabályzatának 2. melléklete (visszavételi jegyzőkönyv) kitöltése után az Ügyvezető Igazgató meggyőződik:

- A jegyzőkönyven feltűntetett adatok helyességéről
- A visszaszolgáltatott eszköz(ök) állapotáról.

4.2 Adathordozók kezelése

4.1.3 A cserélhető adathordozók kezelése

Adathordozó: Az adat tárolására és terjesztésére alkalmas eszköz.
Az adathordozók biztonságos kezelésének kialakításával megakadályozható a Szervezet magasabb szintű adatbiztonsági kategóriákba besorolt adatainak illetéktelen kézbe való kerülése. A Szervezet tulajdonában lévő, a magasabb szintű adatbiztonsági kategóriákba besorolt adatok tárolására használt adathordozókat, amennyiben az a kockázati értékelésen egy előzetesen meghatározott értéket elér, azt egyedi azonosítóval kell ellátni, nyilvántartást kell vezetni róla.
Adathordozók tárolására vonatkozó szabályok:

- figyelembe kell venni a gyártó által meghatározott tárolási környezetre vonatkozó paramétereket, a tároló helynek tűzbiztos, elektromágneses hatásoktól védett helynek kell lennie,
- az adatbiztonsági kategóriákba besorolt adatokat tartalmazó adathordozók tárolásánál figyelembe kell venni a szabályzat adatok kezelésével kapcsolatos előírásaiban megfogalmazottakat,
- két példányban való tárolás esetében a tároló helyet úgy kell kiválasztani, hogy szükség esetén az arra jogosult akadálytalanul és viszonylag gyorsan hozzáférhessen, de célszerűen, viszonylag távol legyen egymástól a két tárolásra szolgáló helyiség (amennyiben ez értelmezhető), ezzel megakadályozva mindkét példány egyidejű megsemmisülését természeti katasztrófa esetén,
- adathordozókat zárható szekrényben kell őrizni/tárolni, amikor éppen nincsenek használatban, főként a munkaidőn kívüli időszakban.
- USB portok és optikai meghajtók írási jogának korlátozása az egyes számítógépeken

Az adatok osztályozása után meg kell határozni az osztályba sorolási szintnek megfelelően az adatok elvárt rendelkezésre állását is. Ennek alapján az Informatikának meg kell határoznia azokat az információ-kezelő eszközöket is, amelyek szükségesek az adatok rendelkezésre állásához (szerverek, tárolók, aktív eszközök, adathordozó, stb.). Ha az Információbiztonsági szabályzat az eszközök különböző rendelkezésre-állású adatokat kezelnek, akkor azok közül a legszigorúbb követelményt kell figyelembe venni.

4.1.4 Adathordozók eltávolítása

Megsemmisítés/törlés: Csak az Adatgazda (Adatvagyonleltárban megjelölt felelős) engedélyével törölhető/semmisíthető meg. Az elektronikus adathordozón lévő adatokat törölni kell (minőségi törléssel, többszöri felülírással), a hibás adathordozókat fizikailag meg kell semmisíteni,

A maximális élettartamuk lejárta után az adathordozókat át kell másolni új adathordozóra, majd a régi adathordozót le kell selejtezni, és meg kell semmisíteni,

A Szervezet mindaddig elzárva tárolja a meghibásodott adathordozókat, ameddig azok szakszerű fizikai megsemmisítése és elszállítása meg nem történik.

Megsemmisítéskor az adathordozót fizikailag kell megsemmisíteni, és az IBSZ 4. mellékletében szereplő megsemmisítési jegyzőkönyvben szükséges vezetni. Adathordozónak kell tekinteni a papír alapú dokumentumokat is.

Az adathordozót le kell selejtezni akkor is, ha vélhetően az adathordozó hibája miatt az adatmentés sikertelen volt, illetve ha a katasztrófa vagy visszatöltési próbák során az adat visszatöltés sikertelenné vált.

Amennyiben az adathordozón elérhető még a tartalma, a selejtezés előtt szükséges minőségi törléssel eltávolítani az adathordozón lévő adatokat.

4.1.5 Fizikai adathordozók szállítása

Fizikai adathordozón Szervezeti információt a Szervezet telephelyeiről kivinni csak az Ügyvezető Igazgató Írásos engedélye esetén lehetséges. Minden más esetben fegyelmi eljárást von maga után.

5. HOZZÁFÉRÉS FELÜGYELET

A Szervezet az üzletvitele során köteles gondoskodni az üzleti és a személyes adatok biztonságáról, köteles továbbá megtenni azokat a technikai, és szervezési intézkedéseket, és kialakítani azokat az eljárási szabályokat, amelyek a tulajdonosi elvárások, adatvédelmi törvény, az ügyfélelvárások, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.
A Szervezetnek jelentős üzleti és vagyoni érdekei is fűződnek az IT rendszerek biztonságához, így fontos biztosítani azt, hogy a Szervezet adataihoz egy ellenőrzési folyamat után dokumentált módon és indokolt időtartamig lehessen hozzáférni.
Jelen szabályzat célja a Szervezet jogosultságkezelési folyamataival kapcsolatos szabályok meghatározása.

A szabályzat kiterjed a Szervezet belső informatikai rendszereihez és szolgáltatásaihoz történő hozzáférésekre.

5.1 A hozzáférés-felügyelettel kapcsolatos üzleti követelmények

5.1.1 Szabály a hozzáférés felügyelethez

A jogosultságok kiosztásának alapelve, hogy mindenki a munkájának elvégzéséhez szükséges információkhoz a feladatának megfelelő módon tudjon hozzáférni, de sem ennél több, sem ettől eltérő típusú hozzáféréssel ne rendelkezzen, valamint minden feleslegessé vált jogosultságot késedelem nélkül megszüntessenek. A jogosultságok kiosztását, azaz a jogosultság kezelés folyamatát úgy kell megoldani, hogy a munkavégzéshez szükséges alapvető jogosultságok mindig rendelkezésre álljanak minden feladatkörben, és az ezt meghaladó igényeket megfelelő jóváhagyási folyamaton át ellenőrzött módon zökkenőmentesen lehessen teljesíteni. A jogosultság kezelési folyamatnak biztosítania kell a kiosztott jogosultságok ellenőrizhetőségét, és a visszavonás hiánytalan megtörténtét.

A szabályozás naprakészen és a szabályozásban foglaltak szerinti működés feltételeinek biztosítása az Ügyvezető Igazgató felelőssége.

5.1.2 Hozzáférés hálózatokhoz és hálózati szolgáltatásokhoz

A Szervezet belső hálózatához kívülről (nem Szervezet által felügyelt hálózatból) az arra jogosultságot kapott felhasználók, csak az Szervezet által biztosított VPN kapcsolaton át csatlakozhatnak. Szigorúan TILOS bármiféle ettől eltérő megoldás megkísérlése a felhasználók részéről.
A Szervezet belső hálózatához csak a Szervezet ellenőrzése alatt álló eszközöket szabad csatlakoztatni.
Külső cégeknek tilos a berendezéseiket a Szervezeti hálózaton külön engedélyezés nélkül üzemeltetniük.

Minden, a belső hálózatra csatlakozó berendezést azonosítani kell tudni. A belső hálózathoz csak az arra jogosult, azonosított eszközök csatlakozhatnak. A megkötés alól

kivételt képeznek a vendég WiFi csatlakozási lehetőségek, amik a vendégek számára biztosítanak Internet elérést. Ezek a csatlakozások úgy kerülnek kialakításra, hogy azokról a Szervezet belső hálózatán található szolgáltatások semmiképpen nem lehetnek elérhetők.

5.2 Felhasználói hozzáférések kezelése

5.2.1 Felhasználók regisztrálása és törlése

Regisztrálás:
A felhasználókat egyedi felhasználónévvel kell azonosítani. Csoportos felhasználóneveket TILOS használni. A felhasználók azonosítása a mindenkori névkonvenció szerint egyedi, a felhasználó nevéből képzett azonosítók használatával történik. Ügyelni kell azonban arra, hogy a munkatársak távozását követő 1 éven belül ezen névkonvenciók törlésre kerüljenek
A névkonvenció szabálya: Keresztnév, majd a Vezetéknév ékezet jelek és szóközök nélkül ponttal elválasztva. Ugyanazon nevű munkavállalók esetében a Keresztnév után növekvő római sorszámmal (II-től induló számozás) került megkülönböztetésre.
A felhasználók regisztrálása és a felhasználói adatok módosítása az Informatika feladata. Az említett munkautasítások naprakészségéért az Ügyvezető Igazgató felelős.
Minden külső IT szolgáltató munkatársai rendelkezhetnek jogosultsággal, de ennek a ténynek a Szervezet és a szolgáltató közti szerződésben rögzíteni kell.

Felhasználó törlése:
Munkavállaló kilépése esetén a folyamatot elindításáért a munkavállaló közvetlen vezetője a felelős. A felhasználó törlésére az Informatika jogosult.
A bejelentő vezető ezzel egyidejűleg – ha a kockázatok indokolják – soron kívül teszi meg a szükséges további információvédelmi intézkedéseket is. (pl. visszaélés gyanúja esetén soron kívüli felfüggesztés elrendelése stb.)
A Szervezet irodájába történő belépéshez használt riasztókódok törlése szükséges minden olyan esetben, amikor egy munkavállaló távozik vagy egy alvállalkozóval felmondják a szerződést (amennyiben ismerte a riasztó kódót).

5.2.2 Felhasználói hozzáférés biztosítása

A jogosultságkezelési folyamatban az alábbi általános szabályok az irányadóak:

- Hozzáférést csak a szükséges mértékben és időtartamra szabad engedélyezni, olyan személyek számára, akiknek a feladataik ellátása és/vagy jogaik gyakorlása érdekében indokolt. A szükséges mértékre és időtartamra történő korlátozás nemcsak a hozzáférés kockázatát minimalizálja, hanem a hozzáférő személy által viselt felelősséget is.

- A Szervezet rendszereihez csak a jogosultságkezelési folyamat betartásával adható hozzáférés.

- Külső partnerek (vállalkozók stb.) vonatkozásában a Szervezet IT rendszereihez való hozzáférés csak szerződés alapján biztosítható.

- A Szervezet IT rendszereihez hozzáférési jogot kapott természetes személyek, jogi személyek és jogi személyiséggel nem rendelkező szervezetek a hozzáférési jogot a velük kötött szerződés, megállapodás vagy titoktartási nyilatkozatok alapján gyakorolhatják.

- A hozzáférési jogosultságokkal történő visszaélés gyanúja esetén a Szervezet minden dolgozója köteles értesíteni az Ügyvezetőt.

- Jelen szabályzattól eltérni az Ügyvezető Igazgató engedélye esetén lehetséges. (Ilyen esetekben is szükséges a folyamat megfelelő dokumentálása)

A Szervezetnél a jogosultságigénylő lap alapján kapnak jogosultságot a munkatársak. Ezen kívül dedikált jogosultság jár, ha egy adott csoport tevékenysége alapján szükséges, előre meghatározott jogosultságok, amelyeket személyre szólóan kell igényelni. Ide tartoznak az alapjogosultságokon felüli, a Szervezet rendszereihez való hozzáférések (pl. számlázó program…stb.).

5.2.3 Kiemelt hozzáférési jogok kezelése

Privilegizált jogosultságok (rendszergazdai jogosultságok)
Minden olyan jogosultság ebbe a körbe tartozik, amely a felhasználói jogoknál több jogot jelent (pl. rendszeradminisztrátor stb.). Főbb szabályok a privilegizált jogosultságokkal kapcsolatban:

- A rendszerek adminisztrációjához kellő rendszergazdai jogosultságot (előjogokat) csak a rendszergazdai feladatkörben foglalkoztatott munkatársak kaphatnak és csak a feladatkörüknek megfelelő rendszerekre érvényesen. A rendszergazdai jogosultságok (előjogok), ahol ennek kifejezett műszaki akadálya nincsen, legyenek egyértelműen személyhez kötöttek, a csoportos azonosítók használata mindenképpen kerülendő.

- A rendszergazdák az előjogokat biztosító azonosítójukat csak a munkavégzéshez feltétlenül szükséges mértékben használják, minden más esetben a normál felhasználói azonosítójukkal dolgozzanak.

- Mindenképpen kerülni kell olyan rendszerek üzembe állítását, amelyek nem rendszergazda munkakörben dolgozó felhasználók rendszergazdai jogosultságokkal történő felruházását igényelnék (kivételt képezhetnek a termelésben részt vevő eszközök, amelyek bizonyos telepítések kapcsán hitelesítő eszköz kezelőben kivételként kezelendők illetve network adminisztrátori jogosultsággal rendelkezhetnek).

- A Szervezet partnereivel kötött megállapodásokban (adatfeldolgozói szerződésekben) tisztázni kell azon felelősségi köröket, amelyek a közös rendszergazdai tevékenység útján keletkezhetnek (pl: több Szervezet által közösen használt szoftvermegoldás vagy adatbázis közös használata).

A Szervezet üzemeltetési feladatait a Silver Frog Informatikai Kft. látja el, így a fenti szabályok érvényesítendők a megnevezett szervezetre is.

A Szervezet a weboldalak kezelését illetve a marketing célú levelek kiküldését az Online Marketing Stratégia Kft. végzi. A GDPR szempontjából kiemelten fontos tevékenység kiszervezése kapcsán, a Szervezet a marketing tevékenységet végző szervezettel a felelősségi köröket írásos szerződésben köteles rendezni.

5.2.4 Felhasználói hozzáférési jogok átvizsgálása

A felhasználó által igényelt jogosultságok indokoltságát és információbiztonsági megfelelőségét a munkahelyi vezetőnek és az adatgazdának kell rendszeresen (évente legalább egyszer) átvizsgálnia.
A már regisztrált felhasználók adatainak helyességét és a részükre megadott jogosultságokat rendszeresen, legalább évente egy alkalommal át kell vizsgálni, azzal a céllal, hogy az adminisztráció során bekövetkezett hibákat/tévedéseket kiszűrjék.

Ellenőrizni kell az adatok helyességét, ki kell szűrni
- a már kilépett, de esetleg a rendszerben bennmaradt munkatársakat,
- a megváltozott munkakör után megmaradt régi jogosultságokat,
- az ideiglenesen megadott, már lejárt jogosultságokat.

5.2.5 A hozzáférési jogok visszavonása vagy módosítása

A hozzáférési jogosultságok megszüntetéséről (teljes visszavonásáról) a felhasználó közvetlen vezetője az alábbi esetekben köteles intézkedni és felelősséggel eljárni:
- dolgozó kilépése esetén,
- ha a munkavállaló szervezeti egységen belül marad, de a munkaköre jelentősen megváltozott
- ha a külső partner szerződése lejárt vagy megszűnt,
- tartós (3 hónapon túli) betegség, távollét, illetve helyettesítés esetén,
- tartós (3 hónapon túli) kirendelés esetén,
- visszaélés gyanúja vagy hasonló súlyos biztonsági esemény felmerülése esetén.

Bármely - a munkavállaló kilépésén kívül - a jogosultsági igényekben bekövetkező változás miatt szükségessé váló jogosultság visszavonása esetén az Informatika írásos értesítése szükséges.

IT rendszerek közötti kapcsolat megszüntetését vagy felfüggesztését az Informatika kezdeményezheti.

5.2.6 Felhasználói jogosultságok nyilvántartása

Az Informatika felelőssége az IBSZ 3. mellékletét képző „Jogosultsági mátrix" napra készen tartása.

5.3 Felhasználói felelősségek

5.3.1 Titkos hitelesítési információk használata

Minden Szervezet dolgozó a hozzá tartozó titkos hitelesítő információkat bizalmasan kezeli, egy munkatárssal sem oszthatja meg. Papír alapon nem tárolhatja sem a munkahelyén, sem otthonában.

Gondatlan hitelesítési információ használatból fakadó károkért a dolgozó vállal felelősséget.

Ezen információk csak az Ügyvezető Igazgató írásos engedélyével osztható meg.

5.4 Rendszer és alkalmazás-hozzáférés felügyelete

5.4.1 Információhoz való hozzáférés korlátozása

Az információhoz történő hozzáférést ezen fejezet 5.1 pontjában megadott elvek gyakorlati megvalósításával kell a szükséges mértékre korlátozni.
Ezen elveknek és a Jogosultság kezelési folyamatnak az alkalmazásával kell a felhasználók információ hozzáférését korlátozni a különféle szolgáltatásokban és alkalmazásokban.
A szolgáltatásoknak és alkalmazásoknak lehetővé kell tenniük a felhasználói információ-hozzáférés ellenőrzés alatt tartását, úgy, hogy minden egyes felhasználó csak a részére, a Jogosultság kezelési eljárásban engedélyezett jogosultságoknak megfelelő módon korlátozottan tudjon a tárolt információkhoz hozzáférni/létrehozni/módosítani/törölni és az alkalmazásokban az információk kezelésére/feldolgozására utasításokat adni.
Az Informatika köteles a felelősségébe tartozó rendszerekben a hozzáférési jogok korlátozásáról gondoskodni.

5.4.2 Biztonságos bejelentkezési eljárások

Jelen szabályzat a jelszókezelésre vonatkozó rendelkezés, melynek célja meghatározni a Szervezet IT rendszereihez hozzáférést biztosító jelszavak és felhasználói nevek kezelését, képzését, módosítását, valamint az IT rendszerek jelszókezelő alrendszerének egységes követelményeit.

A Jelszó

A jelszó az egyik fő eszköz arra, hogy a felhasználó az IT rendszerekhez való hozzáférési jogosultságát érvényesítse, és az illetéktelen hozzáférést meggátolják.

A jelszóhasználat fő szabályai:

- A jelszó jogosulatlan személynek történő átadása vagy hozzáférhetővé tétele üzleti titoksértésnek minősül, ami munkajogi és büntetőjogi felelősségre vonás alapját képezheti.

- A felhasználóknak a jelszavaikat bizalmasan kell kezelniük, azt senkivel nem közölhetik. A jelszó közlését senki nem kérheti a felhasználótól.

- Egy adott IT rendszerben minden felhasználó számára egyedi felhasználói azonosító és ehhez rendelt jelszó alkalmazása kötelező. Csoportos jelszó és felhasználói azonosító használata tilos.

- A felhasználók a jelszavaikat csak abban az esetben jegyezhetik fel, ha az Ügyvezető Igazgató által erre a célra meghatározott, engedélyezett eszközzel és módon történik.

- Valamennyi új hozzáférésnél minőségi induló jelszó megadása kötelező, melyet az felhasználónak, kikényszerített módon azonnal, az első használat alkalmával, a kiadást követően legfeljebb egy napon belül, le kell cserélnie saját jelszavára.

- Az átadás során a kezdeti jelszó bizalmasságának megőrzését és az illetéktelen hozzáféréstől történő megóvását zárt boríték használatával kell biztosítani.

- Az felhasználó személyazonosságának megbízható megállapítása a borítékot személyesen átadó Ügyvezető Igazgató feladata.

- Az Informatikának TILOS a felhasználó kérése alapján jelszót beállítaniuk, a jelszót minden esetben a felhasználónak kell magának beállítania.

- A jelszavakat nyílt szöveg formájában TILOS tárolni vagy bármilyen csatornán továbbítani.

- Jelszavak begépelése során a billentyűzetet illetéktelen személyek rálátásától védeni kell.

- A Szervezet rendszereiben használt jelszóval azonosat TILOS más, például nyilvános vagy otthoni rendszerekben használni.

- Ha a felhasználó jelszavának visszaállítása válik szükségessé, akkor a jelszó visszaállítása előtt meg kell győződni a visszaállítást igénylő felhasználó személyazonosságáról. Ideiglenes, egyszeri bejelentkezésre használható jelszót kell kiadni a kezdeti jelszó kiadásával azonos követelmények szerint.

- A nem megszemélyesíthető felhasználók részére is legalább a jelen szabályzatban meghatározott minőségi jelszavakat kell megadni.

- Amennyiben a használt rendszer lehetőséget biztosít rá, kötelező a rendszer által felkínált két faktoros authentikáció alkalmazása.

- Kötelező a minőségi jelszó alkalmazása

Minőségi jelszó:

A Szervezet IT rendszereiben csak minőségi jelszó használható. A minőségi jelszó képzésének szabályai az alábbiak:

- Minimálisan 8 alfanumerikus karakterből áll.

- Amennyiben az adott IT rendszer támogatja, írásjeleket és speciális karaktereket is tartalmaz, pl. ( ),.?+.

- Csak ékezetmentes betűből áll.

- A jelszó nem lehet azonos a felhasználói azonosítóval.

- jelszó legyen összetett, a négy típusú karakterből (kisbetű, nagybetű, szám, speciális jelek) legalább három típus szerepeljen a benne.

- Nem tartalmazhat azonos karakterből, vagy egymás után következő számból, betűből, vagy a billentyűzeten egymást követő karakterekből álló csoportokat (karaktercsoportnak számít 3 egymást követő karakter),

- Semmi olyat nem tartalmazhat, amelyet bárki más könnyen kitalálhat, vagy az illető személyével kapcsolatos adatokból kinyerhet, például nevekből, telefonszámokból, születési adatokból stb.

- A jelszó módosításánál az új jelszó kialakításánál törekedni kell arra, hogy szerkezetében ne hasonlítson az előző, lecserélendő jelszóra.

A minőségi jelszó generálása a WI-FI és adminisztrátori jelszavak generálása esetén is érvényes.

5.4.3 A programok forráskódjához való hozzáférés felügyelete

A belső IT rendszer szolgáltatásaihoz külső fejlesztőkkel készíttetett rendszerek forráskódját, amennyiben az a fejlesztési szerződés alapján átadásra kerül az Ügyvezető Igazgató őrzi.

6. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

Ez a fejezet a Szervezet vezetőségének biztonsági elvárásait tartalmazza a fizikai biztonság vonatkozásában.

A standardizált elvárások bemutatásával és a biztonsági szabályozások vonatkozásában a Szervezet definiálta a szükséges, magas fokú biztonsági elvárást és adat védelmet minden létesítményre.

Ez a dokumentum egy átlátható, tiszta összegzés a standard követelményekkel az átláthatóság, összehasonlíthatóság, ismételhetőség biztosításának érdekében egyeztetve a Szervezeti biztonság specifikus álláspontokkal.

A szabályok és azok konkrét elvárásai magasabb szintű és részletesebb utasításokat tartalmaznak az alkalmazottak számára, hogy hogyan járjanak el biztonságtudatos módon és a biztonsági védelem alapjaként szolgálnak a biztonság-releváns fenyegetések esetén.

Az Ügyvezető Igazgató és az Informatika biztosítja a felelős személyeknek a jogok és kötelezettségek meghatározását mind tulajdonosi mind felhasználói szerepkörökben. Emellett tartalmazza a specifikációkat a létrehozásra és a fejlesztésre vonatkozóan, a fizikai és szervezeti védelmi törekvések tekintetében.

Ez a biztonsági szabályozás érvényes minden jelenlegi és jövőbeli Szervezet helyszínen.

Jelen biztonsági elvárások alkalmazásakor az eredmények a környezeti változók függvényében eltérőek lehetnek, (pl. helyi hatósági előírások) ennek megfelelően bizonyos esetekben az egyedi igények figyelembevételével, de ezen dokumentumban foglalt elveknek megfelelően kell eljárni.

6.1 Berendezések elhelyezése és védelme

Minden technikai eszközt rendeltetésének megfelelően kell elhelyezni a Szervezet által birtokolt vagy bérelt létesítményben. Amennyiben munkavédelmi előírás vonatkozik egyes eszközök beállítására, azokat figyelembe véve kell elhelyezni. A jogszabályi előírások betartatásáért az Ügyvezető Igazgató felel.

Minden helyiség védelmét az előző alfejezetben taglalt előírásoknak megfelelően kell biztosítani.

6.2 Vagyonelemek eltávolítása

A munkavállaló a telephelyről csak a részére használatra átadott mobil eszközöket viheti ki. Minden más esetben az illetékes munkahelyi vezető engedélyét kell kérni.
Tilos az informatikai infrastruktúra elemeit engedély nélkül, nem a munkaköri feladatba tartozó módon megváltoztatni, vagy eltávolítani.

6.3 Berendezések és vagyonelemek biztonsága a telephelyen kívül

- Ha a készülék a szállítás során túlzottan lehűlt, vagy felforrósodott, használat előtt meg kell várni amíg szobahőmérsékletre kerül.

- Használat közben óvni kell az erős napsugárzástól, portól, nedvességtől, erős rázkódástól.

- Különösen külföldön az elektromos hálózatra történő csatlakozás előtt győződjön meg róla, hogy a hálózat megfelel a készülékére megengedett értékhatároknak.

- Telephelyen kívül lehetőleg soha ne hagyja felügyelet nélkül a mobil eszközöket. Ha ez nem lehetséges, mindig kapcsolja ki.

- A mobil eszközök telephelyen kívüli használatával kapcsolatban a távmunkavégzés szabályai érvényesek.

- Tilos a mobil eszközök használatát 3. feleknek átengedni, sem idegenek, sem családtagok, rokonok, ismerősök nem használhatják ezeket.

6.4 Berendezések biztonságos eltávolítása vagy újrafelhasználása

A Szervezet eszközeinek cseréje, mozgatása, áthelyezése az Ügyvezető Igazgató engedélyével és jelenlétében történhet csak meg.

Ennek elmulasztása esetén bekövetkező baleset és kár a dolgozót terheli.

6.5 Őrizetlenül hagyott felhasználói berendezések

A Szervezet által képviselt magas adatbiztonság a munkatársak oldaláról is alapkövetelmény.

Az őrizetlenül hagyott munkaeszközöknek nem szabad jogosulatlan hozzáférést biztosítaniuk illetéktelenek, ezért minden dolgozótól elvárt követelmény, hogy egy eszköz akár rövid időre sem hagyható őrizetlenül lezárt felhasználói fiók nélkül.

A munkaállomásokat úgy kell beállítani, hogy ha azokat hosszabb időre (több mint 5 perc) felügyelet nélkül hagynák, akkor az operációs rendszer automatikusan zárolja önmagát és csak a felhasználó újbóli azonosítását követően lehessen azt használni.

6.6 Tiszta asztal és tiszta képernyő szabálya

Az irodahelységekben 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.

A felhasználók kötelesek a munkájuk megszakítása vagy befejezése után a számítógépüket zárolni vagy kikapcsolni.

A munkatársak a munkához szükséges file-jaikat az arra kijelölt hálózati helyen kötelesek tárolni. A számítógép asztalán csakis az egyes alkalmazások parancsikonjai helyezhetőek el. A gyorsabb munkavégzés miatt a számítógépre másolt adatokat a dolgozó saját mappájában köteles tárolni a munkavégzés idejére, melyet ugyancsak köteles a hálózati adattárhelyre visszamásolni a munkamenet lezárását követően (a számítógépről pedig törölnie szükséges).

7. ÜZEMELÉS BIZTONSÁGA

7.1 Üzemeltetési eljárások és felelősségek

7.1.1 Dokumentált üzemeltetési eljárások

Az IT rendszerek, eszközök üzemeltetéséről rendszerenként külön dokumentumokban szükséges rendelkezni. Az üzemeltetési dokumentációért az Informatika a felelős. Az üzemeltetési dokumentációnak a rendszerek használatbavételekor rendelkezésre kell állnia. Az Informatika a felelős az üzemeltetési dokumentáció naprakészen tartásáért.

7.1.2 Kapacitáskezelés

Az informatikai rendszer megfelelő teljesítőképességének biztosítása érdekében a rendszer erőforrásainak felhasználását az Informatika monitorozza, és a mérések alapján előrejelzéseket készít a jövőbeli kapacitásigényekre vonatkozóan.

7.1.3 A fejlesztési, tesztelési és az üzemi környezetek elkülönítése

A Szervezet fejlesztési, tesztelési és üzemi környezetei egy infrastruktúrában találhatók, de elkülönített adatbázist használnak a különböző folyamatokra.

A következő fő információbiztonsági és GDPR által támasztott szempontokat szükséges figyelembe venni a biztonságos szoftverfejlesztés és támogatási folyamatok betartásának érdekében:

- A szoftvernek szükséges megfelelnie a GDPR rendeletben támasztott adatkezelési alapelvek érvényesíthetőségének, különös tekintettel az integritásra és bizalmas jellegre (5. cikk (1) f)).
- Az érintettek jogainak érvényesítési szándéka esetén a rendszer megfelelő felkészítése szükséges, fokozott figyelemmel a törléshez- (17. cikk), a hozzáféréshez- (15. cikk) és az adathordozhatósághoz való jogra (20. cikk) (adathordozhatósági kérelem esetén az érintett adatait lehetőség szerint .XML vagy .CSV formátumban kell átadni).
- A felhasználók munkájának dokumentációkkal történő segítése, a szoftverek funkcionális működésének megismerése érdekében.
- A kiszervezett fejlesztés során a teljes fejlesztési folyamat felügyelete és a kiszervezett rendszerfejlesztési tevékenységek megfigyelése (szerződéses keretek, biztonsági követelmények, elfogadási és átvételi kritériumok meghatározása).
- A rendszerfejlesztési és integrációs tevékenységek számára biztonságos fejlesztési környezet létrehozása és védelme, amelyek lefedik a rendszerfejlesztés teljes életciklusát.
- A szoftverekben tárolt adatokhoz történő munkatársi hozzáférés lehetőség szerinti szűkítése mezőszinten, így biztosítva a bizalmas jellegnek történő megfelelést.
- A személyes adatokat tartalmazó adatbázisok elkülönített tárolása – amennyiben

technikailag megoldható –, így biztosítva azok védelmét és kezelhetőségét (pl.: biztonsági mentés)

- A fejlesztés során történő anonimizált-, vagy teljesen véletlenszerű adatokból álló adatbázis használata, éles adatbázis használatának kerülése.
- Amennyiben a fejlesztőknek szükséges az éles működési környezetbe történő betekintés, ideális azt a Szervezet telephelyén megvalósítani. A betekintést minden esetben felügyelet mellett indokolt végezni - erre lehet megoldás egy azonosítást igénylő, távoli asztali kapcsolat minden egyéb művelet korlátozásával történő felépítése (pl.: az eszköz egyéb területeihez való hozzáférés). Amennyiben a Szervezet munkatársának nincs lehetősége a munkamenet felügyeletére, úgy a támogatási folyamatról felvétel készíthető.
- Az éles adatbázis kívülről történő elérhetőségének korlátozása (jóváhagyáshoz kötött), írási és olvasási jogosultsággal, csak az adott adatbázist használó szoftver rendelkezhet.
- Elfogadási tesztprogramok, valamint hozzájuk kapcsolódó kritériumok létrehozása az új információs rendszerekre, a továbbfejlesztésekre és új verziókra.
- Biztonsági követelmények alkalmazása minden tervezési szinten, minden architektúra rétegben, ezen biztonsági funkciók tesztelése.
- A szoftvercsomagok módosításának elkerülése, illetve a változtatások szigorú felügyelete.
- Az alkalmazások személyes adatokat tartalmazó adatbázisainak biztosítása annak érdekében, hogy az ne tárolódjon harmadik országban (lehetőség szerint a Szervezet saját felügyelete alatt álló eszközök használata ezek tárolására).
- Az adatbázisok és hozzáférések titkosított tárolásáról való gondoskodás.
- A jegykezelő rendszerekben illetve levelező rendszerekben tárolt személyes adatokat tartalmazó jegyek és kérések egy évig őrizhetők meg vagy amíg más okból az adott személyes adatot törölni szükséges.
- A kritikus infrastruktúra elemeket tároló helyiség kulcsát zárható helyen szükséges tárolni és kulcsfelvételi jegyzőkönyv vezetése szükséges.
- A szerverszoba biztonságát minden külső környezeti és illetéktelen behatás ellen védeni szükséges (pl: zárható rack szekrény alkalmazása).
- Amennyiben szükséges éles adatokkal tesztelni az fejlesztési elemeket, azt minden esetben csak a Szervezet alkalmazottja végezheti, a fejlesztő útmutatása vagy a korábbi gyakorlat alapján.

7.2 Védelem a rosszindulatú szoftverek ellen

7.2.1 Intézkedések a rosszindulatú szoftverek ellen

A Szervezet minden munkaállomása rendelkezik anti-vírus szoftverrel.

- A vírusvédelmi rendszert ki kell terjeszteni minden olyan eszközre, amire a vírustámadás értelmezhető (céges mobil eszközökre is).
- A vírusvédelemnek ellenőrzés alatt kell tartania a mobil adathordozókat is.
- Az elektronikus üzenetküldő rendszerekben és azok kliens oldali alkalmazásaiban is működtetni kell a vírusvédelmet.
- A vírusvédelemnek az úgynevezett Spyware és Malware fenyegetések ellen is védelmet kell biztosítania.

- A vírusvédelmi rendszer által használt adatbázisokat rendszeresen, a gyártó biztosította gyakorisággal, de legalább hetente frissíteni kell
- A rendszernek tájékoztatást kell adnia a frissítések sikerességéről, a vírus észlelésekről valamint a megtett automatikus ellenlépésekről.
- A notebookokat és más mobil eszközöket úgy kell beállítani, hogy a frissítések a Szervezet rendszerén kívül is megtörténjenek kellő gyakorisággal.
- . Jóváhagyott anti-vírus szoftver nélkül privát eszközzel a munkavégzést megkezdeni tilos.

A vírusvédelem működési paramétereit minden érintett eszközre kötelező érvénnyel kell beállítani úgy, hogy az kellő biztonság mellett a munkavégzést ne akadályozza. Jelszóval kell gátolni ezen beállításoknak a felhasználók általi indokolatlan megváltoztatását.

A monitorozás során a rendszer működőképességének ellenőrzésén túlmenően

- figyelni kell a frissítések megtörténtét a felhasználói gépeken,
- a munkatársak által használt gépeken a frissítési hibákat mielőbb ki kell javítani,
- oda kell figyelni a rendszer ellenőrzése alól kiesett eszközökre, az okot tisztázni kell,
- figyelni kell a nagyszámú vírus észlelésekre és tisztázni kell az okokat.

A vírusvédelmi rendszer logjait a rendszerben kell gyűjteni, és legalább egy hónapig meg kell őrizni.

7.3 Biztonsági mentés

A Szervezet munkatársai a használt dokumentumokat O365 rendszerben tárolja, így külön biztonsági mentéseket nem készítenek. Mivel dedikált biztonsági másolat nem készül, így az ideiglenes a laptopokon és PC-ken tárolt információkat köteles minden munkatárs és külső partner a központi felhő szolgáltatás megfelelő könyvtárába menteni.
A munkatársak által használt kliensekről és privát anyagairól biztonsági mentés nem készül.
A Szervezet által használt számlázó program (Infomatrix számlázó modul) adatbázisáról legalább havi rendszerességgel szükséges biztonsági mentést készíteni.

7.4 Naplózás és megfigyelés

7.4.1 Eseménynaplózás

A felhasználói tevékenységeket, kivételeket, hibákat és információbiztonsági eseményeket naplózni kell a működő rendszerekben. A Szervezet által használt O365 fiókokban végzett tevékenység az alábbi fájlműveleti információkat rögzíti:

- az esemény forrása
- az esemény azonosítója, vagy egyértelműen azonosítható megnevezése
- az esemény időpontja,
- az esemény helye, ha értelmezhető és azonosítható

- az eseményben felhasználók azonosítja.

Egyéb naplózási tevékenységet a Szervezet nem végez.

7.4.2 Naplóinformációk védelme

A naplóinformációkat meg kell védeni a sérülésektől és a manipulációktól, annak érdekében, hogy az információbiztonsági események kivizsgálásakor bizonyítékként szolgálhassanak.

A naplóinformációkat a munkatársak által használt számítógépek tárolják, a Szervezet által használt felhő tárhelyben pedig a rendszer üzemeltetői őrzik.

7.4.3 Adminisztrátori és operátori naplók

A naplóinformációt gyűjtő rendszer beállításainak egyúttal biztosítaniuk kell a rendszergazdai tevékenységének logolását is.

7.5 Az üzemelő szoftverek védelme

Biztosítani kell, hogy csak alaposan tesztelt szoftverek, egymással hibátlanul együttműködő szoftver csomagok kerüljenek telepítésre.

Biztosítani kell, hogy a szoftver ne tartalmazzon fejlesztési kódokat, fordítóprogramokat, hanem csak végleges jóváhagyott végrehajtható kódokat tartalmazzon.

Biztosítani kell a szoftverekhez a gyártói támogatás rendelkezésre állását. Az Informatika felelőssége legalább fél évvel a lejárat előtt értesíteni a Szervezetet.

Ezen követelmények teljesítése érdekében

- A munkaállomáson és mobilszámítógépeken a Szervezetnél előírt érvényes szoftvert kell használni.
- A tesztelt, telepíthető szoftvereket a Szervezet Ellenőrzött Szoftverkatalógusában kell elhelyezni, és nyilván kell tartani.

- A gyártói támogatással már nem rendelkező elavult szoftvereket mielőbb le kell cserélni, vagy frissíteni kell.

7.6 A műszaki sebezhetőségek felügyelete

7.6.1 Műszaki sebezhetőségek felügyelete

A műszaki sebezhetőségek ellenőrzés alatt tartása érdekében, a rendszerek műszaki sebezhetőségeit jelentős késedelem nélkül, tervszerűen és ellenőrzött módon ki kell javítani a gyártók által biztosított frissítések, patchek, megkerülő megoldások használatával. Az

erről történő gondoskodás az Informatika felelőssége és az Informatika feladata. A javítások beszerzésére, tesztelésére és telepítésére vonatkozóan az alábbi alapvető követelményeknek kell megfelelni.

- Az IT szolgáltatásokat biztosító kiszolgálókon és hálózati elemeken minden javítás telepítését az üzleti igényekhez igazodva, a lehetséges teljesítmény csökkenés és szolgáltatás kiesés kockázatára figyelemmel csak a rendelkezésre álló javítás megfelelőségének gondos ellenőrzése után, megtervezett módon, ütemezetten szabad és kell végrehajtani, úgy, hogy közben biztosítják a javítás előtti állapotra történő azonnali visszaállás lehetőségét.

- A Windows alapú munkaállomásokra az új, stabil verziójú frissítéseket telepíteni kell.

- A BIOS/ROM/FIRMWARE jellegű frissítéseket csak abban esetben kell telepíteni, ha azok üzleti szempontból lényeges hibák vagy sérülékenységek kijavítását, funkció bővítést eredményeznek.

- A Szervezet által használt számítógépek dedikált UTP portokhoz tartoznak, így külső számítógépek hálózati csatlakoztatása nem lehetséges.

Amennyiben olyan sebezhetőség kerül nyilvánosságra, amely súlyosan veszélyezteti az üzemelő rendszerek biztonságát, akkor az Informatika sürgősségi javítást rendel el, amit késedelem nélkül végre kell hajtani.

7.6.2 Korlátozások a szoftvertelepítésre

Nem jogtiszta szoftver telepítése és alkalmazása minden körülmények között tilos.

A Szervezet munkaállomásokra az operációs rendszer és a munkaköröknek/felhasználási módnak megfelelő alkalmazás csomag, valamint a megfelelő biztonsági beállítások telepítése az egységes szoftver katalógus segítségével történik.

A Szervezet munkatársai nem rendelkeznek local admin jogosultsággal, így csak a Rendszergazda képes telepítéseket futtatni.

Azon területeken, beosztásokban, ahol a munkafeladatok ellátása ezt elengedhetetlenné teszi, ott az Ügyvezető Igazgató külön engedélye alapján megengedett, a Szoftver Katalógustól eltérő, egyedi software környezet kialakítása, például más, vagy többféle operációs rendszer alkalmazása. Az ilyen eltérő szoftver környezet használatát csak abban jártas, megfelelően szakképzett munkatársak részére lehet megengedni. Ezen munkatársak maguk felelősek az általuk használt szoftver csomag biztonságos üzemeltetéséért.

7.7 Az információs rendszerek auditálásával kapcsolatos megfontolások

A Szervezet valamennyi területét belső auditok formájában rendszeresen felül kell vizsgálni annak érdekében, hogy megfeleljenek a biztonsági szabályzatoknak és szabványoknak. Ezt a felülvizsgálatot legalább éves gyakorisággal el kell végezni.

A külső auditorokkal titoktartási megállapodást kell elfogadtatni.

8. A KOMMUNIKÁCIÓ BIZTONSÁGA

8.1 A hálózatbiztonság biztosítása

8.1.1 Hálózati intézkedések

A hálózatokat úgy kell kezelni, hogy azok legyenek védettek a fenyegetésekkel szemben és legyenek biztonságosak az azokat használó rendszerek számára, beleértve a hálózatokon áthaladó információk bizalmasságának és sértetlenségének megőrzését.

Ennek megvalósítása érdekében biztosítani kell a hálózatok

- magas rendelkezésre állását
- használatának szabályozottságát és ellenőrzöttségét
- az idegen hálózatokon áthaladó információ védelmét az illetéktelen hozzáféréstől és manipulációtól,
- a saját hálózatok védelmét az idegen hálózatok felől érkező fenyegetésektől

oly módon, hogy eközben az üzletileg indokolt szolgáltatások rendelkezésre állását és elérhetőségét ne korlátozzák.
Dokumentáltan rögzítjük helyi hálózatunk topológiáját.

A hálózatok védelméről történő gondoskodás az Informatika felelőssége.

A Szervezetnél elkülönítésre került egy vendég Wi-Fi hálózat.

8.1.2 A hálózati szolgáltatások biztonsága

A Szervezet üzleti tevékenységéhez szükséges hálózati szolgáltatásokról történő gondoskodás az Informatika felelőssége. Ezeknek a szolgáltatásoknak meg kel felelniük az alábbi általános biztonsági követelményeknek.

- Annak érdekében, hogy az üzletileg kritikus szolgáltatások megfelelő biztonsággal álljanak rendelkezésre, az alapvető hálózati szolgáltatásokat biztosító műszaki rendszereket magas rendelkezésre állással hibatűrő módon, redundánsan kell megvalósítani mind a külső szolgáltatók oldaláról, mind a Szervezet rendszereiben.

- A hálózati szolgáltatások biztonságos működését folyamatosan monitorozni kell, az eseményeket és incidenseket kezelni kell a szokásos incidenskezelési folyamaton át.

- A hálózati szolgáltatásokra irányuló külső vagy belső eredetű támadások ellen védekezni kell, a támadásokat fel kell ismerni és el kell hárítani. Az ehhez szükséges rendszereket magas rendelkezésre állással kell megvalósítani.

- A hálózati szolgáltatásokat úgy kell megvalósítani, hogy azok használatát figyelemmel lehessen kísérni, és az információbiztonsági incidensek sikeres kivizsgálásához szükséges bizonyítékok biztosan rendelkezésre álljanak.

8.2 Mobil eszközök és távmunka

8.2.1 Szabály Mobil eszközökre

A munkavállaló részére használatba adott információ feldolgozó, továbbító és tároló eszközök (például számítógép (laptop, notebook), telefon, mobil telefon, stb.) valamint a mobil eszközökre biztosított informatikai szolgáltatások (például szoftver-alkalmazások, internet elérés, elektronikus üzenetküldés) a munkáltató tulajdonát képezik, annak felügyelete, ellenőrzése alatt állnak. Ezen rendszereket csak a munkavégzésre, a munkavégzés hatékonyságának javítására engedélyezett használni.

- A munkáltató által a munkavállalónak biztosított mobil eszközt dokumentált átadás-átvételben kell rögzíteni.

- A rendelkezésre bocsátott informatikai infrastruktúrát a munkavállalónak rendeltetésszerűen kell használnia hardverek, mobil eszközökhöz biztosított szoftverek és szolgáltatások tekintetében egyaránt. A munkavállaló felelős az általa okozott károkat megtéríteni.

- Szigorúan tilos az információ feldolgozó rendszereket és hálózati szolgáltatásokat bármilyen jogsértő, vagy a Szervezet jó hírnevét veszélyeztető tevékenységre használni, azokon jogsértő vagy etikátlan tartalmakat tárolni továbbítani, vagy sokszorosítani. Tilos bármely jogszabályba ütköző tevékenységre bátorítás, bujtogatás, vagy akár csak ilyen tevékenységgel való egyetértés kifejezése.

- Szigorúan tilos adatok, információk jogosulatlan megszerzésére irányuló tevékenység, vagy annak kísérlete, üzleti, szolgálati titkok, vagy személyes adatok nyilvánosságra hozatala, más személy, vagy szervezet számítógépes szoftver vagy hardver elektronikus kommunikációja biztonsági rendszerének feltörése vagy annak kísérlete, tekintet nélkül arra, hogy a behatolás vagy a kísérlet adatok károsodását, adatvesztést, vagy más kárt okoz.

- A munkavállalónak tilos magáncélú eszközeit a munkahelyi számítógéphez vagy a Szervezeti hálózathoz csatlakoztatnia. Ez alól kivételt képez a Szervezeti levelező rendszer, amelyet csak úgy lehet mobil eszközre telepíteni, ha a készülék feloldásához és a rendszerbe való belépéshez jelszó szükséges.

- Tilos a munkahelyen engedély nélkül kép vagy hangfelvételt készíteni.

- Ha a munkát bármilyen okból, bármilyen rövid időre is megszakítja, vagy befejezi, köteles a számítógépet kikapcsolni vagy zárolni, az iratokat elzárni (Clear desk elv).

- Az Informatika kötelessége minden visszavett eszközön tárolt privát adatokat teljes formázással törölni mielőtt új Munkatársnak adják ki

- A munkavállaló privát vagy a Szervezet által biztosított mobileszközein a kapcsolatokat csak a Szervezet által biztosított Exchange/Google/Apple fiókhoz szabad csatolni.

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.

- A munka befejeztekor a mobil eszközt ki kell kapcsolni. Tilos a mobil eszközt 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, felhő alapú tároló eszközökön kell elhelyezni.

- Informatikai eszközök, adathordozók elvesztését, ellopását, megrongálódását haladéktalanul jelenteni kell a Informatikának és az Adatvédelemért felelős megbízottnek.

- 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 helyen legyen.

- Az informatikai eszközökhöz veszélyes közelségben tilos veszélyes tárgyakat elhelyezni, például vázák, virágcserepek, akvárium, hősugárzó, mágnes stb.

- A távoli hozzáférést (VPN) biztosító tanúsítvány fájlok átadása és nem céges mobil eszközön történő tárolása szigorúan TILOS!

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, erős mágneses hatástól, erős rázkódástól.

- Repülőgépen a kézipoggyászban kell szállítani.

- Szállítás közben a számítógépnek teljesen kikapcsolt állapotban kell lennie, szigorúan tilos hibernált vagy alvó állapotban szállítani a számítógépet!

- Gépkocsival történő szállítás esetén a zárt/fedett csomagtartóban kell elhelyezni, a jármű elhagyásakor magával kell vinnie. A számítógépet és adathordozókat TILOS (még rövid időre is) az autóban hagyni!

- Szállítás előtt mindig bizonyosodjon meg róla, hogy minden külső tartozékot becsomagolt, (pl. tápegység!)

Mobil eszközök védelme a telephelyen kívüli használat közben

- Ha a készülék a szállítás során túlzottan lehűlt, vagy felforrósodott, használat előtt meg kell várni amíg szobahőmérsékletre kerül.

- Használat közben óvni kell az erős napsugárzástól, portól, nedvességtől, erős rázkódástól.

- Különösen külföldön az elektromos hálózatra történő csatlakozás előtt győződjön meg róla, hogy a hálózat megfelel a készülékére megengedett értékhatároknak.

- Telephelyen kívül lehetőleg soha ne hagyja felügyelet nélkül a mobil eszközöket. Ha ez nem lehetséges, mindig kapcsolja ki.

- A mobil eszközök telephelyen kívüli használatával kapcsolatban a távmunkavégzés szabályai érvényesek.

- Tilos a mobil eszközök használatát 3. feleknek átengedni, sem idegenek, sem családtagok, rokonok, ismerősök nem használhatják ezeket.

Mobil eszközök használata nyilvános helyen

A mobil eszközök, mint például laptopok, tablet PC – k, USB memóriakártyák használata nagyobb kockázatot hordoz, mint a helyhez kötött desktop PC-k használata, hiszen ezek a Szervezet védett területén kívül is használhatók. Az említett kockázatok mind az eszközök elvesztése, mind a rajtuk tárolt információ elvesztése szempontjából fennállnak. A Szervezet ugyanakkor kárt szenvedhet az információ jogosulatlan hozzáférése vagy az eszközök nem megfelelő használata miatt is. Ezen kockázatok minimalizálása érdekében a következő szabályok betartása kötelező:

- A mobil eszköz védelmének biztosításáért, valamint a rajta tárolt információ megfelelő feldolgozásáért (beleértve az adatmédiát és az eszközhöz való hozzáférést) annak használója a felelős.

- A mobil eszköz használója köteles különös figyelmet fordítani arra, hogy az eszköz ne kerülhessen harmadik fél kezébe. Ne hagyjuk felügyelet nélkül gépjárműben, vonaton, repülőgépen, hajón; és biztosítsunk megfelelő védelmet hotelekben és konferenciákon, hogy az eszközt ne lophassák el.

- Csak akkor kerül információ tárolásra mobil eszközökön, ha az okvetlenül szükséges és az eszköz titkosított

- Az óvintézkedések magukban foglalják a mobil eszközök hálózati elérésének és rajtuk futtatott alkalmazások védelmét a harmadik személyek általi eléréstől. Emiatt ne tároljuk az authentikációs eszközöket PIN kóddal, vagy bármely olyan információval együtt, ami az azonosításukat biztosítja.

- A jelszavaknak meg kell felelniük a ”Minőségi Jelszó” részben leírtaknak.

- Mobil eszközök nem használhatóak szimultán módon több hálózat (pl. védett VPN és publikus internet egyszerre) elérésére.

  Amennyiben nyilvános helyen használjuk a mobil eszközt (pld. hotel előcsarnok, internet kávéház, vonaton, hajón) jogosulatlan személyek belső céges információhoz férhetnek hozzá. Tilos ingyenes és olyan WIFI hálózathoz csatlakozni, amelynek a forrása ismeretlen (pl: a szállodákban csak az a szálloda által biztosított és kellő azonosítással ellátott hálózatok használata engedélyezett)

- Tilos a saját mobil eszközzel ingyenes hot spotként megosztani internetet! A saját mobil eszköz hot spot védettségét biztosító jelszó elvárásait a Jelszókezelési szabályzatban foglaltaknak megfelelően kell beállítani.

- Céges adatok elérése csak a Szervezet által rendelkezésre bocsátott eszközökkel (notebook, mobiltelefon) védett csatornán lehetséges (VPN)

8.2.2 Távmunka szabályzat

A rendszeres otthoni munkavégzés során olyan új információbiztonsági kockázatok merülnek fel, amik a normál munkahelyi környezetben hiányoznak, vagy az ott meglévő kockázatkezelő intézkedések sorának köszönhetően lényegesen kisebbek. Az lenne kívánatos, hogy az otthoni munkavégzés se legyen kockázatosabb, mint a munkahelyi. Ezeket a kockázatokat az otthoni munkahely speciális adottságainak megfelelően, a meglévő adottságok és a reális lehetőségek határain belül kezelni kell. Ez a szabályzat ezen kockázatok kezelése, a kockázatok elfogadható szintre csökkentése érdekében készült.

A szabályzat hatóköre: A Szervezet minden otthoni munkavégzést engedélyező és végző munkatársára érvényes.

Az engedélyezés biztonsági szempontjai

Az otthoni munkavégzést a munkavállaló számára kizárólag az Ügyvezető Igazgató engedélyezi. Az engedélyezés során megfontolás tárgyává kell tenni, hogy a munkavállaló

- személyisége,
- fegyelmezettsége,
- információbiztonsági tudatossága.

alkalmasak-e az otthoni munkavégzéssel járó kockázatok kezelésére.

Az engedély csak akkor adható meg, ha az otthoni munkavégzésre vonatkozó információbiztonsági szabályok betartásához szükséges feltételek rendelkezésre állnak.

A munkavégzés engedélyezéséhez kapcsolódóan minden esetben meg kell határozni,

- hogy a munkavállaló milyen munkafeladatokat végezhet el az otthoni munkahelyen,
- milyen egyébként a munkakörébe tartozó munkafeladatokat kifejezetten TILOS az otthoni munkahelyen végezni,
- milyen információkat (ezeket tartalmazó adathordozókat) szállíthat, tárolhat az otthoni munkahelyen.

A döntésnél figyelembe kell venni

- a kezelt információk bizalmasságát, az információ kiszivárgás kockázatát
- a kezelt információ rendelkezésre állásának kritikusságát (adatvesztés)
- az ügyfél szerződésekből és kapcsolódó jogszabályokból adódó korlátozásokat (jogi következmények)

Üzletileg indokolt esetben az otthoni munkavégzést engedélyező vezető saját felelősségére engedélyezheti az eltérést a jelen szabályzatban megadott követelményektől. Az eltérési engedélyt minden esetben írásba kell kiadni.

A számítógép védelme

Az otthoni munkaeszköz kizárólag a Szervezet által biztosított számítógép illetve RDS hozzáférés lehet.

Az otthoni munkavégzéshez a munkavállaló részére az

- otthoni munkavégzés körülményeihez
    - méretében,
    - energia fogyasztásában,
    - környezetállóságában alkalmas eszközt kell biztosítani.

Az eszköznek az alábbi tulajdonságokkal kell rendelkeznie

- a fokozott biztonsági fenyegetések ellen kellően védett, azaz
    - titkosított adathordozóval ellátott, melyhez a hardware kulcsot vagy a PIN kódot a Szervezet rendelkezésre bocsájtja
    - a hálózaton titkosítva kommunikáló, a Szervezeti hálózathoz VPN-en át kapcsolódó
    - automatikusan frissülő vírusvédelemmel ellátott
    - a képernyőt automatikusan lezáró kell legyen.

- a Szervezet informatikai rendszerében felügyelt, azaz
    - a biztonsági házirendek érvényesíthetőek, és nem megkerülhetők,
    - a szoftver frissítések felügyelt módon telepíthetők
    - a fontos biztonsági események logoltak, és gyűjtöttek,
    - a kezelt dokumentumok tárolása a központi tároló eszközökkel megoldott.

Az otthoni munkavégzésre alkalmas és a fenti követelményeknek megfelelő munkaeszköz biztosítása a munkáltató feladata.

A munkavállaló felelős az otthoni munkavégzésre használt eszközt felügyelete alatt tartani, annak biztonságosságáról folyamatosan gondoskodni éppen úgy, mint a telephelyen használt eszközök esetében.

- A munkavállaló felelős a Szervezeti eszközökben esett károkat megtéríteni. A levonás összege a dolgozó következő havi munkabéréből kerül rendezésre. Ha a fizetésének 50%-át meghaladja a levonandó összeg, akkor részletekben kell teljesíteni. Amennyiben az okozott kár miatt az eszköz használhatatlanná válik, a dolgozó a bejelentés napján nyilvántartott könyv szerinti értéket köteles a munkáltató számára megtéríteni.
- Amennyiben az eszköz alkatrészeinek cseréjével megjavítható, az esetben az alkatrész(ek) és a javítás munkadíját köteles megtéríteni a munkáltató részére. A fizetendő összeget a javítás számlájával igazolja a munkáltató.

Az Internet kapcsolat védelme

Az otthoni munkahelynek saját internet kapcsolattal kell rendelkeznie, aminek a megosztását a munkavállaló ellenőrzése alatt tartja. Az otthoni internet megosztás során a router, tűzfal, és/vagy a WIFI biztonságos beállítása a munkavállaló felelőssége az eszközök gyártó által biztosított felhasználói kézikönyvei alapján:

- Az eszközök gyári jelszavait (alapbeállítás) meg kell változtatni.
- A jelszavaknak meg kell felelniük a Szervezet jelszó használati szabályozásában előírt minőségi követelményeknek.
- A routerben a tűzfal funkciót be kell kapcsolni, ha van .
- A router adminisztrációját le kell tiltani a WAN oldalon, és ha lehetséges a WIFI oldalon is.

- A WIFI-n wpa2 titkosítást kell beállítani.
- A saját tulajdonú router/tűzfal/WIFI eszköz(ök)-höz elérhető gyártói szoftver-frissítéseket rendszeresen telepíteni kell. Legalább negyedévente ellenőrizze, hogy van-e frissített szoftver az eszközhöz. Ehhez segítséget talál a használati utasításban és a gyártó honlapján. Csak a gyártó által támogatott, jóváhagyott frissítéseket telepítsen.
- A munkavégzés az esetben kezdhető meg, amint a munkatárs a VPN kapcsolatot felépítette. Az internetkapcsolat automatikusan korlátozva van mindaddig, amíg a VPN hálózat nincs felépítve.
- Bármilyen változtatást jelezni kell azonnali hatállyal az Informatikának.

Fizikai Biztonsági intézkedések, szabályok

Az ezen pont alatt felsorolt, az otthoni munkahely információbiztonsági kockázatainak csökkentését szolgáló szabályok betartása és a kapcsolódó feltételek biztosítása minden esetben a munkavállaló felelőssége és feladata. Az ezzel kapcsolatos kiadások, ha erről másként nem állapodnak meg, a munkavállalót terhelik.

Az otthoni munkahelyen a betörés és lopás veszélye fokozottan jelen van, mivel a portaszolgálat, a biztonsági őrség, és az elektronikus beléptető rendszer általában nem áll rendelkezésre. Az ebből adódó kockázatok csökkentése érdekében az alábbi követelményeket kell teljesíteni:

-

-
    - a dolgozó munkája során nem használ papír alapú bizalmas dokumentumokat vagy adathordozókat,
    - nem vesz részt olyan telefonkonferencián, ahol bizalmas információk elhangzanak.

- Amennyiben a munkavégzéshez bizalmas információt tartalmazó adathordozók, vagy papír alapú dokumentumok kezelése szükséges, akkor ezek védelme érdekében a szobában egy kulccsal zárható szekrénynek vagy fióknak kell lennie, amihez másoknak nem lehet kulcsuk.

- Az épületnek meg kell felelnie a lakóépületekre vonatkozó tűz és villámcsapás elleni védelmi szabályoknak.

- A lakás áramellátása legyen üzembiztos és feleljen meg az érintésvédelmi szabályoknak.

- A munkahely áramellátását (áram elosztást) úgy kell megoldani, hogy azt munkavégzés közben mások ne szakíthassák meg, kerülni kell az elosztók sorba kötését.

- Az eszközöket olyan stabil védett helyen kell elhelyezni, hogy a használat, vagy a takarítás során azok ne essenek le és nedvesség ne érje őket.

Viselkedési szabályok az otthoni munkahelyen

Az otthoni környezet sok esetben gyorsabb, koncentráltabb, ezáltal hatékonyabb munkavégzésre ad lehetőséget, mint egy közös nagy irodatér. Ugyanakkor az otthoni környezetben újfajta, az irodában megszokottól eltérő zavaró tényezőkkel, esetenként információbiztonsági kockázatokkal találkozunk. A családtagok, látogatók nem is lehetnek tisztában azzal, hogy valamilyen viselkedésükkel információ-biztonsági kockázatot okoznak.

Minden a családtagok vagy látogatók okozta információbiztonsági incidensért a munkavállaló a felelős.

Ha ezekre a váratlan helyzetekre tudatosan felkészülünk, akkor a családtagok és látogatók tiszteletben tartása mellett is képesek leszünk biztonságosan és hatékonyan dolgozni az otthoni irodában. Ebben adunk segítséget az alábbi szabályok megfogalmazásával.

- A munkavállaló tudatosítsa a közvetlen környezetének tagjaiban,
    - hogy Ő otthon a környezetükben fog dolgozni, és ez kényelmetlenséget okozhat nekik, vagy korlátozhatja őket valamilyen megszokott tevékenységükben,
    - a munkavégzéshez használt eszköz munkaeszköz, azt illetéktelen személy nem használhatja, erre fokozottan ügyelni kell, mert az esetlegesen okozott károkért a dolgozó felel.

- A munkavállaló tágabb környezetével szemben kezelje bizalmasan az otthoni munkavégzést, és erre kérje meg a közvetlen környezetének tagjait is.

- A munkavégzés közben abban a helyiségben, ahol a munkavégzés folyik a Szervezet munkatársainak kivételével mások nem tartózkodhatnak.

- Annak a helyiségnek az ajtaját, ahol a munkavégzés folyik lehetőleg zárva kell tartani.

- A képernyőt úgy kell elhelyezni, hogy azt az ablakokból és a lakás többi részéből se lehessen leolvasni.

- Ha a helyiség ajtaja nem biztosít elegendő hangszigetelést, hogy mások a telefonbeszélgetéseket vagy hang üzeneteket ne hallják, akkor tilos a telefont kihangosítani, és a számítógépet fejhallgatóval kell használni.

- A munkavégzés váratlan megszakításakor, ha az eszközök és adathordozók elzárására nincs idő, akkor a szobát kulcsra kell zárni.

- A munkavégzés befejeztével a belső használatú adathordozókat, iratokat a zárható szekrényben kell elzárni. Ha megoldható, akkor a notebookot is a célszerű a szekrényben elzárni.

- Az otthoni munkahelyen fokozottan figyelni kell az adathordozók összecserélésének a veszélyére, ezért a munkához használt adathordozókat egyértelműen meg kell jelölni, és a személyes adathordozóktól jól elkülönítve kell használni.
- Tilos személyes használatú eszközöket (például otthoni számítógép, adattároló, audio/video berendezés, játék konzol) a Szervezeti számítógéppel összekapcsolni, kivétel a router/wifi.

- Tilos adatokat a személyes használatú eszközökre (számítógépekre, adathordozókra, egyéb mobil eszközökre) átmásolni.

- Tilos a képernyőről fényképet készíteni. Ügyeljen rá, hogy a helységben munkavégzés közben ne készülhessen fényképfelvétel, amin a képernyő akár csak részben is látszik.

- Elhasználódott, meghibásodott, felesleges adathordozót (iratot) TILOS otthon kidobni! Minden esetben a munkahelyre visszaszállítva kell azokat szakszerűen megsemmisíteni.

- A helyiség takarításának idejére a munkavégzést be kell fejezni, az eszközöket el kell zárni.

- Ha a munkavégzés elkülönített, bizalmas jellege valamilyen okból, például családi esemény következtében tovább nem biztosítható, a munkavégzést meg kell szakítani, és fel kell függeszteni, amíg a körülmények ismét alkalmasak lesznek. Természetesen ilyenkor is mindent el kell zárni a szokott módon.

8.3 Információ átvitel

A Szervezet elektronikus üzenetküldő rendszerének használatának szabályozása. A szabályzat meghatározza az elfogadható és helyes használatot, a használat során betartandó információbiztonsági szabályokat, és a használattal kapcsolatos feladatokat és felelősségeket.

A szabályozás kiterjed a Szervezet minden munkavállalójára, valamint mindazon külső személyekre, akik a Szervezet elektronikus üzenetküldő rendszerének használatára engedélyt kaptak.

A levelezőrendszerben lévőinformációkat szükséges csoportokba rendezni (email könyvtárstruktúra), hogy a megőrzési időket könnyebben tudják nyomon követni a munkatársak.

8.3.1 Szabályok és eljárások az információátvitelre

Az üzenetküldő szolgáltatások a Szervezet által a felhasználók részére privát eszközökön keresztül is elérhetőek. A felhasználónak biztosítania kell, hogy minden egyes bejelentkezés alkalmával (a Szervezet levelező rendszerbe) jelszóval azonosítania kell magát a privát eszközén.
A rendszer, valamint a rendszerben előállított, elküldött, továbbított, megkapott, tárolt vagy archivált üzenet a Szervezet felügyelete alatt áll, ezeket a Szervezet monitorozhatja, és tartalmába indokolt esetben szorosan a célhoz kötött módon betekinthet. Ilyen célok lehetnek: az üzletmenet folytonosság biztosítása, bizonyítékok gyűjtése információbiztonsági incidensek és fegyelmi ügyek kivizsgálásakor, valamint az erre jogszabályban feljogosított hatóságoktól érkező kérések teljesítése. A betekintés során megismert magántitok és személyes adatok kezelése csak a célhoz kötötten bizalmasan történhet.

A szolgáltatások nem használhatók személyes vagy magánjellegű üzenetváltás céljára, a Szervezet nem vállal felelősséget az ilyen tartalmú üzenetekben a személyes adatok védelméért.

A szolgáltatással mindennemű jogszabályellenes, vagy akár csak részben jogszabályba ütköző tartalom továbbítása és tárolása tilos, ideértve a szerzői jogi jogsértéseket is.

A felhasználó köteles biztosítani, hogy a tőle telhető legnagyobb diszkrécióval kezeli a Szervezeti információkat és az információbiztonsági elvek nem sérülnek a napi munkavégzés során, például amikor nem oldható meg egy megbeszélésen a prezentálás kiterjesztett képernyő segítségével, ki kell kapcsolnia az elektronikus üzenetküldő alkalmazást.

Elektronikus levelek továbbítása esetén fontos ügyelni arra is, hogy ne juttassunk át személyes adatot olyan felek között, akik nincsenek kapcsolatban egymással.

A levelezésben lévő különösen szenzitív csatolmányokat szükséges jelszavas védelemmel ellátni, illetve a csatolmány megnyitásához tartozó jelszót egy másik csatornán (pl.: SMS) eljuttatni a fogadó félhez.

Az elektronikus üzenetküldő rendszer használata során nem megengedett:
- indokolatlanul nagy mennyiségű és méretű üzenetek küldése;
- reklámok és hirdetések közzététele;
- lánclevelek terjesztése, továbbítása;
- olyan üzenetek, illetve csatolt fájlok küldése, továbbítása, amelyek bármely módon történő jogszabálysértést vagy arra való felhívást tartalmaznak, sértik a Szervezet jó hírét.

8.3.2 Megállapodások az információátvitelre

A Szervezet minden tőle elvárható intézkedést megtesz az e-mail szolgáltatás megbízható és biztonságos üzemeltetése érdekében, de nem tud felelősséget vállalni egy üzenet elvesztése, késedelmes vagy hibás továbbítása okozta károkért. Ezért minden felhasználó köteles a kritikus fontosságú üzeneteinek célba érkezéséről magának meggyőződni. Erre a célra használható az olvasás visszaigazolás funkció, vagy szóbeli érdeklődés.

A felhasználó tudomásul kell vegye, hogy a Szervezetnek nem áll módjában a hálózatának határain túl az elküldött üzenetek továbbításának útvonalát felügyelet alatt tartani, azok biztonságáról gondoskodni. Ezért tilos az e-mail rendszeren át olyan tartalmú üzenetek küldése, amiknek a megengedett továbbítási útvonalát törvényi rendelkezés, szerződéses kötelezettség, vagy belső utasítás előírja vagy korlátozza.
Az e-mail szolgáltatás során történő jelszó használatra is a Szervezet Jelszókezelési Szabályzatában megadott jelszóhasználati szabályok vonatkoznak.

Az e-mail rendszerben tárolt és továbbított dokumentumok kezelésénél is be kell tartani az érvényben lévő Iratkezelési szabályzatban leírtakat.

8.3.3 Elektronikus üzenetküldés

A Szervezet nevében folytatott üzenetváltásban kizárólag az erre a célra biztosított elektronikus levelezési cím, a felhasználónak engedélyezett szolgáltatás használható. Más szervezet vagy szolgáltató által biztosított e-mail szolgáltatás üzleti céllal nem használható.

A felhasználó tudomásul kell vegye, hogy a leveleinek feladója, címzettje, és tárgya a technikai üzemeltetés során az üzemeltető személyzet részére látható lehet.

A felhasználó tudomásul kell vegye, hogy a munkaviszony megszűnése esetén a postafiókja a munkahelyi vezetője kérelme alapján archiválható, az abban található üzenetek az üzletmenet zökkenőmentes folytatása érdekében felhasználhatóak.

Minden esetben tiltott

- A Szervezet által biztosított e-mail címre érkező üzenetek átirányítása külső e-mail címre.
- a nem Szervezethez tartozó e-mail címre érkező üzenetek átirányítása a Szervezethez tartozó e-mail címekre.
- Ezen általános tiltások alól kivételes esetekben fontos üzleti érdekből az Ügyvezető Igazgató adhat felhatalmazást.
- A csatolmányokat lehetőség szerint titkosítani vagy jelszóval ellátni szükséges és a feloldáshoz használt jelszót egy másik csatornán kell eljuttatni a fogadó félhez.
- Emailek Szervezeten kívüli továbbítása során a beszélgetés előzményeit törölni kell.
- VoIP alapú megoldások céges használata TILOS!

8.3.4 Bizalmassági vagy titoktartási megállapodások

Az általános információkezelési eljárásoknak megfelelően bizalmas információt e-mailben vagy annak csatolmányában lehetőség szerint titkosított módon szabad küldeni.

Bizalmas információt tartalmazó e-mailt vagy e-mailben kapott csatolmányt tilos a feladó kifejezett beleegyezése nélkül továbbítani.

Bizalmas információt tartalmazó üzenetet tilos levelezési listára küldeni.

Az információk kiszivárgása ellen védekezni kell. A védekezés elsődlegesen jelen szabályzat más pontjaiban felsorolt technikai intézkedések megvalósítása és viselkedési szabályok betartása révén valósul meg. Az információk kiszivárgását legjobban a munkatársak információbiztonság tudatos viselkedése akadályozhatja meg.

Minden munkatárs kötelessége, hogy a tudomására jutott, vagy a környezetében észlelt esetekben, az információbiztonságot veszélyeztető módon tevékenykedő, vagy viselkedő munkatársát figyelmeztesse, az esetet jelentse az Informatikának vagy az Ügyvezető Igazgatónak.

Az információk kiszivárgása elleni védekezés érdekében a személyzet oktatásában tárgyalni kell az információbiztonsági fenyegetések aktuális trendjének témaköreit

- az információbiztonság tudatos általános viselkedési szabályok
- lehallgatás elleni védekezés
- social engineering elleni védekezés
- megtévesztés, félrevezetés elleni védekezés

A technikai védekezés keretében az alábbi megoldásokat alkalmazzuk.

- A munkaállomásokon és mobil számítógépeken a rosszindulatú kódok elleni védelem része a bújtatott csatornákon át információt kiszivárogtató kém és trójai programok elleni védelem.
- Az információknak a mobil adathordozókon, faxon, email-ben, telefonon, vagy beszédben történő kiszivárgása ellen az információkezelési szabályokban megadott módon védekezünk. A védelem erősítését oktatásokkal és ismeret frissítésekkel valósítjuk meg.
- Az asztali és mobil munkaállomásokon a mobil adathordozók ellenőrizetlen használatát korlátozó műszaki megoldásokat alkalmazunk.

9. RENDSZEREK BESZERZÉSE, FEJLESZTÉSE ÉS KARBANTARTÁSA

9.1 Az információs rendszerek biztonsági követelményei

9.1.1 Információbiztonsági követelmények elemzése és meghatározása

Új információfeldolgozó és továbbító rendszerek
- beszerzése
- tervezése
- létrehozása
- vagy meglévő rendszerek átalakítása

előtt meg kell határozni az
- információbiztonsági
- és az üzletmenet folytonossági

követelményeket.

Meg kell határozni a követelmények teljesítéséhez szükséges, a projektben megvalósítandó/elérendő
- műszaki/technikai jellemzőket,
- az üzemeltetéshez szükséges személyi és technikai feltételeket,
- a fejlesztés/megvalósítás egyes szakaszaiban elvégzendő biztonsági átvizsgálásokat és elfogadási kritériumokat,
- a GDPR által támasztott beépített és alapértelmezett alapelvet,
- a beszerzések során alkalmazandó kiválasztási és elfogadási kritériumokat.

A projekt tervezése és megvalósítása során az vezetőség konzultál az Informatikával.

A követelmények meghatározásához fel kell használni az egyéb Szabályzatokban meghatározott követelményeket,

9.2 Biztonság a fejlesztési és támogatási folyamatokban

9.2.1 Rendszerek változásfelügyeleti eljárásai

A Szervezet változásfelügyeleti eljárása során a rendszer működésével kapcsolatos változások nyomon követése a cél, aminek alapját a fejlesztést és üzemeltetést nyomon követő rendszerben történő lista képzi. A változások alapvető célja, hogy a felhasználók által érzett működésre és minőségre minimális hatást gyakoroljon.

9.2.2 Az alkalmazások műszaki vizsgálata a működtető környezet változásai után

A működési környezet megváltoztatása során az üzletkritikus alkalmazások teljes körűen átvizsgálásra és tesztelésre kerülnek annak érdekében, hogy annak ne legyen kedvezőtlen hatása a szolgáltatásnyújtásra.

9.2.3 Szoftvercsomagok változásainak korlátozása

A szoftvercsomagok módosításai során el kell kerülni a nagymértékű változtatást, vagy bizonyos területek módosításait korlátozni kell, és minden változtatást szigorúan monitorozni kell.

9.2.4 Biztonságos rendszerek tervezési elvei

A Szervezet alapvető működéséből eredően a biztonsági elvárások nagyon magas szintűek és minden tevékenység/fejlesztés/szolgáltatás magas szintű biztonsági alapelveknek felel meg és azokat minden tervezési és kivitelezési fázisban alkalmazza. Esetlegesen kiszervezett tevékenységek esetében ugyanezen elvárásoknak kell a kivitelezőknek megfelelni.

9.2.5 Kiszervezett fejlesztés

A Szervezetnél több külső szolgáltatást vesz igénybe, amelynek fejlesztése az adott szolgáltatóknál folyik. Az egyik legfontosabb információbiztonsági elv ilyen esetekben, hogy a külső szolgáltatók a fejlesztések során nem férhetnek hozzá valódi személyes adatokat tartalmazó adatokhoz. A támogatási tevékenység során ez néhány esetben elkerülhetetlen, ilyen esetben a támogatási tevékenység minden lépését monitorozni és logolni kell.

9.2.6 A rendszer biztonsági tesztelése

A Szervezet által működtetett informatikai rendszert bármilyen változtatás után az Informatika biztonsági tesztelésnek veti alá és ennek eredményéről feljegyzést készít.

9.2.7 A rendszer elfogadási tesztelése

A specifikáció elvárásainak teljesülését ellenőrző teszteket hozunk létre és tovább fejlesztjük az új verziók működésének ellenőrzése érdekében.

10. SZÁLLÍTÓI KAPCSOLATOK

10.1 Információbiztonság a szállítói kapcsolatokban

Az ellátási láncok minimális szinten történő működéséhez néhány alapvető Szervezeti adatot mindenképpen szükséges a többi résztvevő számára biztosítani (pl.: értékesítési adatok és előrejelzések, vevői rendelések állapota, kapacitásadatok…stb). A Szervezet által előírt belső információbiztonsági követelményekről világos, dokumentált tájékoztatást kell adni az ellátási lánc többi tagjának. A Szervezet a külső vállalkozásokkal ismerteti az Információbiztonsági Szabályzatát és a benne foglaltak szerint szabályozza a vonatozó tevékenységeket.
A vállalkozások megismerhetik egymás belső Szervezeti folyamatait, ezért a titoktartási nyilatkozat aláírása alapvető elvárás.
Amennyiben a szállítói lánc növekedésével az információbiztonsági fenyegetettség is növekszik, az esetben integrált információbiztonság irányítási rendszer kialakítása elvárt.
Az ellátási lánc információs és kommunikációs rendszerének kialakítása során törekedni kell a megbízható, alacsony költségű és csak a szükséges információk áramoltatását lehetővé tevő rendszer kialakítására.

10.2 A szállítói szolgáltatásnyújtás irányítása

10.2.1 A szállítói szolgáltatások figyelemmel kísérése és átvizsgálása

A stratégiai üzleti partnerek kiválasztásánál ma legalább olyan fontos a stabil, megbízható IT alapokon nyugvó kapcsolattartási lehetőség, mint a megvásárolt termék vagy szolgáltatás ára és minősége, valamint a leellenőrizhető referenciák megléte.
Egy információs rendszerek kölcsönös, de természetesen korlátozott használatát is megengedő üzleti kapcsolatban alapvető, a partnerekkel egyetértésben megfogalmazott elvárások a következők a Szervezet esetében:

- A titoktartási nyilatkozat elkészítése és mindkét fél által történő elfogadása.
- A fizikai beléptetés szabályozása.
- A megfelelő jogosultsági rendszer kialakítása.
- Az információ továbbítás és hordozás szabályainak megállapítása (pl. másolatok készítése, a megsemmisítés kérdése…).
- Az alárendelt szerződő partner felelősségvállalása a saját alkalmazottjaiért
- Csak a szükséges és elégséges adatok/információk biztosítása a partnerek számára.
- Az együttműködés során bekövetkezett káros események (incidensek) tapasztalatainak leszűrése, a hibaelhárítás ráfordításainak számszerűsítése és a felelősség egyértelmű megállapítása.
- Formális eljárások lefolytatása, ha valamelyik fél alkalmazottai megsértik a megállapodásokat.

- Az üzleti kapcsolat fenntartásában nélkülözhetetlen szoftverek szabályozott, írott megállapodások alapján történő átadása.
- Az elektronikus kereskedelem és levelezés biztonságának szabályozása különös tekintettel az üzleti tranzakciós adatok, ill. az üzenetek hitelességére, titkosságára és sértetlenségére.
- Az elfogadott feltételek és követelmények írásba foglalása a későbbi jogviták elkerülése miatt.

Az információbiztonsági irányítási rendszer kiépítésének célja a partnerek elvárásainak, a vonatkozó hazai és nemzetközi előírásoknak megfelelő működés és az információbiztonság megteremtése, az adatok és információk sértetlenségének, bizalmasságának megőrzése, ezek rendelkezésre állásának biztosítása. Minimalizálható legyen az esetlegesen bekövetkező üzleti kár és biztosítani tudjuk az üzletmenet-folytonosságot.

11. AZ INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE

11.1Információbiztonsági incidensek és javítások kezelése

Minden olyan
- eseményt
- emberi cselekedetet
- gépi működést

információbiztonsági eseménynek tartunk, ami az IBSZ-ben meghatározott
- alapelvek,
- célok,
- szabályok

megvalósítását, érvényesülését, vagy betartását
- megsérti, vagy
- közvetlenül fenyegeti

függetlenül az
- elkerülhetetlen
- véletlen, vagy
- szándékos

jellegétől.

Példák információbiztonsági eseményekre:
- Rendelkezésre állás sérülésére utaló események
  - IT eszköz meghibásodása
  - hálózati kapcsolatok megszakadása
- Sértetlenséget veszélyeztető jellemző események
  - vírustámadás
  - adatok megváltozása
- Bizalmasságot veszélyeztető jellemző események
  - illetéktelen hozzáférés
  - hálózati behatolás

11.1.1 Felelősségek és eljárások

Az információbiztonsági események kivizsgálása az Informatika feladata. Ebben a vizsgálatban felkérésre kötelesek közreműködni az üzemeltetők, és más érdekelt vezetők és kijelölt szakértők.
A vizsgálat során meg kell állapítani, hogy:
- Milyen események történtek?
- Az események milyen és mekkora kárt okoztak, illetve okozhattak?
- Milyen intézkedések szükségesek a kárelhárításhoz, illetve mérsékléshez?
- Mik voltak az események kiváltó okai, előzményei?
- Kik az eseményért közvetlenül és közvetve felelős személyek és milyen a felelősségük mértéke?
- Történt-e bűncselekmény?

A vizsgálatnak gyorsnak és lényegre törőnek kell lennie. Amennyiben visszaélés gyanúja merül fel, az érintett személytől az ügy kivizsgálásának befejezéséig jogosultságait és betekintési engedélyeit vissza kell vonni, az általa ismert jelszavakat meg kell változtatni és más további érdeksérelmet megelőző intézkedéseket kell foganatosítani. Az Informatika a kivizsgálás eredményéről írásban is tájékoztatja az ügyvezetést. A tájékoztatásban javaslatot kell tenni a felelősségre vonandó személyekre, illetve a további hasonló károk, biztonságsértések elkerülésére teendő intézkedésekre.

Amennyiben az információbiztonsági esemény a Szervezet felelősségi körén belül ügyfél rendszereket, vagy adatokat érintően történik, az Ügyvezető Igazgató kötelessége az ügyfél (vagy Szervezeti kapcsolattartójának) értesítése, azzal való együttműködés és folyamatos tájékoztatása a vizsgálat során.

11.1.2 Információbiztonsági események jelentése

A munkatársak feladatai információbiztonsági események észlelésekor:

- Minden vélt vagy valós információbiztonsági incidenst a Munkatársaknak e-mailben azonnal jelenteni kell az ilyen e-mail fogadására kijelölt Munkatársnak, aki az incidenst a megfelelő elektronikus feljegyzésben rögzíti az Informatika felé.
- A jelentésben minél pontosabban meg kell adni az esemény leírását és annak körülményeit. Az Informatika szükség szerint az Ügyvezető Igazgatóval közreműködve intézkedik az incidens kezelésére.
- A munkatársak kötelesek az intézkedő személyektől a további teendőkre vonatkozóan kapott utasításokat haladéktalanul végrehajtani.
- A bejelentő munkatársak az eseményről harmadik felet külön felhatalmazás nélkül ne értesítsenek, ne nyilatkozzanak.

Az Adatvédelemért felelős megbízott feladatai az információbiztonsági események bejelentésekor:

- rögzítsen minden a bejelentésben foglalt körülményt és eseményt;
- szükség esetén az Informatika bevonásával tevékenyen kezdeményezze az esemény okozta károk csökkentését, az esemény további kiterjedésének megakadályozását;
- az esemény jellegétől függően a bejelentést késlekedés nélkül továbbítsa/eszkalálja a megoldásra kijelölt személy felé.
- Minden olyan esetben, amikor valamilyen bűncselekményre (például lopás) vagy súlyos hanyagságra (elvesztés), vagy szándékos károkozásra utaló körülmény áll fenn, az Értesítendő Személyek működjenek együtt a bejelentővel a bizonyítékok összegyűjtése és hiteles megőrzése érdekében.
- az esemény lezárásakor küldjön visszajelzést a bejelentőnek, amiben tájékoztatja az esemény mivoltáról, az esemény kezelésének menetéről és eredményéről.

Az Ügyvezető Igazgató a felelős az egyes bejelentések prioritás szerinti kategorizálására, valamint az eszkalációs lépésekre vonatkozóan.

A rendszer üzemeltetők bejelentési kötelezettsége:

Amennyiben a rendszerüzemeltetők a monitorozó rendszertől kapott riasztások, vagy a rendszerek kezelése karbantartása során tapasztalnak vélhető vagy valós információbiztonsági vagy adatvédelmi eseményt, amely a bizalmasság vagy a sértetlenség sérülésére utal, akkor azt késlekedés nélkül ugyanúgy jelentsék az Értesítendő Személyeknek, mint ahogy a felhasználóknak kell. A továbbiakban az Értesítendő Személyektől kapott utasítások szerint járjanak el.

Az adatvédelmi incidenst a Szervezetnek indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

A Rendelet szigorú eljárási követelményeket tartalmaz az adatvédelmi incidensek bekövetkezése esetére. A Szervezetnek kötelessége haladéktalanul, de legkésőbb az incidens észlelését követő 72 órán belül jelenteni azt a NAIH-nak. Ez alól csak akkor mentesülhet, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ezt a Szervezet csak úgy tudja megállapítani, ha azonnal vizsgálatot végez, amint felvetődik az incidens legenyhébb gyanúja. A vizsgálat során szükséges teljes körűen felderíteni az alábbiakat:

- az incidens körülményei,
- okai,
- pontosan milyen adatokat, mekkora alanyi kört érint,
- mennyiben sérültek az érintettek jogai és szabadságai
- mi vezethetett az incidenshez,
- milyen következményekkel jár,
- mennyiben sérültek az érintettek jogai és szabadságai,
- milyen eszközökkel tudja a Szervezet enyhíteni a következményeket,
- az incidens kezelését követően milyen intézkedéseket kell hoznia, hogy többet ne történhessen ilyen.

A 72 órás határidő minden esetben érvényes, ez alól a szabad-, ünnep- és munkaszüneti napok sem képeznek kivételt. Amennyiben a Szervezet a bejelentési kötelezettségének nem tesz eleget, büntetésre számíthat.

A bejelentés során minden lényeges információt közölni kell a hatósággal, így főként, hogy hogyan történt, kik az érintettek, az adatok mely kategóriáját érinti, milyen következményekkel járhat, továbbá milyen intézkedéseket tett a Szervezet a következmények enyhítése érdekében.

11.1.3 Információbiztonsági gyengeségek jelentése

Minden munkatársnak feladata, hogy az IT rendszerekben, szolgáltatásokban található bármely megfigyelt vagy gyanított biztonsági gyengeséget jelezze a Informatikának.

A bejelentés történhet szóban vagy írásban, a névtelen bejelentéseket is ki kell vizsgálni.

Az információbiztonság iránti figyelemfelkeltést szolgáló oktatások során az Informatika feladata tudatosítani a munkatársakban, hogy semmilyen körülmények között ne kíséreljék meg a vélt vagy valós gyenge pontok ellenőrzését, bejelentésüket bátran tegyék meg. Az Informatika a bejelentés eredményéről adjon pozitív tartalmú visszajelzést a bejelentőknek.

11.1.4 Információbiztonsági események felmérése és döntéshozatal

Az információbiztonsági incidenset jellegétől függően az arra specializálódott munkatársnak kötelessége kivizsgálni, amely személyt/személyeket az Ügyvezető Igazgató jelöl ki.

A kijelölt munkatárs nem közölhet információkat az incidenssel kapcsolatosan a vizsgálat lezártáig egy munkatárssal sem, kivéve az Informatikával és az Ügyvezető Igazgatóval konzultálhat az incidenssel kapcsolatosan.

11.1.5 Válasz az Információbiztonsági incidensekre

Minden egyes bejelentett információbiztonsági incidens bejelentést a lehető leghamarabb (de legfeljebb 24 órán belül) vissza kell igazolni, illetve a kivizsgálást követően a bejelentő felet az eredményről tájékoztatni kell.

11.1.6 Tanulás az Információbiztonsági incidensekből

Az információbiztonsági incidenseket évente legalább egyszer a Vezetőségi átvizsgálás keretében ki kell értékelni az információbiztonsági incidensek fajtái, mennyiségei és hatásai figyelemmel kísérése valamint a kezelésüket szolgáló eljárások javítása érdekében.

Az értékelés során az alábbi kérdésekre kell választ adni:

- Reakció idők
    - Milyen gyorsan történt meg az esemény észlelése, kell-e az észlelési idő csökkentése érdekében műszaki intézkedéseket tenni, például monitorozást bevezetni
    - Mennyi ideig tartott, amíg a jelentés a szükséges jelentési utat bejárta
    - Milyen gyors volt a döntéshozatal az esemény kezelésére
    - Mennyi ideig tartott a meghozott döntések, intézkedések végrehajtása
    - Milyen gyorsan sikerült az egyéb érintetteket értesíteni
- Az eszkaláció megfelelősége
    - Helyesen érvényesítették-e az eszkalációs eljárásokat
    - Sikerült-e az eszkalációs döntésekhez kellő információkat összegyűjteni
    - Szükséges-e az eszkalációs eljárás javítása
- Az esemény kivizsgálásának hatékonysága
    - Az esemény súlyosságának megbecsülése helyes volt-e
    - Az esemény kezelése során az üzleti prioritások érvényesültek-e

  - Az esemény kezelését a legmegfelelőbb személyek, szervezeti egységek végezték-e
- Az érintettek megfelelő értesítése
  - Sikerült-e a megfelelő érintetteket időben értesíteni
  - Kell-e az értesítendők körén, elérési módján változtatni
- Visszajelzések a bejelentőknek
  - A bejelentők időben és megfelelően tájékoztatva lett a bejelentésének eredményéről
  - Sikerült-e a bejelentők motiváltságát növelni, az információbiztonság iránti figyelmet javítani
- Az elkövetők motivációjának felderítése
  - Belső eredetű szándékosságra visszavezethető események esetén van-e kapcsolat a munkahelyi légkör és a cselekmény között
  - A motiváció egyedi vagy több személyt is érinthet
  - A motiváció kialakulásában hibáztatható-e valamely munkahelyi vezető
- Eljárások kidolgozása, javítása
  - Indokolt-e az egyes esemény típusokra a kezelésben segítő új eljárások kidolgozása
  - Indokolt-e egyes az üzletmenet folytonossággal kapcsolatos tervek javítása
  - Szükséges-e az oktatás javítása

11.1.7 Bizonyítékok összegyűjtése

Az információbiztonsági események kezelése során úgy kell eljárni, hogy a fellelhető bizonyítékokat hiánytalanul és hitelesen összegyűjtsék egy esetleges későbbi jogi eljárásban történő felhasználás érdekében. Ezzel összefüggésben a sértetlenség és bizalmasság sérülését okozó események után a védekező és helyreállító eljárásokat csak az Informatika engedélyével szabad megkezdeni. Az Informatika feladata a bizonyítékok összegyűjtésére irányuló tevékenységek irányítása, és az összegyűjtött bizonyítékok tárolása, megőrzése.

A bizonyítékok hitelesítése és hitelességük megőrzése érdekében minden bizonyíték azonosításáról, és kezelésének minden lépéséről jegyzőkönyvet kell vezetni, amit lehetőleg szakértő tanúkkal kell hitelesíttetni. A bizonyítékok összegyűjtése az Informatika fellelősége, az érintett munkatársak, valamint az általuk bevont szakértők feladata.

A bizonyítékokon történő minden tevékenység (például: kiértékelés, jogi eljárásokban történő bemutatás) esetén az eredeti példányok használatát kerülni kell, megbízható körülmények között készített hiteles (megfelelő szakértőkkel hitelesített) másolatokkal kell dolgozni. A bizonyítékok minden lemásolásáról, a másolatok továbbításáról, átadásáról jegyzőkönyvet kell felvenni.

11.2 Adavédelmi Incidens nyilvántartás

A Szervezetnek szükséges incidens nyilvántartást vezetni, amely a következő elemeket tartalmazza:

- Incidens sorszáma,
- Incidens leírása,
- Tudomásra jutás időpontja,
- Incidens kockázata,
- Jelenlegi védelem leírása,
- Valószínűsíthető következmények,
- Adatvédelemért felelős megbízott neve,
- Adatvédelemért felelős megbízott elérhetősége,
- Tájékoztatás időpontja,
- Kapcsolattartó neve (amennyiben Adatvédelemért felelős megbízottsel nem rendelkezik a Szervezet),
- Kapcsolattartó elérhetősége (amennyiben Adatvédelemért felelős megbízottsel nem rendelkezik a Szervezet),

Az incidens bejelentő minta Excel táblát jelen Szabályzat 1. melléklete tartalmazza.

12. ADATVÉDELMI HATÁSVIZSGÁLATI ELJÁRÁSREND

Az adatvédelmi hatásvizsgálat célja, biztosítani, hogy a Szervezet elektronikus információs rendszereiben történő fejlesztéseknél a tervezett adatkezelési műveletek a személyes adatokat megfelelően védjék.

Alapkövetelmények

Ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor a Szervezet az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek.

Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:

- természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is –alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
- a személyes adatok különleges kategóriáira vonatkozó személyes adatok nagy számban történő kezelése; vagy
- nyilvános helyek nagymértékű, módszeres megfigyelése.

A hatásvizsgálat kiterjed legalább:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben a Szervezet által érvényesíteni kívánt jogos érdeket;
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
- a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

A Szervezet szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

A hatásvizsgálatokat nyilvántartó minta Excel táblát jelen Szabályzat 2. melléklete tartalmazza.

13. A MŰKÖDÉSFOLYTONOSSÁG BIZTOSÍTÁSÁNAK INFORMÁCIÓBIZTONSÁGI VONATKOZÁSAI

A Szervezet a működés folytonosságot, illetve ennek zavara vagy kiesése esetén a csökkentett működést, majd a teljes funkcionális helyreállítást az Informatika köteles biztosítani. A működés helyreállításáért az Ügyvezető Igazgató és az Informatika közösen felel.

14. MEGFELELÉS

14.1 Megfelelés a jogi és szerződéses követelményeknek

A működés során el kell kerülni bármilyen jogszabályi, vagy szerződéses kötelezettségnek a megszegését.
A működés során alkalmazandó jogszabályok figyeléséről történő gondoskodás az integrált menedzsment rendszerben az Ügyvezető Igazgató felelőssége.
Az információbiztonság területét érintő, nem jogszabályi jellegű, de a Szervezet számára versenyelőnyt jelentő módszertanok/elvárások figyelése az Informatika felelőssége.