SZABÁLYZAT

Think. Plan. Create.

IT BIZTONSÁGI SZABÁLYZAT (IBSZ)

WDM-3608-/2023

WEBDREAM

TARTALOM

1 A SZABÁLYZAT CÉLJA

A WebDream Magyarország Kft. (a továbbiakban: WebDream) a belső szabályozások magas szintű kezelése és menedzselése, a hazai és nemzetközi minőségirányítási sztenderdeknek és jogszabályoknak való megfelelés, valamint a kiszervezésként végzett szolgáltatások átlátható kezelése érdekében aktualizálta szabályozási rendszerét. Az informatikai eszközök egyre szélesebb körű használata változó és mindig megújuló kockázatot is jelent a WebDream számára, ezért jelen szabályzat célja egységes keretszabályokat, értelmezéseket, iránymutatást adni az adatgazdák, az informatikai eszközök üzemeltetői, fejlesztői, felhasználói és az információbiztonsági felelős számára, rögzítve azokat a szabályokat, melyeket a munkakörükhöz rendelt adatok kezelése során követniük kell.

Emellett az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) célja:

- Egységes szemléletben meghatározni a felhasználók és a technikai rendszerek viszonyát az informatikai rendszerek által kezelt adatok bizalmasságának, sértetlenségének, rendelkezésre állásának megőrzése érdekében;
- Azon alapvető biztonsági normák és működési keretek meghatározása, melyek érvényesítésével a WebDream az elfogadható minimumra csökkentheti az adatkezelés és adatfeldolgozás kockázatait, beleértve a hatályos jogszabályi feltételek betartását is;
- A WebDreamhez bekerülő, illetve ott keletkező adatok, információk számítástechnikai rendszeren történő adatfeldolgozásával szemben támasztott biztonsági követelmények rögzítése;
- Az adatbiztonsággal kapcsolatos szerepek, felelősségi és jogkörök rögzítése;
- A számítástechnikai alkalmazási rendszerek, berendezések, hálózati eszközök biztonságának elősegítése.

Az IBSZ-t az elektronikus közbeszerzés részletes szabályairól szóló a 424/2017. (XII. 19.) Korm. rendelet 2. § (7) da) pontjának megfelelően a WebDream honlapján is közzé kell tenni.

2 A SZABÁLYZAT HATÁLYA

2.1 SZEMÉLYI HATÁLYA

A szabályzat szervezeti hatálya kiterjed a:

- WebDream minden munkatársára,
- WebDreammel szerződéses viszonyban tevékenykedő partnerekre.

2.2 TÁRGYI HATÁLYA

A szabályzat tárgyi hatálya kiterjed a WebDream:

- szervereire,
- munkaállomásaira,
- levelező rendszerére,
- internet kapcsolatára
- és minden egyéb eszközére valamint dokumentációjára.

2.3 TERÜLETI HATÁLYA

A szabályzat területi hatálya kiterjed a tárgyi hatálya alá tartozó informatikai erőforrások üzemelési helyszíneire:

- a WebDream telephelyére,
- a külső szolgáltatók által a WebDreamnek nyújtott szolgáltatásban érintett helyszínekre.

2.4 IDŐBELI HATÁLYA

A jelen utasítás a jóváhagyás napján lép hatályba, a dokumentumban foglalt feladatok és szabályok ezen időponttól alkalmazandók. A szabályzat visszavonásig érvényes.

3 A SZABÁLYZAT MINŐSÍTÉSE

A jelen szabályozás belső nyilvános dokumentum, amelyet a szabályzat személyi hatálya alá nem tartozó harmadik személy csak és kizárólag az Igazgatóság elnökének előzetes írásos engedélye alapján ismerhet meg. Jelen szabályzat személyi hatálya alá tartozóknak a szabályzat előírásait kötelezően ismerniük (a munkaviszony kezdetének napján, de legkésőbb az első munkában töltött napon) és követniük kell, azonban harmadik személynek a szabályzatból információt nem adhatnak ki.

4 A SZABÁLYZAT FELÜLVIZSGÁLATA

A szabályzatot évente felül kell vizsgálni, a felülvizsgálat az Informatika Biztonsági Felelős (a továbbiakban IBF) feladata.

5 AZ IBSZ SZERVEZETE

5.1 BELSŐ SZERVEZET

5.1.1 A VEZETÉS ELKÖTELEZETTSÉGE AZ INFORMÁCIÓBIZTONSÁG ÜGYE IRÁNT

Az Informatika Biztonsági Politika (IBP) és a jelen IBSZ által meghatározott követelményrendszeren keresztül testesül meg azon vezetői akarat és elkötelezettség, amely meghatározza minden érintett személy viszonyát az informatikai rendszer által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzéséhez. Meghatározza mindazokat az informatikai biztonság területén alkalmazandó védelmi alapelveket, amelyek a teljeskörűségre, a zártságra, a kockázatarányosságra, a védelem szintjének folytonos biztosítására, a szabályozás zárt folyamatára és az informatikai rendszer teljes életciklusára vonatkoznak. Alapot teremt az informatikai stratégia részét képező biztonsági stratégia kialakításához. A proaktív, azaz megelőzésre törekvő magatartást tartja szem előtt, elősegíti az informatikai biztonsággal összefüggő szabályoknak, intézkedéseknek a WebDream szintjén egységes értelmezését. Biztosítja, hogy a rendszerek védelme a jogszabályi előírásoknak eleget tegyen, valamint a védelem hiányából eredő kockázatokkal legyen arányos. Elősegíti, hogy a WebDreamet kiszolgáló kommunikációs és informatikai rendszereket az adatok titkosságára,

bizalmas jellegére és biztonságára vonatkozóan (pl. adatvédelmi törvényeknek megfelelően) üzemeljenek.

5.1.2 AZ INFORMÁCIÓBIZTONSÁG KOORDINÁLÁSA

Az információbiztonsági tevékenységek koordinálására a WebDream Informatika Biztonsági Felelőst (IBF) nevezett ki. Hatásköre alá tartoznak az informatikai biztonsági eljárások betartásának ellenőrzése, továbbá az eljárásokkal kapcsolatos folyamatok kontrollálása. Az IBSZ kidolgozásának, rendszeres aktualizálásnak és a benne foglaltak érvényre juttatásának elsődleges felelőse az IBF. Az Ügyvezető Igazgató felé jelentési kötelezettsége van, aki elbírálja a felé intézett igényeket és azokat jóváhagyja, illetve elutasítja.

5.1.3 AZ INFORMÁCIÓBIZTONSÁGI FELELŐSSÉGI KÖRÖK KIJELÖLÉSE

FELELŐS	TEVÉKENYSÉG
Ügyvezető Igazgató	Biztosítja a munkavégzéshez szükséges személyi és tárgyi feltételeket. A WebDream teljes működéséért felelős, feladata a WebDream szabályozása.
Ügyvezető	Feladata a WebDream operatív tevékenységének koordinálása és ellenőrzése.
Információbiztonsági Felelős (IBF)	Az információbiztonsági tevékenységek meghatározásáért, szabályozásáért, ellenőrzéséért és betartatásáért felelős.
Változásmenedzser	A felügyelete alá helyezett alkalmazással és eszközzel kapcsolatos változások nyomon követése, ütemezése továbbá közvetett felelősség a változások végrehajtásáért.
Adatgazda	A meghatározott adatokon adatkezelést végez vagy végeztet, e tevékenységért felelősséggel tartozik, a rábízott joga szerint adatot minősít és osztályba sorol, valamint felelős az általa minősített adat kezeléséért.
Rendszergazda, Alkalmazásüzemeltető	Mindenkori közvetlen felelősség az informatikai rendszerek üzemeltetésével kapcsolatosan. Az informatikai infrastruktúra működésének a biztosítása. A vonatkozó szabályzatokban foglaltak szerint. A vírusvédelmi és a határvédelmi rendszerek üzemeltetése, közvetlen felelősség e rendszerek működtetéséért. Jelentési kötelezettség az IBF felé.
Fejlesztő	A WebDream folyamatait, vagy termékeit támogató fejlesztések megvalósítása.

5.1.4 TITOKTARTÁSI MEGÁLLAPODÁSOK

A WebDream minden munkatársa és szerződéses partnere csak előzetes titoktartási nyilatkozat megtételét követően férhet hozzá a munkakörének, megbízásának megfelelő jogosultságokkal bíró informatikai rendszereihez és az ahhoz kapcsolódó adatokhoz.

5.1.5 AZ INFORMÁCIÓBIZTONSÁG FÜGGETLEN ÁTVIZSGÁLÁSA

A rendszeres információbiztonsági felülvizsgálatok célja a kialakított védelmi rendszer működési hatékonyságának mérése az egyenszilárdságot veszélyeztető hiányosságok és sebezhetőségek feltárása, a szükséges helyesbítő védelmi intézkedések kidolgozása, és előterjesztések elkészítése az Ügyvezető Igazgató részére. Az Ügyvezető Igazgató feladata az információbiztonsági kockázatok független szakértővel történő felülvizsgálata legalább kétévente (külön szabályzat szerint). A felülvizsgálatoknak az alábbi területekre kell kiterjednie:

- adminisztratív biztonság,
- személyi biztonság,
- fizikai és környezet biztonság,
- hozzáférés védelem,
- informatikai rendszer biztonság, melynek részét képezik az
    - alkalmazások,
    - központi kiszolgálók,
    - hálózatok, kommunikáció,
    - határvédelem és vírusvédelem,
- fejlesztés biztonság,
- üzemeltetés biztonság.

Külön figyelmet kell szentelni az előző felülvizsgálat során, vagy az adott időszakban észlelt hiányosságok vizsgálatára, a megvalósított védelmi intézkedések működőképességére. Az Ügyvezető Igazgató a felülvizsgálatba bevonhat belső és külső szakembereket is, azonban minden esetben kötelessége az összeférhetetlenség kizárása. Az IBF feladata, hogy a felülvizsgálat során tapasztalt, magában nagy kockázatot rejtő hiányosság javítását célzó intézkedési javaslatot, a vizsgálatot követő két héten belül az Ügyvezető Igazgató elé terjessze. Az Igazgatóság feladata, hogy az intézkedési tervet jóváhagyja és a végrehajtási felelősségeket meghatározza, vagy elutasítsa. Az egyéb hiányosságok feltárása esetén az IBF feladata a hiányosságok okának felderítését és a kiküszöbölést célzó intézkedési javaslat elkészítése.

5.2 KÜLSŐ ÜGYFELEK ÉS PARTNEREK

5.2.1 A KÜLSŐ PARTNEREKKEL ÖSSZEFÜGGŐ INFORMATIKAI BIZTONSÁGI KOCKÁZATOK AZONOSÍTÁSA

A WebDream külső partnere lehet:

- kiszervezett tevékenységet ellátó (adatfeldolgozó),
- egyéb szerződéses partner.

A kiszervezett tevékenységet végzővel szemben támasztott információbiztonsági követelmények nem lehetnek enyhébbek, mint a WebDreamel szemben támasztott jogszabályi követelmények. A kiszervezési szerződésnek tartalmaznia kell a törvényben megfogalmazott általános elemeket. A szerződés megkötését párhuzamosan kísérnie kell egy intézkedési tervnek, amelyben az adatkezelés, az adatfeldolgozás vagy az adattárolás folyamatosságának biztosításához szükséges személyi, tárgyi és biztonsági követelmények érvényesülésére tett feladatokat kell megjeleníteni a WebDream üzletmenet folytonosságának biztosítása érdekében.

A WebDream külső partnerekkel kötött szerződéseit – az információbiztonsági követelmények szempontjából – minden esetben az IBF-nek és szükség esetén a jogi képviselőnek is felül kell

vizsgálnia, továbbá az észrevételeket meg kell vitatni az érintett szakterületi vezetőkkel, valamint az Ügyvezető Igazgatóval.

5.2.2 AZ INFORMÁCIÓBIZTONSÁG AZ ÜGYFELEKKEL VALÓ FOGLALKOZÁS SORÁN

A WebDream ügyfelei számára többféle módon biztosítja a kapcsolattartás lehetőségét (személyes, papír alapú levelezés, elektronikus levelezés, internet stb.). Az ügyfél adatainak megfelelő kezelését minden esetben biztosítani kell. Az internet felöl érkező, ügyfelek által küldött adatok megfelelő védelmét biztosítani kell, amelyeket illetéktelen személyektől elrejtve (titkosított csatornán) kell szállítani.

5.2.3 A BIZTONSÁG KÉRDÉSÉNEK KEZELÉSE HARMADIK FÉLLEL KÖTÖTT MEGÁLLAPODÁSOKBAN

A WebDream szerződéseiben rögzíteni kell azokat a feltételeket, amelyek alapján a szerződő partner magára nézve kötelezőnek ismeri el a WebDreamre vonatkozó jogszabályi követelményrendszert, továbbá a jelen szabályzatban előírtakat (a szabályzatból a szükséges kivonatot el kell készíteni).

6 VAGYONTÁRGYAK KEZELÉSE

6.1 FELELŐSSÉG A VAGYONTÁRGYAKÉRT

6.1.1 VAGYONLELTÁR

6.1.1.1 A VAGYONLELTÁR SZEREPE

Az adatvagyon leltár egységes rendszerbe foglalja a folyamatok és alfolyamatok által kezelt irattári tételeket, a nem iratkezelt elektronikus formában tárolt adatokat, adatköröket, a kapcsolódó egyéb információkat, valamint információk feldolgozására és tárolására szolgáló informatikai erőforrásokat:

- adathordozókat,
- alkalmazásokat,
- alapszoftvereket,
- hardvereket,
- környezeti infrastruktúra elemeit.

Az adatvagyon leltár elsődleges célja, hogy az Ügyvezető Igazgató és a szakterületi vezetők naprakész módon tájékozódhassanak a WebDream kezelésében vagy tulajdonában található adatvagyonról, hogy folyamatosan meghatározott legyen a védelem tárgya.

6.1.1.2 A VAGYONLELTÁR FELÉPÍTÉSE

Az adatvagyon leltár az alábbi részekből épül fel:

- adatok leltára adatkörönként megjelölve,
- szoftver leltár (benne az informatikai alkalmazás leltár),
- hardver leltár,
- dokumentum leltár.

6.1.1.3 INFORMATIKAI ERŐFORRÁS LELTÁRAK

Az egyes informatikai erőforrásokról rendelkezésre álló nyilvántartások:

- Informatikai alkalmazás leltár, amely naprakész nyilvántartás a szolgáltatásait megvalósító alkalmazások és segédprogramok
  - nevéről
  - és verziójáról.
- Szoftver leltár, amely hardver elemenként rögzíti a telepített alapszoftverek
  - nevét,
  - verzióját, a javítókészletek verziójával egyetemben,
  - és a telepítéshez szükséges kulcsokat.
- Hardver leltár, amely hardver elemenként, értékhatárhoz kötötten rögzíti az eszköz kiépítettségét a WebDream tárgyi eszköz nyilvántartásának a környezeti infrastruktúra elemeire szűkített lekérdezése.

Valamennyi vagyontárgyat egyértelműen azonosítani kell, és valamennyi fontos vagyontárgyról leltárt kell felvenni és azt meg kell őrizni.

6.1.2 VAGYONTÁRGYAK TULAJDONJOGA

Az adatvagyonnal összefüggő vagyontárgyaknak (papír formában és elektronikusan kezelt iratok) minden esetben a WebDream tulajdonában kell lenniük (iratok, felhasználási jog, hozzáférési jog stb.). Szakterületenként szükséges adatgazdákat kijelölni, aki felelős a szakterületi adatleltárak elkészítéséért és karbantartásáért. Az adatgazda kijelölése az Ügyvezető Igazgató feladata. A szoftvereszközök tulajdonjogát illetően a szoftver lehet a WebDream tulajdonában és lehet bérlemény. A szoftver és hardver elemek műszaki nyilvántartása a rendszergazda felelőssége. A szoftver és hardver leltár naprakészségének ellenőriztetése az Ügyvezető feladata.

Kiszervezett tevékenységek esetében a hardver és a szoftver a kiszervezett tevékenységet végző tulajdonában is lehet. Használatukkal kapcsolatban a jelen IBSZ által meghatározott biztonsági kritériumoknak kell megfelelni. Egyéb szerződéses partnerek estében magának a szerződésnek kell meghatároznia, hogy a szerződés időtartama alatt melyik fél tulajdonában lévő szoftvereket és hardvereket használja a partner.

6.1.3 VAGYONTÁRGYAK ELFOGADHATÓ HASZNÁLATA

A WebDream tulajdonában lévő adatvagyont mind a dolgozók, mind a kiszervezett tevékenységet végzők, mind az egyéb szerződéses partnerek csak a munkájukhoz feltétlenül szükséges mértékben, s csak szabályozott és engedélyezett formában használhatják.

6.1.4 INFORMATIKAI NYILVÁNTARTÁSOK KEZELÉSE

Az informatikai irányítás magas szintű megvalósításának alapfeltétele a teljes körű és folyamatosan aktualizált informatikai nyilvántartások rendelkezésre állása. A minimálisan szükséges nyilvántartások az alábbiak:

- IT szabályzatok listája,
- IT vonatkozású szerződések listája,
- jogosultság nyilvántartás,
- hardver nyilvántartás,
- szoftver nyilvántartás,
- licenc nyilvántartás,

- média nyilvántartás.

A WebDream fenti nyilvántartásai a WebDream belső hálózatán kialakított könyvtárban találhatók. A szabályzat kiadásakor:

- \BelsőDokumentumok\Nyilvántartások\

A nyilvántartások folyamatos karbantartásáért az Ügyvezető, a nyilvántartások rendszeres ellenőrzéséért az IBF felel.

A WebDream biztonsága szempontjából legfontosabb nyilvántartás a hozzáférések és jogosultságok felsorolását tartalmazó jogosultság nyilvántartás, amelyet a WebDream a szerverén a \BelsőDokumentumok\Nyilvántartások\Jogosultságok mappában rögzít. A jogosultságok folyamatos nyilvántartásáért a Rendszergazda, a jogosultságok rendszeres felülvizsgálatáért és ennek kapcsán a nyilvántartás megbízhatóságáért az IBF felel a „Jogosultságkezelési szabályzat”-nak megfelelően.

Az informatikai jellegű kéréseket a Help Desk rendszeren (iTop) keresztül kell kezelni. A beérkezett kérések dokumentálását és menedzselését az iTop Help-Desk rendszer végzi, amely tartalmazza a munkatársaktól érkező kéréseket illetve bejelentéseket, és itt kerül dokumentálásra az előre nem szabályozott folyamatban történő probléma megoldás, azaz az incidensek kezelése is. A Help-Desk kérések listáját a „Help-Desk és incidenskezelési szabályzat”-nak megfelelően kell kezelni.

6.2 INFORMÁCIÓK OSZTÁLYOZÁSA

6.2.1 OSZTÁLYOZÁSI ELVEK

A WebDream teljes feldolgozási, végrehajtási munkafolyamataira biztosítani kell a három alapfenyegetettség bekövetkezési valószínűségének csökkentését, vagyis az adatok, információk és az azokat kezelő rendszerek:

- bizalmasságát,
- sértetlenségét,
- rendelkezésre állását.

Minden számítógépes rendszernél alapvető szempont az adatok biztonsága. A bekövetkezendő adat- és információvesztésekből adódó károk minimalizálásának leghatékonyabb eszköze a helyesen megtervezett és következetesen végrehajtott adatkezelési, mentési és helyreállítási rendszer, valamint a hatályban lévő biztonsági szabályozások betartásának rendszeres ellenőrzése. A vonatkozó törvényi előírások szerint mindenkor rendelkezésre kell állnia az informatikai rendszer elemeinek a WebDream által meghatározott biztonsági osztályokba sorolási rendszerének. Az erre vonatkozó felügyeleti ajánlás alapján a WebDream kialakította egyrészt az informatikai eszközök rendelkezésre állási követelményei szerinti biztonsági osztályba sorolási rendszerét valamint a WebDream adatainak bizalmasság szerinti biztonsági osztályokba sorolási rendszerét.

6.2.2 A WEBDREAM INFORMATIKAI ESZKÖZEINEK BIZTONSÁGI BESOROLÁSA

A WebDream egyes informatikai eszközei valamint a rajtuk futtatott alkalmazásai különböző jelentőséggel bírnak a WebDream biztonságos működésének szempontjából. A tevékenységek biztonsági kockázatának figyelembe vételével a következő szinteket kell kialakítani.

Kiemelt (High):

Ebbe a szintbe tartoznak az alapfunkciók működtetése és biztonsága szempontjából legfontosabb adatok, alkalmazások, rendszerszoftverek, eszközök, berendezések és a környezeti infrastruktúra ide tartozó elemei. Közös jellemzőjük, hogy még rövid időre (0 - 24 óra) történő működéskiesésük sem viselhető el a rendszer számára, illetve hiányuk és a rajtuk tárolt adatok bizalmasságának, sértetlenségének, hitelességének elvesztése olyan biztonsági problémákat okoz, amelynek kockázata nem vállalható. Ide tartoznak azok a szerverek, alkalmazások és adatbázisok, amelyek a WebDream létfontosságú feladatait, üzletvitelét hivatottak szolgálni valamint a hálózati eszközpark azon aktív elemei, amelyek nélkül a hálózatnak olyan szegmensei válnának kommunikáció képtelenné, amelyek a működés szempontjából létfontosságúak illetve azok a speciális informatikai eszközök, amelyek a WebDream, mint szervezet biztonságos működését és védelmét hivatottak szavatolni

Fokozott (Medium):

Az ide tartozó informatikai eszközök, alkalmazások működésének viszonylag rövid ideig (24 – 48 óra) tartó kiesése elviselhető terheket ró a WebDreamre, mind a tevékenység ellátása, mind biztonsági szempontból. Ebbe a szintbe tartoznak azok a szerverek, amelyek működésének kiesése ideiglenesen elviselhető kockázatot jelent valamint a hálózati eszközpark azon aktív elemei, amelyek nem sorolhatók a Kiemelt szintbe, illetve azok a személyi számítógépek, amelyek kiemelt fontosságú adatokat tartalmaznak, vagy kiemelt fontosságú hálózati kapcsolattal rendelkeznek (kiszolgálók, aktív hálózati eszközök konfigurálása, banki szoftvert tartalmazó PC).

Alap (Low):

A harmadik szintbe tartozó informatikai eszközök, alkalmazások működésének még hosszabb ideig (1 hét) tartó megszűnése sem befolyásolja jelentős mértékben a WebDream működését. Ide tartoznak az egyéb, a Kiemelt és Fokozott szintbe be nem sorolt informatikai eszközök, amelyeken nem tárolnak kiemelt jelentőségű adatokat, illetve amelyek működésének kiesése a feladatellátás szempontjából nem meghatározó valamint azok a munkaállomások és hordozható számítógépek.

Az informatikai vagyon minden elemét be kell sorolni valamelyik szintre, annak megfelelően, hogy működésének megszűnése hogyan hat a WebDream egészének funkcionalitására. Az adatgazdák feladata az adatvagyon besorolása, s ezt követően az informatikai alkalmazások és eszközök besorolása. A három kategóriába tartozó eszközökre csoportonként és eszköztípusonként más-más biztonsági előírások vonatkoznak.

6.2.3 AZ ADATOK ÉS INFORMÁCIÓK OSZTÁLYOZÁSA

A WebDreamben keletkező és ott kezelt adatokat, információkat biztonsági osztályokba kell sorolni az alábbi szempontok figyelembe vételével:

- az adatok nyilvánosságra kerülésének kockázata és lehetséges következményei,
- vonatkozó törvényi és szabályozói rendelkezések (a jogszabály által előírt védelmi szint az osztályozással nem csökkenhet),
- az adatok bizalmasságára és pontosságára/helyességére vonatkozó követelmények.

A WebDream módszertanával összhangban az alábbi négy osztály valamelyikébe kell sorolni az adatokat.

- Nyilvános (Public): Olyan adatok és információk, amelyek a WebDreamen belül és kívül szabadon terjeszthetők.

- Belső használatra (Internal Use Only): Olyan adatok és információk, amelyek a WebDreamen belül szabadon terjeszthetők. Alapértelmezés szerint ebbe a csoportba tartozik minden, másképpen nem osztályozott adat, továbbá az olyan harmadik félhez tartozó adatok, melyek nem képezik titoktartási megállapodás tárgyát.

- Bizalmas (Confidential): Olyan adatok és információk, melyek nyilvánosságra kerülése anyagi, jogi vagy reputációs kárt okozhat a WebDreamnek. Bizalmas adatokhoz csak azok férhetnek hozzá, akiknek a munkájához szükséges a hozzáférés és/vagy az adatgazda engedélyezte számukra a hozzáférést. Alapértelmezés szerint ebbe a körbe tartoznak a személyes adatok, üzleti titkok és banktitkok.

- Szigorúan Bizalmas (Strictly Confidential): Olyan adatok és információk, amelyek nyilvánosságra kerülése jelentős anyagi, jogi vagy reputációs kárt okozhat a WebDreamnek. Az ebbe az osztályba sorolt adatokhoz csak az adatgazda által erre külön felhatalmazottak férhetnek hozzá. Az adatok kezelése fokozott körültekintést igényel.

Az adatkör végleges biztonsági osztályát az alapkövetelmények általi besorolásból a legmagasabb minősítésű adja meg.

Az adatok osztályozását a jelen szabályozással együtt a WebDream elvégezte, figyelembe véve a WebDream speciális üzleti működését és kockázatait.

- Bizalmas (Confidental) kategóriába tartozik minden a WebDreamnél elektronikusan, vagy papír alapon keletkező, tárolt és használt információ.
- Nyilvános (Public) kategóriába tartozik minden olyan elektronikusan, vagy papír alapon keletkező, tárolt és használt információ, amit az Ügyvezető Igazgató annak nyilvánít.

6.2.4 AZ ADATKEZELÉS SZABÁLYAI OSZTÁLYOK SZERINT

Miután az adatok osztályozása megtörtént, azokat a dokumentum minden oldalán jelezni kell. Ezen túlmenően az adatokat a következő szabályok szerint kell kezelni, figyelemmel a hatályos jogszabályi előírásokra is:

Nyilvános (Public) adatok:

- Elektronikus formában:
  - szabadon tárolhatók
  - szabadon másolhatók
  - szabadon megoszthatók
  - szabadon törölhetők, ha törvény vagy más szabályozás másképp nem rendeli
- Papír formában:
  - szabadon tárolhatók
  - szabadon másolhatók
  - szabadon megoszthatók
  - szabadon selejtezhetők, ha törvény vagy más szabályozás másképp nem rendeli

Belső használatra (Internal use only) rendelt adatok:

- Elektronikus formában:
  - olyan formában tárolhatók, hogy csak a terjesztési körön belül lévők férhetnek hozzá (pl. WebDreamen belüliek)
  - terjesztési körön belül másolhatók
  - terjesztési körön belül megoszthatók
  - szabadon törölhetők, ha törvény vagy más szabályozás másképp nem rendeli
- Papír formában:
  - olyan formában tárolhatók, hogy csak a terjesztési körön belül lévők férhetnek hozzá (pl. a WebDreamen belüliek)
  - terjesztési körön belül másolhatók
  - terjesztési körön belül megoszthatók
  - a selejtezés során az adatokat meg kell semmisíteni (pl. iratmegsemmisítővel)

Bizalmas (Confidental) adatok:

- Elektronikus formában:
  - olyan formában tárolhatók, hogy csak az erre felhatalmazott felhasználók férhetnek hozzá. Amennyiben lehetséges, a bizalmas adatokat titkosított formában kell tárolni. Laptopon csak titkosított formában tárolhatók.
  - a hozzájuk kapcsolódó feladatok végrehajtásához szükséges mértékben másolhatók
  - harmadik féllel történő megosztásukkor (amennyiben arra jogszabály/megfelelő érintett hozzájárulás lehetőséget ad) gondoskodni kell az adatok védelméről (lehetőleg titkosítással)
  - törlésük során helyreállíthatatlan formában meg kell semmisíteni az adatokat
- Papír formában:
  - csak zárt helyiségben vagy helyen tárolhatók
  - a hozzájuk kapcsolódó feladatok végrehajtásához szükséges mértékben másolhatók
  - csak zárt, nem átlátszó borítékban továbbíthatók
  - a selejtezés során az adatokat meg kell semmisíteni (pl. iratmegsemmisítővel)

6.2.5 AZ ADATGAZDA SZEREPE ÉS FELELŐSSÉGE

A vonatozó törvényi előírásoknak való megfelelés illetve a fenti adatbesorolás megvalósítása érdekében az Ügyvezető Igazgatónak adatgazdákat és helyetteseket kell kijelölni. Az adatgazdákat okiratban kell kijelölni, amely minimálisan tartalmazza az adatgazda nevét, beosztását, szervezeti egységét, valamint az adatgazdai felelősségi körébe tartozó rendszereket (adatköröket).

Az adatgazdák kinevezése határozatlan időre szól, amely kinevezési eljárást meg kell ismételni, ha az adatgazdai funkciót betöltő személy munkaköre megváltozik, valamint új adatgazdát szükséges kijelölni, ha a korábban az adatgazdai posztot betöltő személy munkaviszonya megszűnik.

Az adatgazda felméri és minősíti a szabályzatban foglaltak alapján azokat az adatköröket, amelyekben az általa képviselt szervezeti egység érintett, meghatározza az adatkörrel kapcsolatban az adatkezelés célját és módját (beleértve a felhasznált informatikai rendszert), meghozza a vonatkozó döntéseket és végrehajtatja azokat.

Az adatgazda határozza meg a felelősségi körébe tartozó adatkörökre vonatkozóan a kezelés módját, feltételeit valamint az adatgazda dönt a felelősségi körébe tartozó adatkörökre vonatkozóan az adatok biztonsági besorolásáról, minősítéséről, hozzáférési szabályairól.

Az adatgazda az adatkör felméréssel kapcsolatos tevékenységet delegálhatja az általa kijelölt, az adatkörrel kapcsolatos folyamatfelelősnek, de az adatkörök előzetes besorolásával kapcsolatos döntési kompetencia NEM delegálható, mivel az adatgazda felelős az általa kezelt (tulajdonolt) adatvagyon kezeléséért, hozzáférési szabályainak jóváhagyásáért, betartásáért és az elszámoltathatóságáért.

7 AZ EMBERI ERŐFORRÁSOK BIZTONSÁGA

7.1 AZ ALKALMAZÁST MEGELŐZŐEN

7.1.1 FELADAT- ÉS FELELŐSSÉGI KÖRÖK

A WebDream az alkalmazottakkal, kiszervezett tevékenységet ellátó felekkel, egyéb szerződéses partnerekkel és harmadik felekkel szemben támasztott követelményei a következők:

- erkölcsi bizonyítvány megléte,
- szakmai képesítések és az azokat igazoló bizonyítványok megléte,
- indokolt esetben ellenőrizhető referenciák.

7.1.2 ÁTVILÁGÍTÁS

Munkavállaló alkalmazását megelőzően javasolt a jelentkező referenciáit ellenőrizni, továbbá erkölcsi bizonyítványát bekérni. Szerződéses partner esetében a szerződésben rögzíteni kell a partner alkalmazottaival szemben támasztott követelményeket.

7.1.3 ALKALMAZÁSI FELTÉTELEK

A munkáltatói jogokat gyakorló, vagy nevében eljáró kötelessége, hogy a WebDreamnél felvételre kerülő személy részére a munkaszerződésben, a kinevezési okiratban, vagy a munkaköri leírásban rögzítse az információbiztonsági kötelezettségeket, megszegésük esetére pedig hívja fel a figyelmet a fegyelmi, kártérítési és büntetőjogi következményekre.

A WebDream minden munkatársa, szerződéses partnere csak előzetes titoktartási nyilatkozat megtételét követően férhet hozzá a munkakörének, megbízásának megfelelő jogosultságokkal a WebDream informatikai rendszereihez és adataihoz. A munkáltatói jogokat gyakorló, vagy nevében eljáró köteles az információbiztonsággal kapcsolatos szerepeket ellátó minden egyes munkavállaló munkaköri leírásában rögzíteni az információbiztonsággal kapcsolatos kötelezettségeket.

Egy szerződött szolgáltató vagy alkalmazottja esetében a vonatkozó szerződésben meg kell határozni, hogy a bizalomvesztésre okot adó magatartás, vagy a feltételek hiánya (szerződés alatti megszűnése) egyoldalú elállási ok.

7.2 AZ ALKALMAZÁS IDŐTARTAMA ALATT

7.2.1 A WEBDREAM VEZETÉSÉNEK FELELŐSSÉGE

A WebDream vezetésének felelőssége a biztonságos munkavégzés feltételeinek biztosítása, továbbá a munkakör ellátásához szükséges eszközök megteremtése.

7.2.2 AZ OKTATÁSOKKAL ÉS KÉPZÉSEKKEL KAPCSOLATOS ALAPELVEK

A WebDream működése szempontjából kiemelt fontosságú a munkatársak szakmai képességének színvonala, ebből következően kiemelt cél a WebDream működtetéséhez szükséges képességek fenntartása és bővítése. A WebDream alapvető értéke az emberi erőforrások minősége, azaz munkatársainak tudása, elkötelezettsége, hatékonysága.

A munkatársak szaktudásának mértéke fontos szempont a WebDream személyi létszámának növelésekor. Ebből következően az új felvételkor kiemelt szempont a lehető legmegfelelőbb és legnagyobb szaktudással és szakmai tapasztalattal rendelkező személyek felvétele.

A meglévő szakembergárda szakmai tudásának fenntartása és tudásszintjének emelése a vezetés kiemelt szempontja, és ezért a vezetés elkötelezett a rendszeres szakmai oktatás biztosításában. Ennek érdekében az éves költségek tervezésekor gondoskodni kell a képzésre és oktatásra szánt pénzek rendelkezésre állásáról.

Minden évben oktatási tervet kell készíteni, és a jóváhagyott oktatási tervek megvalósulásáról gondoskodni kell. Az éves képzési, oktatási terv elkészítése a Területi vezetők feladata, az oktatási terv jóváhagyása és a szükséges anyagi erőforrások biztosítása pedig az Ügyvezető Igazgató feladata és hatásköre.

Minden új munkatárs belépésekor részletes tájékoztatást kap a belső működésről, a szervezet felépítéséről, a belső szabályozásokról és az Információbiztonsági Szabályzásokban leírtakról, valamint a munkavállalói jogokról és kötelezettségekről. Minden új belépő oktatásban részesül az alábbi témakörökben:

- tűzvédelem,
- munkavédelem,
- informatikai rendszerek használata, jogok, jogosultságok,
- közlekedés az irodai területen,
- nyomtatás, másolás.

A Területi vezetők minden évben felmérik a munkatársak képzettségi szintjét, a WebDream stratégiájának teljesítéséhez szükséges továbbképzési igényeket, és az igények alapján megtervezik a munkatársak továbbképzését. Az összesített területi oktatási terveket az Ügyvezető Igazgató a rendelkezésre álló erőforrások figyelembe vételével hagyja jóvá.

A szakmai képzések mellett minden évben kötelező általános munkavédelmi és információbiztonsági képzést szervezni. Új rendszerek esetén a beszállítóktól meg kell követelni az új rendszerekre vonatkozó speciális ismeretek leírását és oktatását. A konferenciákon, szakmai utazásokon vagy egy társszervezetnél történő konzultáció szintén a képzés szerves részét képezi.

Minden olyan beosztást, amelyhez valamilyen ismeretanyag elsajátítására van szükség, és ahol ennek az ismeretanyagnak a hiánya problémát okozna a szolgáltatások minőségében vagy a biztonsági rendszer működésében, ott a képzést a terület folyamatosan és igény szerint oldja meg.

Mivel a vonatkozó jogszabályokban előírták, hogy a belső szabályzatában meg kell határoznia az egyes munkakörök betöltéséhez szükséges informatikai ismeretet, ezért az alábbiak tartalmazzák az egyes munkakörök esetén szükséges minimális informatikai szakismereteket.

A WebDream minden munkakörének betöltéséhez az alábbi informatikai ismeretek (Alapszintű) megléte szükséges:

- a Microsoft Office programcsomag Word, Excel, Outlook rendszerének felhasználói szintű ismerete,
- az internet/intranet használatának felhasználói szintű ismerete, amely magába foglalja az alapszintű biztonsági ismereteket is.

Az informatikai rendszergazdai munkakör betöltéséhez – a fenti Alapszintű ismereteken túl – az alábbi informatikai ismeretek szükségesek:

- a felelősségi területe tekintetében igazolt rendszergazdai ismeretek,
- a WebDreamnél alkalmazott egyéb hardver és szoftver infrastruktúra elemek ismerete.

A WebDream üzleti tevékenységének támogatásához használt üzleti/alkalmazói rendszerek ismerete az egyes munkakörök betöltése esetén nem alapfeltétel, de a próbaidő időtartama alatt a szakterületi vezetőnek gondoskodnia kell a megfelelő ismeretanyag elsajátításához szükséges feltételek biztosításáról. A munkaszerződés véglegesítésének feltétele a munkavállaló által használt üzleti/alkalmazói rendszerek ismerete.

7.2.3 AZ INFORMÁCIÓBIZTONSÁG TUDATOSÍTÁSA, OKTATÁS ÉS KÉPZÉS

A WebDream minden felhasználóját információbiztonsági oktatásban kell részesíteni. A WebDream vezetésének biztosítania kell az oktatások előfeltételeit. Az oktatásokkal kapcsolatos anyagok előállítását, a megrendezését, továbbá a szakmai továbbképzés lehetőségét.

Az IBF feladata az oktatási anyag szakmai részének elkészítése, naprakészségének és minden felhasználó részére való hozzáférhetőségének biztosítása, valamint az oktatások megtartása, amelyben

- Fel kell hívnia a felhasználók figyelmét az IBSZ munkavégzésükre vonatkozó irányelveire és az ezzel kapcsolatos felelősségekre;
- Ismertetnie kell azokat a kockázatokat és sebezhetőségeket, amelyek a felhasználó adat és rendszer biztonságát veszélyeztető magatartását használják ki;

Az IBF kötelessége az oktatási anyag és oktatási tematika szerint felhasználói biztonság tudatosság építő oktatást megtervezni és megszervezni. A biztonsági oktatások megtörténtét dokumentálni kell.

Minden új felhasználó számára a munkakezdést követő egy hónapon belül biztosítani kell az oktatási anyag (írott prezentáció, oktatásvázlat – legfontosabb tudnivalók) megismerését. Az oktatáson való részvételt a felhasználó aláírásával jegyzőkönyvön hitelesíti. A jegyzőkönyvnek tartalmaznia kell a következő mondatot:

"Alulírott, felelősségem teljes tudatában kijelentem, hogy az információ biztonsági oktatáson részt vettem, az azon elhangzottakat megértettem, tudomásul vettem."

Az információbiztonsággal kapcsolatos kockázatokat csökkenti, ha a WebDream munkavállalói tisztában vannak a munkafolyamataikat támogató informatikai rendszerekkel. A WebDreamnél a dolgozók kötelesek az érvénybe léptetett, valamint módosított IBSZ-t megismerni, az abban

foglaltakat betartani és betartatni, valamint az oktatáson részt venni. Az oktatás lebonyolítható a munkavállalókra vonatkozó tudnivalókat tartalmazó tájékoztató anyag átadásával, elektronikusan, vagy személyes konzultáció lehetőségének biztosításával is.

Oktatást kell tartani az érintett munkavállalóknak hardver- és szoftvereszközök, valamint a használatukat szabályozó eljárások jelentős változásakor. Minden oktatás után a munkavállalóknak a jelenléti íven történő aláírásukkal kell nyilatkozniuk, hogy a rájuk vonatkozó rendelkezéseket megismerték és tudomásul vették.

A szükséges oktatásokat elektronikus rendszerben is el lehet végeztetni. Ebben az esetben az elektronikus oktatási rendszerben rögzített részvétel a jelenléti ív aláírásának felel meg.

7.2.4 FEGYELMI ELJÁRÁS, ALKALMAZHATÓ SZANKCIÓK

Az IBF a felhasználó súlyos mulasztását, az információ gondatlan veszélyeztetését köteles írásba foglalni és jelentést készíteni az Ügyvezető Igazgató, valamint a felhasználó felett munkáltatói jogokat gyakorló vezető számára.
A jelentésnek tartalmaznia kell:

- a biztonságsértés időpontját,
- a vétkes nevét és beosztását,
- a tevékenység által közvetlenül okozott kárt,
- a tevékenységgel közvetve okozható kár becsült mértékét,
- a javasolt intézkedéseket.

A biztonsági esemény kivizsgálása során az eseménnyel kapcsolatban érintett munkatársaknak együtt kell működniük az IBF-el, nem akadályozhatják a vizsgálat lefolytatását.

7.3 AZ ALKALMAZÁS MEGSZŰNÉSE VAGY MEGVÁLTOZÁSA

7.3.1 FELELŐSSÉGEK AZ ALKALMAZÁS MEGSZŰNÉSEKOR

A megszűnési igényt (esetenként változást) dokumentált formában (papír vagy email) kell megküldeni az Ügyvezető Igazgató részére. A közvetlen vezetők hatásköre a jogosultságokat visszavonni, illetve megadni. A kint levő eszközök visszaszolgáltatásáról jegyzőkönyvet kell készíteni, amelyet a munkavállalónak, a közvetlen vezetőnek aláírással hitelesíteni kell. A munkaszerződés bontásnak előfeltétele a kint levő eszközök maradéktalan visszaszolgáltatása.

7.3.2 VAGYONTÁRGYAK VISSZASZOLGÁLTATÁSA

Valamennyi alkalmazottnak, szerződőnek és a felhasználó harmadik félnek vissza kell szolgáltatnia a WebDream valamennyi birtokukban lévő vagyontárgyát, amikor alkalmazásuk, szerződésük, illetve megállapodásuk lejár, illetve megszűnik. A kiadást és visszaszolgáltatást a kísérőlapon aláírással igazolni kell. A visszaszolgáltatás teljességét a közvetlen vezető vagy a HR vezető határozza meg. A kilépéshez szükséges dokumentációk csak abban az esetben adhatók ki, amennyiben minden kintlévőséget visszaszolgáltatott az adott személy.

7.3.3 HOZZÁFÉRÉSI JOGOK MEGSZŰNÉSE

A felhasználói hozzáféréseket dokumentált és ellenőrizhető formában nyilván kell tartani. A jogosultságok megszüntetésének az iTop ticketing rendszerben nyomon követhető formában kell történnie. A jogosultságok visszavonását legkésőbb a munkavállaló (szerződő, felhasználó)

utolsó munkanapjának végeztével kell megtenni. A jogosultságok visszavonását a közvetlen vezető felelőssége elvégeztetni; a hozzáférések visszavonásáért ő felel. A Jogosultságkezelésre vonatkozó részletes szabályokat a „Jogosultságkezelési szabályzat" tartalmazza.

8 FIZIKAI VÉDELEM ÉS A KÖRNYEZET VÉDELME

8.1 TERÜLETEK VÉDELME, BIZTOSÍTÁSA

8.1.1 FIZIKAI BIZTONSÁGI HATÁRZÓNA

8.1.1.1 WEBDREAM DOLGOZÓK ÉS PARTNEREK

A WebDream telephelyén elhelyezkedő, valamint a kiszervezett tevékenységeket végzők telephelyén elhelyezkedő szerverekre, kiszolgálókra az alábbi rendelkezéseket kell betartani:

- A szervereket zárható helyiségben, gépteremben kell elhelyezni, üzemeltetni.
- A szerverszobának kulccsal zárhatónak kell lennie és biztosítani kell a szerverszobába történő ki- és belépés naplózását (elektronikus, vagy papír formában).
- A helyiségbe csak megfelelő jogosultságokkal rendelkező személyek léphetnek be, jogosultság hiányában csak kísérettel történhet meg a belépés, majd azt követően az ott tartózkodás, munkavégzés.

A partnerek látogatását külön, az Ügyvezető engedélyéhez kell kötni. Kiszervezett szolgáltatás esetén azon géptermekbe, ahol a WebDream szerverei vannak, a kiszervezett szolgáltató vezetője engedélyezheti a belépést, de a kontrollnak működnie kell, amit az IBF ellenőriz.

8.1.1.2 IDEGENEK, ÜGYFELEK

Az idegenek és ügyfelek belépése esetén biztosítani kell, hogy a látogatók csak kísérettel tartózkodhassanak a gépterem területén.

8.1.2 FIZIKAI BELÉPÉS ELLENŐRZÉSE

A WebDream irodáiba a belépést elektronikus ajtónyitó rendszerrel (Roger) biztosítják.

A munkavállalók a munkába álláskor automatikusan kapnak ajtónyitó kódot, minden munkatárs egyedi kóddal rendelkezik. A belépésre jogosító kódot az ajtónyitó rendszert üzemeltető munkatársak adják.

A kód kiadásakor megfelelően dokumentálni kell a személy nevét.

A kódot érvényteleníteni kell az alábbi esetekben:

- A munkavállaló munkaviszonya és ezzel belépési jogosultsága megszűnik.
- A munkavállaló – szabadság, betegség, tartós kiküldetés, átirányítás stb. miatt előre láthatóan – 90 napot meghaladóan munkavégzésre az adott munkahelyen nem kötelezett.
- A munkavállaló felmentése vagy felfüggesztése esetében.
- Egyéb indokolt esetben az Ügyvezető Igazgató döntése alapján.

A kód kiadásának és törlésének dokumentálása az Ügyvezető feladata.

Az ajtónyitó rendszert úgy kell kialakítani, hogy abból a belépések dátummal, időponttal együtt egyaránt visszakereshetőnek kell lenni.

8.2 ZÁRT LÁNCÚ KAMERA RENDSZER

Az irodában az összes helyiségben van kamera. A képfelvételek kezelését az üzemeltető végzi a hatályos törvények figyelembevételével. A kamerarendszer képfelvételeinek visszajátszását csak indokolt esetben (biztonsági incidens) az Ügyvezető Igazgató hajtja végre. A kamerák képeit a mobiltelefonján is bármikor megnézheti.

8.3 KULCSOK, RIASZTÓKÓDOK

Az irodába történő bejutás elektronikus ajtónyitó rendszerrel védett és menedzselt, amelyet az Ügyvezető kezel és ellenőriz. A bejáratok kulcsainak kezelése, nyilvántartása, kiadása és visszavétele, valamint a riasztó kód kezelése az Ügyvezető felelőssége. Az utolsónak távozó alkalmazott kötelessége ellenőrizni a nyílászárók és a bejáratok bezárását és azt követően a riasztó rendszer aktiválását.

Abban az esetben, ha illetéktelen által elkövetett behatolás gyanúját tapasztalják, haladéktalanul értesíteni kell a WebDream vezetőit, illetve a Rendőrséget. Abban az esetben, ha a riasztó kód titkossága, bizalmassága megsérült, azonnal jelenteni kell a WebDream vezetőinek, majd a kódot azonnal meg kell változtatni!

A WebDream munkatársainak is kötelessége a munka-, a tűz-, a balesetvédelmi és a biztonsági szabályok érvényesítése és ebből következően abban az esetben, ha már a bejáratnál illetéktelen behatolás gyanúját tapasztalják, akkor haladéktalanul értesíteni kell a WebDream vezetőit.

8.4 „TISZTA ASZTAL" POLITIKA („CLEAN DESK" POLICY)

Üzleti titkot, személyes adatot tartalmazó információkat, dokumentumokat munkaidőn túl nem szabad az asztalon tárolni, azokat csak a munkavégzés idejére szabad elővenni.

Az információt mindig célhoz kötötten, a munkavégző számára lehet betekintés céljából megnyitni. Abban az esetben, ha a munkavállaló elhagyja a munkavégzés helyét, köteles gondoskodni az üzleti titkot, személyes adatot tartalmazó információkat tartalmazó dokumentumok megfelelő szintű védelméről.

Napi munkavégzést követően a munkahelyet (asztalt) tisztán, rendesen, üzleti titkot, személyes adatot tartalmazó információkat tartalmazó dokumentumok nélkül, azokat elzártan lehet elhagyni.

Üzleti titkot, személyes adatot tartalmazó információkat tartalmazó dokumentumokat a munkavégzés helyéről – *a WebDream bérelt irodáján kívül* – kivinni alapesetben NEM engedélyezett. Ez alól az Ügyvezető Igazgató adhat felmentést, viszont ebben az esetben a ki- és visszaszállítás során gondoskodni kell a megfelelő szintű fizikai / logikai védelemről.

8.5 IRODA, SZERVERTEREM, ÉPÜLET VÉDELME

8.5.1 IRODÁK, HELYISÉGEK ÉS LÉTESÍTMÉNYEK VÉDELME

Az irodák, helyiségek és létesítmények fizikai védelmét ki kell alakítani és azt alkalmazni kell. Az épület egyes helyiségeinek biztonsági védelmi szint szerinti besorolása az Ügyvezető Igazgató feladata. A központi épületbe történő bejutás beléptető rendszerrel védett és menedzselt. A beléptető rendszert az IT munkatársai kezelik és ellenőrzik, az egyes külön jogi személynek számító leányvállalati belépések elkülönítettek. A központi telephely azonos védelmi szintű kivéve az IT szoba, az IT raktár és a gépterem helyiségeit, amelyek kiemelt védelmi szintbe sorolandók.

A kiemelt védelmi szintű helyiségbe csak az Ügyvezető által meghatározott személyek léphetnek be. A belépő kártyával rendelkező munkatársak csak munkaidőben léphetnek az épületbe, munkaidőn túl csak engedéllyel. Munkaidőn túl a portaszolgálat az épület bejáratait kulcsra zárják és a belépéseket dokumentáltan kontrollálják. A központi épületben kamerás megfigyelésnek, mozgásérzékelőknek és riasztó rendszernek kell működnie. A takarítást a bérbeadó vállalja a szerződésének megfelelő biztonsági feltételekkel. A takarító személyzet a kiemelt helyiségekbe csak kísérettel léphet be.

Munkaidőben a bejáratnál lévő portaszolgálat feladata a látogatók regisztrálása és a WebDream részéről a látogatót fogadó munkatárs értesítése. Külsős személyek belépése csak kísérővel engedélyezett. A látogatót (külső személyt) fogadó munkatárs kötelessége a kíséret biztosítása egészen a látogató kilépéséig. A látogató távozásakor a portán lévő látogató listára rá kell vezetni a kilépés tényét és idejét is.

8.5.2 SZERVERTEREM VÉDELME

A gépterem kialakításánál a következő minimális követelményeknek kell eleget tenni:

- A szerverszobának a lehető legkevesebb nyílászáróval kell rendelkeznie.
- A szervereknek egyenletes hőmérsékletet és páratartalmat kell biztosítani olyan klímaberendezés működtetésével, amely jelzi a tűréshatár túllépéseket.
- Behatolás-védelmi szempontok és "vis major" helyzetek számbavételével a lehető legbiztonságosabb területre kell telepíteni a szerverszobát, és el kell látni megfelelő behatolás-védelmi berendezésekkel.
- Váratlan áramkimaradás esetére a szervereket és a fontosabb munkaállomásokat intelligens UPS-ekkel kell ellátni, amelyek az áramellátás folyamatosságát biztosítják.
- Az áramellátást biztosító UPS-eket rendszeresen ellenőrizni kell. Ezen ellenőrzések elvégeztetéséért a rendszergazda felelős. Az ellenőrzési periódusok meghatározásánál figyelembe kell venni az UPS akkumulátorának korát és élettartamát.
- Az elektromos hálózatban fellépő anomáliák ellen a szerverszobában megfelelő védelmet kell kialakítani (villámvédelem, feszültség-ingadozás, feszültség csúcsok stb.).

A WebDream üzleti titkait tartalmazó, éles környezetet működtető szervereket a gépteremben kell elhelyezni. A gépterem kiemelt biztonsági fokozatú helyiség, ahová csak az arra feljogosított személyek léphetnek be. A gépterembe történő belépés korlátozott, amelyet a beléptető rendszernek kell rögzítenie. A szerverek jelenleg az Integrity által biztosított gépteremben kerültek elhelyezésre, amely a fenti feltételeknek eleget tesz.

8.5.3 KÜLSŐ ÉS KÖRNYEZETI VESZÉLYEKKEL SZEMBENI VÉDELEM

Az épületen belül a tűzrendészeti és munkavédelmi szabályok betartása egységesen vonatkozik minden az épületben tartózkodó személyre. Az épületen belül a dohányzás nem megengedett. Az épületet tűzkár ellen a Tűzvédelmi szabályzatban foglaltak alapján kell biztosítani. A munkavégzés során a Munkavédelmi szabályzat betartása minden munkatársra kötelező.

8.5.4 MUNKAVÉGZÉS BIZTONSÁGI TERÜLETEKEN

A fokozottan biztonságos területeken csak szakképzett személyzet végezhet munkát. Amennyiben külső személy lép a helyiségbe, az ott tartózkodás idejére a Rendszergazdáknak biztosítania kell a folyamatos felügyeletet (pl.: szerver szoba). Az egyéb biztonsági területeken történő munkavégzések – pl. elektromos központ – biztosítása az Ügyvezető feladata.

8.6 BERENDEZÉSEK VÉDELME

8.6.1 BERENDEZÉSEK ELHELYEZÉSE ÉS VÉDELME

A hálózati aktív eszközök esetében az alábbi rendelkezéseket kell betartani:

- A hálózati aktív eszközöket fizikai behatástól védett helyen kell tárolni.
- Amelyik hálózati aktív eszköznél lehetséges, azt a szerverszobában kell elhelyezni, és a szerverekkel kapcsolatos biztonsági előírásokat kell betartani azokra vonatkozóan is.

A munkaállomásként üzemelő számítógépek fizikai hozzáférésénél az alábbi intézkedéseket kell betartani:

- A munkaállomásokat lehetőség szerint zárható helyiségekben kell tárolni.
- A tárgyaló helyiségekbe fixen csak olyan munkaállomások kerülhetnek, amelyek az operációs rendszeren és a kiszolgáló programokon kívül semmilyen adatot nem tartalmaznak, és csak a használatuk időtartama alatt lehetnek hálózatba kötve a felhasználó hozzáférési jogosultságának megfelelően. Ezen munkaállomásokra az egyes tárgyalások anyagai csak a tárgyalás időtartamára kerülhetnek fel.
- A munkaállomások fizikai telepítésénél gondoskodni kell a lehető legbiztonságosabb – rázkódás-, zuhanásmentes – elhelyezésről.

A felhasználók az informatikai eszközöket nem mozgathatják át más helyiségekbe, kivéve a hordozható informatikai eszközöket (pl. notebookokat). Az IT eszközök mozgatását csak a rendszergazda végezheti.

8.6.2 KÖZMŰSZOLGÁLTATÁSOK

A WebDream szerverterménének kiszolgálói áramellátását szünetmentes tápegységgel kell biztosítani. Az eszközök elhelyezési környezetét a közműszolgáltatásokkal összefüggő kockázatok figyelembevételével kell kialakítani, vagy megválasztani. Az esetlegesen felmerülő kockázatok számbavétele az IBF feladata.

8.6.3 KÁBELBIZTONSÁG

Az adatátvitelt lebonyolító, illetve az információ szolgáltatásokat támogató elektromos energiaátviteli és távközlési kábelhálózatot védeni kell az illetéktelen hozzáféréstől, károsodástól. Az elektromos hálózati kábeleket a falon belül kell vezetni. Amennyiben az nem lehetséges, úgy csatornában a környezettől elzártan kell vezetni. Törekedni kell arra, hogy az informatikai eszközök a lehető legrövidebb vezetékkel csatlakozzanak a falon vagy a padlódobozokban kialakított csatlakozó aljzathoz. Az épület villamossági felülvizsgálatát 3 évente meg kell ismételni. Az infrastruktúra kialakításért és az előírások betartásáért a rendszergazda felel. Az adathálózati végpontokra csak a WebDream eszközei csatlakoztathatók. Idegen számítástechnikai eszköz csatlakoztatása csak az Ügyvezető külön engedélyével történhet.

8.6.4 BERENDEZÉSEK KARBANTARTÁSA

Gondoskodni kell az informatikai eszközpark minden elemének célszerű, rendszeres karbantartásáról (hardver és szoftver eszközök esetében egyaránt) a gazdasági racionalitás és a pénzügyi tervek keretein belül. A fő folyamatot támogató kiszolgálók védelmét lehetőleg redundáns kialakítással kell biztosítani. A berendezések rendszeres karbantartásáért a Rendszergazda felel.

8.6.5 BERENDEZÉSEK BIZTONSÁGA A TELEPHELYEN KÍVÜL

A cél, hogy a telephelyen kívüli berendezések kellő biztonságot nyújtsanak, figyelembe véve a szervezet telephelyén kívül történő munkavégzésből eredő különböző kockázatokat. A telephelyről kiszállított eszközöket kizárólag rendeltetésszerűen szabad használni, továbbá a használat során be kell tartani a WebDream belső szabályzataiban foglaltakat az eszköz használatára vonatkozóan. A hordozható számítógépek elvitelére az alábbi rendelkezések érvényesek:

- A felhasználók alapvetően hordozható számítógépet használnak. A kiadott hordozható számítógépeket az irodából el lehet vinni, ám a munkatársaknak a munkaköri leírásuk elfogadásakor nyilatkozniuk kell az eszköz rendeltetésszerű használatáról is.
- A hordozható számítógépnek a leltárban is meg kell jelenniük, azt leltározási időszakban be kell mutatni.
- Gondoskodni kell a hordozható számítógépek biztonságos szállításáról és tárolásáról. Biztosítani kell, hogy illetéktelenül ne férjen hozzá senki.
- Nyilvános helyen szigorúan tilos a WebDreammel kapcsolatos bizalmas adatokat, információkat tartalmazó hordozható számítógépet felügyelet nélkül hagyni.
- A hordozható számítógépek adattárolóit titkosítani kell.

A berendezések telephelyen kívüli használatára vonatkozó előírások betartását az IBF feladata ellenőrizni.

8.6.6 BERENDEZÉSEK BIZTONSÁGOS SELEJTEZÉSE, ILLETVE ÚJRAFELHASZNÁLÁSA

Valamennyi olyan berendezést, amely tárolóeszközt foglal magában, ellenőrizni kell annak biztosítása érdekében, hogy az érzékeny adatok és engedélyezett szoftverek a selejtezést megelőzően eltávolításra, illetve biztonságos felülírásra kerüljenek. Az ellenőrzés végrehajtása a Rendszergazda feladata, aki írásban igazolja az IBF felé az adathordozó állapotát. Az eszközök leltározását és ennek során a már felesleges eszközök selejtezését évente kell elvégezni.

8.6.7 VAGYONTÁRGYAK KIVITELE

Az asztali PC-k és egyéb informatikai eszközök WebDream által használt irodából történő elvitele minden felhasználó számára szigorúan tilos. Ez alól kivételt képeznek

- a személyes használatra kiadott hordozható eszközök,
- a távoli használatra kapott munkaállomások,
- az Ügyvezető engedélyével történő szállítás.

9 A KOMMUNIKÁCIÓ ÉS AZ ÜZEMELTETÉS IRÁNYÍTÁSA

9.1 ÜZEMELTETÉSI ELJÁRÁSOK ÉS FELELŐSSÉGI KÖRÖK

9.1.1 DOKUMENTÁLT ÜZEMELTETÉSI ELJÁRÁSOK

Az üzemeltetési eljárásokat dokumentálni kell és minden olyan felhasználó számára hozzáférhetővé kell tenni, akiknek arra szükségük van. (pl.: rendszergazdák, adatgazdák). Az üzemeltetési eljárások dokumentálását és karbantartását a Rendszergazda végzi. Az eljárások ellenőrzését az IBF-nek eseti rendszerességgel (pl. verzióváltás) kell elvégeznie.

Az üzemeltetési dokumentumnak tartalmaznia kell a következőket:

- a szolgáltatást, amit az eszköz, rendszer kiszolgál,
- az informatikai erőforrások naprakész összerendelését (topológiát),
- a telepítőkészlet fellelhetőségét,
- a telepítés főbb lépéseit
- a rendszer főbb feladatait,
- a rendszer főbb paraméterezését,
- a rendszer napi rendszergazdai szintű üzemeltetési feladatait
- és az adatmentés módját.

9.1.2 VÁLTOZÁSKEZELÉS

Az éles információ-feldolgozó eszközök és rendszerek változtatásaira vonatkozóan bekövetkező tervezett és azonnali változáskezelést dokumentálni szükséges. Tesztkörnyezetben történő változást nem kell dokumentálni.

A részletes feladatok leírása a „Fejlesztési és változáskezelési szabályzat”-ban található.

9.1.3 AZ ÜZEMELTETÉSI FELADATOK, KÖTELEZETTSÉGEK ELHATÁROLÁSA

A feladatköröket és felelősségi területeket szét kell választani az informatikai erőforrásokhoz történő illetéktelen hozzáférés, illetve az azokkal való visszaélés lehetőségeinek csökkentése érdekében. Az informatikai szerepkörök összeférhetetlenségi mátrixát el kell készíteni és amennyiben változások történnek az informatikai tevékenységek ellátásában, úgy azt aktualizálni szükséges. Az alkalmazáshoz történő hozzáférés az adatgazda felelősségi köre. Az alkalmazói rendszerhez történő hozzáférések beállíttatása az adatgazda feladata, a hozzáférések ellenőrzését az IBF-nek kell elvégeznie.

9.1.4 FEJLESZTŐI ÉS ÜZEMELTETŐI HOZZÁFÉRÉSEK KÜLÖNVÁLASZTÁSA

A fejlesztői szerepkör és az üzemeltetői szerepkör egymással összeférhetetlen. A tesztkörnyezetet az éles üzemű környezettől el kell választani. Ezen szerepköröket szét kell választani. A fejlesztő csak a fejlesztői környezethez férhet hozzá. Az alkalmazás csak dokumentált tesztelést követően kerülhet át az éles üzemű környezetbe. A fejlesztőnek az éles üzemű rendszerhez nem lehet hozzáférése. Az IBF feladata az ellenőrzések, kontrollok betartatása.

9.2 RENDSZERTERVEZÉS ÉS ELFOGADÁS

9.2.1 KAPACITÁSMENEDZSELÉS

Az adatgazda számára megfelelő eszközt kell biztosítani ahhoz, hogy a rendszerrel szemben elvárt követelmények teljesítésének kapacitásigényét meg tudja fogalmazni. A vizsgálat irányelvei a következők:

- üzleti szintű kapacitás igény,
- jövőbeni üzleti igények méretezése,
- szolgáltatás szintű kapacitás igény,
- szolgáltatási teljesítmény felügyelete,
- erőforrás szintű kapacitás igény,
- komponensek működtetése, kihasználtságuk felügyelete, elemzése és jelentése.

Az adatgazda ezen tevékenységéhez szükséges erőforrások biztosítása az Ügyvezető Igazgató feladata.

9.2.2 RENDSZEREK ELFOGADÁSA, ÁTVÉTELE

A rendszerek elfogadására és átvételére a dokumentált fejlesztői és felhasználói teszteket követően kerülhet sor. Az erre vonatkozó részletes szabályokat a „Fejlesztési és változáskezelési szabályzat” tartalmazza.

9.3 VÉDELEM A ROSSZINDULATÚ ÉS MOBIL KÓDOK ELLEN

A szerverek, kiszolgálók és munkaállomások vírusvédelmét a jelen szabályozás szerint kell biztosítani.

A WebDream a folyamatos üzletmenetet és az azt veszélyeztető kockázatokat figyelembe véve a rosszindulatú kódok és vírusok elleni védelmét az alábbi elv alapján alakítja ki.

Csak az informatikai eszközök belépési pontjain végez a WebDream ellenőrzést. Ezek a belépési pontok:

- munkaállomás és laptop (USB, CD/DVD),
- internetes kommunikációt végző proxy,
- elektronikus levelezést végző tartalomszűrő.

Azokon a szervereken és munkaállomásokon, amelyeknek közvetlenül nincs külső belépési pontja, vírusvédelmi rendszer nem kerül kialakításra.

A vírusvédelmet teljes, vásárolt és támogatással rendelkező termékkel kell megoldani, mely terméknek minimum az alábbi elvárásokat kell teljesítenie:

- központi naplózási és riasztási funkciók paraméterezhetősége,
- internet, levelező rendszer, fájlszerver, irodai alkalmazás, hordozható adattárolók, mobil eszközökön való hibamentes futás az adott operációs rendszeren,
- időzített online/offline keresési, ellenőrzési lehetőség,
- minta alapú és heurisztikus keresési, ellenőrzési funkciók megvalósítása.

A felsorolt alapkövetelmények munkaállomásokon (PC, notebook), okos telefonokon, valamint szervereken futó védelmi megoldásokra egyaránt vonatkoznak.

9.4 BIZTONSÁGI MENTÉS

A WebDream legfőbb értékét a számítógépeken tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése. A mentés célja egyrészt a ritkán használt adatok, illetve a kulcsfontosságú adatok (pl.: adatbázis) rendszerezett, biztonságos és visszakeresésre alkalmas tárolása, másrészt, hogy előre nem látott adatsérülés, vagy adatvesztés esetén a sérült adatok a korábban, szabályozott módon eltárolt mentésekből hiánytalanul visszaállíthatók legyenek. Mentés során mind az egyes rendszerek adatait, mind az operációs rendszer, adatbázisrendszer és szoftverkörnyezet beállításait is tárolni kell. A mentésekkel kapcsolatos feladatok megfelelő végrehajtásának ellenőrzését az IBF végzi.

A WebDream rendelkezik „Mentési szabályzat”-tal, amelyben a mentéssel kapcsolatos feladatok pontosan meg vannak határozva.

9.5 HÁLÓZATBIZTONSÁG KEZELÉSE

9.5.1 HÁLÓZATOK VÉDELME

A hálózatokat a fenyegetésektől való megóvásuk, a hálózatot használó rendszerek és alkalmazások – beleértve az átvitel alatti információt – biztonságának fenntartása érdekében megfelelő irányítás és ellenőrzés alatt kell tartani.

A tűzfalakra vonatkozó intézkedéseket a Rendszergazda hajtja végre, ő működteti a rendszert és dokumentálja a rendszerdokumentációban, amit az IBF ellenőriz. A tűzfal üzemeltetésére vonatkozó eljárások, a tűzfal konfigurációs beállításai kiemelt üzleti titkot képeznek. A rendszerdokumentációnak a következőket kell tartalmaznia:

- a tűzfalak konfigurálásának, ellenőrzésének módját;
- a statisztikai adatgyűjtést, ezen adatok feldolgozását, a jelentések tartalmát;
- a riasztási és a mentési rendszer specifikációját és működését;
- a jelentési kötelezettségeket;
- az adminisztrátorok jogait és kötelezettségeit.

Az egyes zónák közötti forgalomra vonatkozóan irányonként pontosan meg kell határozni az alábbiakat:

- milyen szolgáltatások (portok) használata engedélyezett,
- milyen erőforrásoktól milyen erőforrásokhoz, célpontokhoz lehet hozzáférni,
- a felhasználókat kell-e (és ha igen, milyen módon) azonosítani,
- milyen információkat kell naplózni.

A belső hálózatot tűzfalaknak kell védenie, amelyekre a következő előírások vonatkoznak:

- Biztosítson lehetőséget a gyanús tevékenység észlelésére, valamint az azonnali beavatkozásra, riasztásra.
- Kezelése, üzemeltetése legyen egyszerű, könnyen elsajátítható.
- Architektúrája legyen nyitott, biztosítson lehetőséget olyan kiegészítésekre, fejlesztésekre, amelyek a mindenkori igények kielégítésére szolgálnak.

A tűzfalak fizikai elhelyezésére, konfigurációik mentésére a szerverekre vonatkozó szabályok érvényesek. A tűzfalmegoldás olyan hardver platformon és operációs rendszeren fusson, amelyről az üzemeltetéssel megbízott Rendszergazda magas szintű szakmai tudással rendelkezik, és amelyet szakképzett módon tud kezelni. A tűzfalon keletkező napló (log) állományokat

a Rendszergazdának rendszeresen ellenőriznie kell. A betörésre utaló bejegyzéseket írásban jelenteni kell az Ügyvezető valamint az IBF felé. A Rendszergazda veszélyhelyzetben vagy ennek gyanúja esetén jogosult a belső és külső rendszerek közötti kapcsolat megszakítására, majd ezt haladéktalanul jelentenie kell az Ügyvezetőnek valamint az IBF-nek.

A tűzfalak üzemeltetésére és karbantartására külső szolgáltatóval kötött szerződéssel kell rendelkeznie a WebDreamnek. A szerződés megkötése és számonkérése az Ügyvezető feladata.

9.5.2 HÁLÓZATI SZOLGÁLTATÁSOK BIZTONSÁGA

A WebDream kettő, egymástól fizikailag elválasztott hálózattal rendelkezik.

- LAN általános
- DMZ

A WebDream rendelkezik továbbá internet eléréssel és bérelt vonali kapcsolatokkal.

A hálózatokra vonatkozó rendelkezések az alábbiak:

- A helyi hálózatra kötött munkaállomás külön engedély nélkül nem rendelkezhet egy időben LAN és modemes, vagy Wifi kapcsolattal.
- A LAN-ba kötött gépeket (szervereket) kívülről (internet, egyéb, nem WebDream hálózat) csak VPN kapcsolat kiépítésével szabad elérhetővé tenni és csak a WebDream által biztosított munkaállomás, vagy laptop használatával.

A DMZ-be helyezett gépeket korlátozott módon elérhetővé lehet tenni az internetről, vagy egyéb, nem WebDream hálózatról. A DMZ-ben csak olyan szervereket lehet elhelyezni, amelyeket funkciójuk miatt elérhetővé kell tenni külső hálózat felől, de semmiképp nem lehet a DMZ-ben olyan szervereket elhelyezni, amelyek üzletileg kiemelten fontos adatbázisokat tartalmaznak.

A hálózat aktuális felépítéséről szerkezeti ábrát kell készíteni, amelyben az alábbiaknak kell szerepelnie:

- tűzfal, és a hozzá kapcsolódó hálózati elemek (LAN, DMZ stb.),
- az összes aktív hálózati elem (switchek, routerek, média konverterek, átjárók),
- szerverek, adattárak.

A fenti eszközök típusát, hálózati nevét, IP címét, valamint fizikai helyét is fel kell tüntetni, vagy a nyilvántartásukra való hivatkozást kell elhelyezni. A nyilvántartást az iTop rendszerben a rendszergazdának kell karbantartania.

9.5.3 HÁLÓZAT BIZTONSÁG, VEZETÉK NÉLKÜLI HÁLÓZAT

A WLAN (Wifi) hálózat kialakításakor az ezt megvalósító eszközök által nyújtott lehetőleg legmagasabb biztonsági előírásoknak kell megfelelni, annak érdekében, hogy ezekkel biztosítani lehessen a WebDreamhez érkező partnerek, vendégek számára a nyilvános internet hálózati elérhetőségét.

WLAN hálózatra vonatkozó előírások:

- Vezeték nélküli felhasználót / munkaállomását mindig azonosítani kell.
- A WLAN és az IP kapcsolat felépítése csak a mobil végponton előre beállított konfigurációnak megfelelő, valós WLAN hálózaton keresztül valósuljon meg.
- Titkosításához minimum a WPA-TKIP, vagy WPA2-AES kulcsmenedzsment-titkosítás párosítás használatával biztosítson lehetőséget a csatlakoztatásra, a végponti kliens tudásának megfelelően.
- A File and print sharing protocol nem kerülhet továbbításra.

- Kizárólag patch-elt és aktív vírusvédelemmel rendelkező munkaállomások, notebookok csatlakozhatnak a WLAN-hoz.
- A belső LAN-hoz kapcsolódás nem engedélyezett.
- A guest userhez kapcsolódó jelszót rendszeresen (negyedévente) módosítani szükséges.
- Guest userek forgalmát, a WebDream belső helyi hálózatától teljesen elkülönítve kell kezelni.
- Csatlakozás előtt a vendégek figyelmét fel kell hívni arra, hogy a WebDream nem vállal semmiféle felelősséget a nyílt Wifi hálózat biztonságára vonatkozóan.

9.5.4 SAJÁT ESZKÖZ HASZNÁLATA (BYOD - BRING YOUR OWN DEVICE)

A belsős, külsős munkatársak saját tulajdonában levő notebook, tablet, okostelefon irodahelységbe történő bevitele alapesetben nem tiltott, viszont annak csatlakoztatása a LAN/WLAN-hoz tiltott és nem engedélyezett! A WebDream telephelyén a BYOD munka célra történő használata tiltott, kizárólag az IT által biztosított nyílt, az éles hálózattól teljesen elszeparált ún. “guest” WLAN-ra történő kapcsolódás engedélyezett.

9.6 ADATHORDOZÓK KEZELÉSE

A WebDream hivatalos adatforgalmazásában felhasználásra kerülő adathordozókon történő adatátvitel esetén a következő előírásokat kell betartani.

9.6.1 AZ ELTÁVOLÍTHATÓ ADATHORDOZÓK KEZELÉSE

A szállítás folyamán az adathordozót sérüléstől védő, kulccsal zárható borítással kell ellátni. Az adathordozó mellé egy kísérőjegyzéket kell mellékelni, amely tartalmazza a feladót, a célt, rövid ismertetőt az adathordozó tartalmáról, valamint a küldő személy cégszerű aláírásával (és esetleges pecsétjével) van ellátva. Az adathordozó csak akkor dolgozható fel, ha az előírt kritériumoknak megfelel.

Mágneses adathordozó esetén a védelemnek ki kell terjednie az erős mágneses tér okozta adatvesztés megelőzésére is.

A beérkezett (és kimenő) adathordozón első (és utolsó) lépésben mindig vírusellenőrzést kell végezni.

A kapott dokumentum alapján ellenőrizni kell a kapott állományokat.

A mentésre, archiválásra és bármilyen szintű elektronikus információtárolásra használt adathordozók (egyéb adathordozók) esetében be kell tartani az alábbi intézkedéseket:

- Az adathordozók várható élettartamának, és a tárolt adatok, információk elévülési idejének figyelembevétele mellett évente felül kell vizsgálni a tárolt adatok rendelkezésre állását, illetve gondoskodni kell azok új adathordozóra történő duplikálásáról. (A Rendszergazda teszteli az adatok rendelkezésre állását.)
- A nem használható adathordozókon tárolt információkat visszaállíthatatlan módon törölni kell. Adott esetben az adathordozó fizikai megsemmisítésével.
- A felülvizsgálatot jegyzőkönyvezni kell, és amennyiben szükséges, a további rendelkezésre állást biztosítani kell. Az adathordozók kezelésével kapcsolatos előírások betartatásáért az IBF felel.

9.6.2 ADATHORDOZÓK SELEJTEZÉSE

A számítógépes feldolgozás során hibás, vagy feleslegessé vált, aktualitását vesztett mágneses és optikai adathordozókat selejtezés útján kell megsemmisíteni. A selejtezésre vonatkozó előírások a „Mentési szabályzat”-ban részletesen leírásra kerültek.

9.6.3 RENDSZERDOKUMENTÁCIÓ VÉDELME

A rendszerdokumentációk tárolása elektronikus úton egy korlátozott jogosultsággal elérhető mappában történik. A mappához különböző jogosultsági engedélyekkel férhetnek hozzá:

- a rendszergazdák,
- az adatgazdák,
- és a szakterületi vezetők.

A rendszerdokumentációk tárolási folyamatának kialakítása és ellenőrzése az IBF feladata. A rendszerdokumentációk hálózati megosztott mappába történő feltöltéséért és a sértetlenség megőrzéséért a Rendszergazda felel. A dokumentációk rendelkezésre állásáért szintén a rendszergazda tartozik felelősséggel.

9.7 INFORMÁCIÓCSERE

9.7.1 FIZIKAI ADATHORDOZÓK SZÁLLÍTÁSA

A hordozható számítógépes eszközök (notebook, pendrive, DVD/CD) külső felhasználása során különös gondot kell fordítani az eszközök fizikai és adatvédelmére. Ezeket az adathordozókat titkosítani kell. Amennyiben ez nem lehetséges, akkor a rajtuk lévő állományokat kell titkosítani. A WebDream tulajdonát képező adathordozókat semmilyen esetben sem szabad személyes célra használni. A privát adathordozók munkahelyi használata külön engedélyhez kötött.

Az adathordozók érzékenyek a külső fizikai, mágneses behatásokra, ezért tilos azokat meghajlítani, törni, mágneses eszközök közelébe vinni (és fordítva!). Óvni kell az adathordozókat bárminemű folyékony anyagtól (italok, virágok öntözésére szolgáló víz, vegyszerek) és fokozottan védeni kell a porszennyeződésektől. Az adathordozókat használaton kívül minden esetben el kell zárni.

A leselejtezett adathordozókat fizikailag meg kell semmisíteni. Ezen adathordozók mind munkahelyi, mind otthoni használata tilos. Az adathordozók (pendrive, DVD/CD) elvesztése esetén, amennyiben azokon nem publikus adatok voltak, haladéktalanul értesíteni kell az Ügyvezetőt és az IBF-et. Az előírások betartásának ellenőrzése az IBF felelőssége.

9.7.2 ELEKTRONIKUS ÜZENETEK KÜLDÉSE/FOGADÁSA

9.7.2.1 AZ ELEKTRONIKUS LEVELEZÉS BIZTONSÁGA

A WebDream a belső elektronikus levelezést napi szinten, a WebDreamen belüli kapcsolattartásra, üzleti folyamatok támogatására, kifelé történő levelezést pedig az ügyfelekkel, külső kapcsolatokkal történő kapcsolattartás egyik nélkülözhetetlen eszközének tekinti.

Kimenő levelezések alapszabályai:

- Hivatalos, üzleti tevékenységgel kapcsolatban kizárólag a „@webdream.hu” domain címről küldött elektronikus levelezés engedélyezett.

- Ha a levéltörzsben (body), valamint a csatolmányban (attachment) üzleti titkot vagy ügyfél személyes adatát tartalmazó információ található, akkor azt védeni, titkosítani szükséges (pl. TLS használatával).
- A levél tárgyában üzleti titkot, védendő információt nem szabad megadni.
- A levelezés során ügyelni kell arra, hogy a levél a WebDreamet képviseli, így minden esetben ennek megfelelően kell fogalmazni.
- Küldés előtt a címzett email címét minden esetben ellenőrizni kell.
- A hivatalos lábléc törlése nem engedélyezett.

Beérkező elektronikus levelekre vonatkozó alapszabályok:

- A bejövő elektronikus levelek vírusfertőzöttek lehetnek, ezért azokat minden esetben ellenőrizni kell. Pozitív kimenet (vírusos levél!) esetén azonnal értesíteni kell az IT-t.
- Ún. „spam" (kéretlen (reklám) levél, levélszemét) vagy gyanús, nem ismert forrásból származó levelek megnyitása NEM javasolt.
- A kinézetre és feladó alapján ismeretlennek tűnő, vagy nyelvtani hibákkal megírt levél esetén azonnal értesíteni kell az IT-t.

Általában az ingyenes, WEB alapú email, csoportmunka szolgáltatások használata üzleti adatokkal NEM engedélyezett. Ilyen jellegű tevékenységre kizárólag a WebDream által vásárolt vagy ingyenesen igénybe vett jogtiszta vagy fejlesztett alkalmazások használhatók vagy olyan külső szolgáltatások, melyek esetében a szolgáltató szerződésben garantálja az adatvédelem biztosítását.

A WebDream az elektronikus levelezés céljára az Outlook levelező szoftvert alkalmazza. Ebből eredően az általános informatikai biztonsági szempontok teljesítése, vagyis a rendszerhez és elemeihez való ellenőrzött hozzáférés, az erőforrások használatának naplózása, az adatok titkosságának biztosítása, az adatok integritásának védelme, az elérhetőség és a megbízhatóság, valamint a következetesség és az elvárt működés a teljes rendszer hasonló követelményeinek kielégítésén keresztül teljesül.

A levelezőrendszer felhasználóival kapcsolatos teendők ellátása az általános felhasználó kezelésen belül történik. A levelező rendszer naplózása biztosítja az elektronikus levélforgalom ellenőrizhetőségét. A naplófájlokat illetve a rendszer elektronikus üzeneteit az esetleges problémák felderítése céljából folyamatosan elemezni kell. A szabályok betartását folyamatosan ellenőrizni kell.

A levelező kliensekkel letöltött emailek központilag a szerveren kerülnek tárolásra. Gondoskodni kell a vírusvédelemnek a levelező szolgáltatásokra történő kiterjesztéséről, ezen keresztül a központi vírusadatbázis letöltéséről és a munkaállomások közötti automatikus szétosztásáról. A levelezéssel kapcsolatos szabályok végrehajtásáért a rendszergazda felel.

9.7.2.2 BELSŐ ELEKTRONIKUS LEVELEZÉS SZABÁLYAI

A WebDream belső levelezésének elsődleges feladata a munkafolyamatok automatizálása, felgyorsítása.

Annak érdekében, hogy az elektronikus levelezés sértetlenségét és bizalmasságát a jelenlegi technológiai környezetben biztosítani lehessen az alábbi szabályok betartása, betartatása kötelező:

- Minden felhasználó egyetemlegesen felel a hozzá rendelt felhasználói azonosítóval elkövetett visszaélésekért.

- Tilos a felhasználóknak olyan tartalmú elektronikus levelet a WebDream informatikai rendszeréből küldeni, amely a WebDream érdekeivel ellentétes.

Az elektronikus levél a papír alapú levelezéssel esik egy tekintet alá. A WebDream által hivatalosan támogatott levelező rendszeren kívül más, elektronikus levelezést (Freemail, Hotmail stb.) belső hivatalos kommunikációra, valamint a WebDream munkaállomásait a munkakörhöz nem kapcsolódó feladatra használni tilos. A levelek kezelése a levelező programon belül a felhasználó felelőssége. Az Ügyvezető Igazgató jogosult az üzleti kockázatok értékelése alapján meghatározni azoknak az információknak a körét, amelyek elektronikus levelezés útján történő forgalmazása korlátozható, továbbá az IBF feladata ellenőrizni az előírásoknak való megfelelőséget.

9.7.2.3 6.7.2.3. KIMENŐ ELEKTRONIKUS LEVELEZÉS HARMADIK SZEMÉLLYEL

A WebDream külső levelezésének elsődleges feladata a munkafolyamatok automatizálása, felgyorsítása és kapcsolattartás az ügyfelekkel, hatóságokkal. Elektronikus levélben jelentős anyagi kiadással járó kötelezettséget vállalni nem lehet, ha a WebDream és a harmadik fél erről külön nem állapodik meg.

A WebDreamtől személyes adat, üzleti és közbeszerzési titok harmadik személy számára elektronikus levélben csak titkosított formában továbbítható. Személyes adatok esetében az érintett személy hozzájárulása is szükséges.

Az Ügyvezető kockázatelemzése alapján a Rendszergazda az egyes fájltípusok, illetve az ún. "levélszemét" forgalmát a levelező szerver beállításaival letilthatja, vagy blokkolhatja. Amennyiben munkavégzési okból ilyen jellegű fájl forgalmára van szükség, a tiltás feloldását írásban kell kérni. A WebDream korlátozza a küldhető fájlok méretét. Jelenleg ez 25 MB.

Mivel mind az email, mind az internet forgalom a WebDream által biztosított eszközökön történik, és ezen eszközök biztosítása a WebDream folyamatok ellátásával kapcsolatos tevékenység megkönnyítésére irányul, az elektronikus levél egy tekintet alá esik a WebDreamhez érkező bármely más hivatalos irattal. Az Ügyvezető Igazgató utasítására a Rendszergazda jogosult a WebDream email címeken (arról érkezett, vagy oda továbbított) bonyolított levelezést, illetve az interneten látogatott oldalakat, temporális internet fájlokat, letöltéseket a felhasználó gépén, vagy a szerveren ellenőrizni. Ennek lehetőségéről az érintetteket tájékoztatni kell, valamint a felhasználókat nyilatkoztatni kell arról, hogy ezen adatok ellenőrzését a fentiek szerint tudomásul veszik és elfogadják.

9.8 NYILVÁNOSAN HOZZÁFÉRHETŐ INFORMÁCIÓK

A nyilvánosan közzétett információk, úgymint a WebDream weboldalán elhelyezett tartalom, jelentős értéket képvisel az ügyfelekkel és a leendő ügyfelekkel való kapcsolattartás céljából. Ebből kifolyólag megfelelő biztonsági védelmet kell kidolgozni az ott megjelenített tartalmak hitelességének és rendelkezésre állásának biztosítása érdekében. A szolgáltatással szemben támasztott követelményeket meg kell fogalmazni a szerződésben. A szerződésben foglaltak betartását időközönkénti audit vizsgálatokkal szükséges ellenőrizni. A rendelkezések betartatásáért az IBF felel.

9.9 FIGYELEMMEL KÖVETÉS (MONITORING)

9.9.1 AUDIT NAPLÓZÁSA

A számon kérhetőség és az auditálhatóság biztosítása érdekében olyan naplózási rendszert kell kialakítani, amely biztosítja a WebDream informatikai rendszereiben bekövetkezett fontosabb események utólagos kivizsgálását, különös tekintettel azokra, amelyek a biztonságot érintik. A naplózásra vonatkozó általános követelményeket és a naplózással kapcsolatos részletes szabályokat a „Naplózási szabályzat" tartalmazza. A naplózási funkció működtetéséért a Rendszergazda felel. Az előírásoknak való megfelelőséget az IBF feladata ellenőrizni.

9.9.2 ÓRAJELEK SZINKRONIZÁLÁSA

A szervezeten belül, illetve adott biztonsági tartományban működő valamennyi érintett információfeldolgozó rendszer órajelét a WebDream központi tartományvezérlőjéhez kell szinkronizálni. a központi tartományvezérlőt pedig egy külső órajelet szolgáltató szerverrel kell összhangban tartani. A rendszergazda felel e tevékenység zavartalan működéséért. Az IBF feladata ellenőrizni a tevékenység előírás szerinti működését.

10 HOZZÁFÉRÉS ELLENŐRZÉS

10.1 FELHASZNÁLÓI HOZZÁFÉRÉS IRÁNYÍTÁSA

Az operációs rendszerekhez való hozzáférést biztonságos bejelentkezési eljárásokkal kell ellenőrzés alatt tartani. A felhasználói bejelentkezésnek felhasználónévvel és egyedi jelszóval kell történnie. A felhasználó és a rendszer között kialakított kapcsolatot minden esetben titkosítani szükséges. A rendszer működtetésének felügyelete és a jelen előírásoknak a betartatása az IBF feladata.

10.1.1 FELHASZNÁLÓK REGISZTRÁLÁSA

A hozzáférések és jogosultságok menedzselése a WebDream szempontjából kiemelkedően fontos biztonsági feladat, amelyre vonatkozóan a „Jogosultságkezelési szabályzat" tartalmaz részletes előírásokat. Az igényléseket az IBF-nek a „Jogosultságkezelési szabályzat"-ban megfogalmazott előírások szerint ellenőriznie kell.

10.1.2 FELHASZNÁLÓI AZONOSÍTÓKHOZ KAPCSOLÓDÓ BIZTONSÁGI ALAPELVEK

A címtárban és egyes integrált vagy helyi alkalmazásokban kezelt felhasználói azonosítókkal *(felhasználó nevekkel)* kapcsolatos alapelvek az alábbiakban kerültek meghatározásra:

- Alapesetben minden munkavállalónak az éles környezetben kizárólag egy megszemélyesített felhasználói azonosítója lehet.
- Csoportszintű (group) és felhasználó (user) szinten vagy munkaállomásra (workstation) definiált policyk, scriptek kiadásra kell, hogy kerüljenek.
- Tartós távollét idejére és kilépést követően a felhasználót azonnal inaktívvá kell tenni.
- A felhasználóval kapcsolatos létrehozási, módosítási, törlési műveletet naplózni kell.
- A minimum elv betartása szerint, igényfelmérést követően az adott feladathoz szükséges speciális jogokat és korlátozásokat *(pl. időbeli, hálózati)* be kell állítani.

10.1.3 JELSZÓHASZNÁLAT ÁLTALÁNOS ALAPELVEI

A jelszavak kezelésénél az alábbi alapszabályokat kell betartani:

- A jelszavakat mindig titokban kell tartani, kiadni senkinek és semmilyen formában nem lehet. A jelszóról tilos mások előtt beszélni.
- Tilos közös jelszavakat használni. Ez alól kivételt képeznek a fiók létrehozásakor megadott jelszavak, amelyeket a felhasználónak első bejelentkezésekor meg kell változtatnia.
- A jelszót nem szabad leírni és elérhető helyen tárolni *(pl. post-it, naptár, cetli a táskában).*
- A jelszót tilos számítógépes rendszeren titkosítás nélkül (pl. egyszerű szövegfájlban) tárolni.
- A jelszót tilos telefonon vagy e-mail-ben továbbítani.
- A jelszót tilos más személynek átadni, más felhasználó jelszavával belépni.
- Ne utaljunk a jelszó tartalmára (pl. „a kedvenc filmem címe").
- Tilos a programok jelszó megjegyző funkcióját használni.
- A jelszót tilos kérdőívekbe, űrlapokba írni.
- Ha a jelszó kompromittálódott, vagy erre utaló jeleket lehet észlelni, azonnal meg kell változtatni, és értesíteni kell a Rendszergazdát.
- A jelszavakat rendszeresen és időszakosan cserélni kell.
- Az induló jelszót az első bejelentkezéskor meg kell változtatni.
- Sikertelen próbálkozás után a felhasználói fiók 15 percre zárolandó.
- Ahol lehetséges, a jelszavakra vonatkozó alapszabályokat *(jelszóhossz és komplexitás, rendszeres jelszócsere, előző jelszavak megadásának tilalma)* az adott informatikai rendszer segítségével ki kell kényszeríteni.

10.1.4 JELSZÓKEZELÉS ÁLTALÁNOS SZABÁLYAI

Minden felhasználó személyesen felel a saját azonosítójával végrehajtott tevékenységekért, a jelszót harmadik személynek, munkatársnak nem adhatja ki, a jelszóval történő visszaélés esetén egyetemleges felelősséget vállal a visszaélő személlyel.

A jelszóhasználatra vonatkozó rendelkezéseket a rendszerek beállításaival kell támogatni. Ennek beállítását az adott rendszer/alkalmazás gazdájának kell elvégeznie.

A jelszóvédelemnek biztosítania kell:

- a felhasználók számára, hogy a jelszavakat megváltoztathassák,
- a jelszavak bonyolultságával kapcsolatos követelmények kikényszerítését,
- az azonosítás protokollja a lehallgatás, ismétléses támadás elleni védelmet,
- jelszavak rejtjelezett tárolását, azaz a hozzáférési rendszernek tilos bármilyen formában a jelszót megjelenthetővé tennie,
- sikeres és sikertelen bejelentkezések, jelszóváltoztatások naplózását,
- a hozzáférés korlátozását meghatározott időszakra (pl.: munkaidőre),
- hogy a hozzáférési adatok törlése oly módon történjen, hogy a jelszó adatbázis esetleges visszaállítása esetén se legyen mód a törölt felhasználói jogosultságok visszaállítására.

10.1.5 FELHASZNÁLÓI JELSZÓKÉPZÉS SZABÁLYAI (KOMPLEXITÁS)

A jelszó:

- kialakítása során kerülni kell az ékezetes betűk, valamint a „@” karakterek használatát az általánosan elterjedt hozzáférési rendszerek fogyatékosságai miatt,
- minimális hossza 8 karakter legyen,
- tartalmazzon legalább egy számot, valamint kis- és nagybetűt egyaránt,
- ne lehessen szótárból választott szó, különös tekintettel az angol és a magyar szótárra,
- nem lehet azonos a felhasználói azonosítóval,
- nem lehet az informatikai rendszerben ismert parancs vagy alkalmazás neve,
- megváltoztatása legalább 90 naponta legyen kikényszerítve,
- megváltoztatásakor a rendszer biztosítsa, hogy az új jelszó ne lehessen azonos az előző 12 jelszó egyikével sem,
- nem tartalmazhatja a belépési azonosítót

Az előírások betartásának ellenőrzése az IBF feladata.

10.1.6 FELHASZNÁLÓI JELSZAVAK KEZELÉSE ÉS ELLENŐRZÉSE

A jelszavakkal és hozzáférésekkel kapcsolatos szabályozás a „Jogosultságkezelési szabályzat”-ban került rögzítésre.

10.2 FELHASZNÁLÓI FELELŐSSÉGEK

10.2.1 JELSZÓHASZNÁLAT

A felhasználóktól meg kell követelni, hogy a jelszavak kiválasztásában és használatában a jó biztonsági gyakorlatot kövessék. Minden felhasználó jelszavát illetéktelenektől gondosan védeni kell. A felhasználók jelszavát a felhasználón kívül senki, még a Rendszergazda sem ismerheti. Amennyiben rendszergazdai teendők merülnek fel egy felhasználó gépén, a felhasználónak kötelessége ott tartózkodni, hogy szükség esetén a nevével be tudjon lépni a rendszergazda. Ha a Rendszergazda megismerte a felhasználó jelszavát, köteles új, a következő belépéskor kötelezően megváltoztatandó jelszót beállítani.

Ha a felhasználó nem tartózkodik elérhető közelségben, a Rendszergazdának új, ideiglenes jelszót kell létrehoznia a felhasználó számára/nevére, aminek a segítségével elvégezheti a felhasználó személyes beállításait. Miután végzett a feladatával, a Rendszergazdának a rendszert úgy kell beállítania, hogy a felhasználónak az első bejelentkezésekor azonnal meg kelljen változtatnia a jelszavát.

A jelszót soron kívül meg kell változtatni, ha illetéktelen (más) személy tudomására jutott illetve juthatott, vagy a felhasználó elfelejtette. A változtatást a változtatási igény értelemszerű kitöltésével kell kérvényezni. A jelszó megváltoztatását soron kívül, a megfelelő dokumentum – Rendszergazdához történő kézbesítését követően – 30 percen belül el kell végezni.

10.2.2 ŐRIZETLENÜL HAGYOTT FELHASZNÁLÓI BERENDEZÉSEK, TISZTA KÉPERNYŐ POLITIKA

Arra az esetre, ha a felhasználó napközben magára hagyja a gépét, zárolást vagy jelszavas képernyővédőt kell alkalmaznia.

10.3 HÁLÓZATI SZINTŰ HOZZÁFÉRÉS ELLENŐRZÉS

10.3.1 HÁLÓZATI SZOLGÁLTATÁSOK HASZNÁLATÁRA VONATKOZÓ SZABÁLYZAT

A határvédelem megfelelő üzemeltetése és működésének biztosítása érdekében a WebDream mind külső, mind pedig belső hálózatának rendelkezésre állása és biztonságos működése is elengedhetetlen. A WebDream határvédelmi rendszerének (tűzfalak, IDS, IPS, vírusvédelem stb.) üzemeltetésével kapcsolatos szabályozását több szabályzatban rögzítette. Ilyen a változáskezelésre és a naplózásra vonatkozó szabályzat. A határvédelmi rendszer működtetéséért a Rendszergazda tartozik felelősséggel, aki köteles:

- a hálózat működőképességét folyamatosan felügyelni, a beérkező riasztásokat haladéktalanul kivizsgálni;
- a WebDream épületén belül kialakított irodáiban a LAN hálózat meghibásodása esetén a hibaelhárítást haladéktalanul megkezdeni;
- az adathálózati aktív eszközök meghibásodása esetén haladéktalanul értesíteni a támogató céget, azt utasítani a hibaelhárításra;
- az előzőleg felsorolt eseményekről írásos feljegyzést készíteni, és a hibajavítás elvégzése után a munkalap másolatát / iTop jegyet eljuttatni az IBF-hez;

10.3.2 FELHASZNÁLÓ HITELESÍTÉSE KÜLSŐ CSATLAKOZÁSOK ESETÉN

A külső hozzáférésnek minden esetben kétfaktoros azonosítás útján kell történnie. A kommunikációs csatornát titkosítani kell. A rendszer kialakításáért a Rendszergazda felel. A követelményeknek való megfelelést az IBF ellenőrzi.

10.3.3 TÁVOLI MUNKAVÉGZÉS A BELSŐ HÁLÓZATON

10.3.3.1 MUNKAÁLLOMÁS CSATLAKOZÁSA VPN HASZNÁLATÁVAL

A belső hálózati erőforrásokhoz való csatlakozás távoli munkavégzés céljából minden olyan munkatárs számára adott, akinek az Ügyvezető erre engedélyt ad. Üzleti partnerek kizárólag az Ügyvezető Igazgató írásbeli engedélyével kaphatnak távoli hozzáférést a rendszerhez (például kiszervezési szerződés mellékleteként). Szállítói partnerek kizárólag az Ügyvezető engedélyével kaphatnak távoli hozzáférést, csak az adott rendszer hibajavításának idejére.

A távoli csatlakozást csak a WebDream által biztosított számítógépekről lehet kezdeményezni.

A távoli munkavégzés során az adatvédelmi követelményeket be kell tartani. Ügyelni kell, hogy a munkavégzés során idegenek ne juthassanak a belső hálózaton tárolt információkhoz.

A távoli számítógépen a belső hálózatról származó állományt csak titkosított módon lehet tárolni.

A csatlakoztatott számítógépet nem szabad felügyelet nélkül hagyni.

A csatlakozáshoz szükséges azonosítókat nem, vagy csak erős titkosítással lehet tárolni a számítógépen. A felhasználó felelőssége biztosítani, hogy a számítógép elvesztése, ellopása esetén se legyen lehetséges idegeneknek a belső hálózatra történő csatlakozás. A távoli munkavégzésből eredő esetleges károkért a felhasználó felelős.

A távoli csatlakozáshoz következő módszer használható:

- Külső számítógép csatlakoztatása a belső hálózatra a hálózat határvédelmi eszközén (tűzfalon) végződtetett, védett és titkosított hálózati kapcsolat (VPN) kialakításával.
- Az azonosításnak kétfaktorosnak kell lennie. Ebből az egyiknek One Time Password elven kell működnie.

10.3.3.2 SZERVER CSATLAKOZÁSA VPN HASZNÁLATÁVAL

Úgynevezett site-to-site szerverkapcsolat kialakítása csak különleges üzleti érdekből, csak az Ügyvezető Igazgató engedélye alapján alakítható ki. Ilyen kapcsolat esetén alkalmazni kell a maximális biztonságot nyújtó technológiai megoldásokat.

A VPN kapcsolat kizárólag a hálózati határvédelmi eszköz (tűzfal) saját VPN megoldásával létesíthető.

A VPN kapcsolatra tűzfalszabályokat kell létrehozni, melyekkel a hálózati forgalom csak a szükséges erőforrások elérésére korlátozható.

A VPN kapcsolat felépítéséhez a csatlakozó eszköz azonosítását lehetővé tevő egyedi név és jelszó párost kell alkalmazni. Amennyiben lehetőség van rá, a kapcsolat kiépítését tanúsítvány alapú hitelesítéssel is meg kell erősíteni. Tanúsítványok alkalmazása esetén a tanúsítványok rendszeres, legalább kétévente történő megújításáról, cseréjéről a Rendszergazda köteles gondoskodni. Amennyiben a tanúsítvány kompromittálódott, vagy ennek veszélye, lehetősége merül fel, a tanúsítványt haladéktalanul le kell tiltani. Az alkalmazott tanúsítványokról a rendszergazda köteles nyilvántartást vezetni (iTop rendszerben), melyben fel kell tüntetni a lejárati dátumot és az eszközt, amelynek a részére a tanúsítvány ki lett adva.

A VPN kapcsolatokat a tűzfalon naplózni kell, mely naplókat a központi naplószerverre kell továbbítani. A sikertelen VPN kapcsolódásokról, kapcsolódási kísérletekről riasztást kell kezdeményezni.

A VPN használat engedélyének lejáratakor, megszűnésekor a tűzfalon az adott eszköz további VPN csatlakozását haladéktalanul le kell tiltani (a felhasználói azonosítót és a számára kiadott tanúsítványt le kell tiltani).

10.3.4 HÁLÓZATHOZ VALÓ CSATLAKOZÁS ELLENŐRZÉSE

Megosztott hálózatoknál, különösen azoknál, amelyek a szervezet határain túlra nyúlnak, a „Jogosultságkezelési szabályzat”-tal és a működési alkalmazások követelményeivel összhangban korlátozni kell a felhasználók hálózati csatlakozási képességeit.

A korlátozásokat a rendszergazda feladata menedzselni, továbbá az IBF ellenőrzi a tevékenység jelen szabályoknak való megfelelőségét.

A hálózati forgalom analizálása, ellenőrzése érdekében a következők megtétele szükséges:

- A rendelkezésre álló eszközök segítségével a WebDream hálózatának a vizsgálat ideje alatt történő hálózati forgalmának figyelése, és az abban felbukkanó hibák, anomáliák, vagy illegális tevékenységre utaló jelek keresése, valamint ezen túlmenően a hasonló jellegű anomáliák elhárítására tett intézkedések vizsgálata.
- Inaktív hálózati felhasználók szűrése, ellenőrzése.
- A hálózatban nem használt, lejárt felhasználói nevek (accountok) és a felhasználói adminisztráció folyamatának vizsgálata.
- Jogosulatlan hálózati bejelentkezések szűrése, ellenőrzése.
- A jogosulatlan hálózati bejelentkezések, valamint jogosulatlan erőforrás-használati kísérletek feltárása és az elhárításukra tett intézkedések vizsgálata.

- Hálózati megosztások ellenőrzése.
- A számítógépes hálózatban üzemelő munkaállomásokon észlelt, adatállományok tárolására alkalmas megosztások (ún. share-ek) összevetése az engedélyezett megosztások listájával.
- Nyitott portok szűrése, ellenőrzése.
- A WebDream szervereken, munkaállomásokon található nyitott portok ellenőrzése és összevetése az engedélyezett portok listájával. A felesleges, nem használt vagy informatikai- és adatbiztonsági veszélyeket jelentő nyitott portok megszüntetésének kezdeményezése az IBF felé.

10.4 INFORMÁCIÓ HOZZÁFÉRÉS KORLÁTOZÁSA

A hozzáférések korlátozására vonatkozó előírások a „Jogosultságkezelési szabályzat”-ban kerültek kialakításra. A jogosultsági csoportokhoz hozzárendelhető szerepkörök kialakítását a szakterületi vezetőknek a felelőssége elvégezni. A tevékenységet az IBF feladata ellenőrizni.

10.5 MOBIL SZÁMÍTÓGÉP HASZNÁLATA ÉS TÁVMUNKA

10.5.1 MOBIL SZÁMÍTÓGÉP HASZNÁLATA

A hordozható számítógépekkel (laptop, notebook, táblagép stb.) kapcsolatban további intézkedéseket kell betartani.

Az eszközökbe épített mikrohullámú hálózati kapcsolatot a WebDream belső hálózatára történő kapcsolódáskor kikapcsolt állapotban, vagy az operációs rendszer számára nem használható állapotban kell tartani. Lehetőség szerint ezt különböző védelmi eszközökkel ki kell kényszeríteni. Amennyiben a vezeték nélküli csatlakoztatás nem kerülhető el, a kapcsolatot titkosított módon kell létrehozni. A szükséges beállításokat csak a Rendszergazda végezheti el. A hordozható munkaállomások adattárolásra használt partícióit fájlrendszer szinten titkosítani szükséges. Az előírásoknak való megfelelőséget a Rendszergazdának kell biztosítania és az IBF-nek ellenőriznie.

10.5.2 TÁVMUNKA

A WebDream rendszeresen végeztet távmunkát. Az általános jogosultsági irányelveken túl minden esetben titkosított csatornán keresztül kell történnie a munkavégzésnek. Az Ügyvezető Igazgató felelőssége a távmunkával szemben támasztott követelmények megkövetelése, az IBF-é ennek ellenőrzése.

11 SZOFTVERHASZNÁLAT

A szerzői jog által védett számítógépes szoftverek illegális használata és másolása törvénybe ütköző cselekedet, amely egyben ellentétes a WebDream belső irányelveivel, szabályozásaival, adatvédelmi és információbiztonsági előírásaival. Minden indokolt szoftverigény kielégítésére a WebDream jogtiszta szoftvert biztosít az összes használatban lévő informatikai eszközre, a megfelelő időben és a szükséges mennyiségben. Minden szoftvervásárlásnál, telepítésnél és változásnál biztosítani kell a szoftverek jogtisztaságára vonatkozó elvek betartását.

A WebDream által vásárolt és a munkatársak által letöltött, használt szoftverek vonatkozásában az alábbi elvárások kerültek meghatározásra:

- Kizárólag a WebDream által beszerzett, ingyenesen letöltött vagy vásárolt és jogtiszta, legális szoftverek használhatók.
- A WebDream minden munkatársa számára biztosítani kell a hatékony és eredményes munkavégzéshez szükséges szoftver/alkalmazás környezetet.
- Szoftverek kiválasztásakor, illetve fejlesztésük során a funkcionális, biztonsági és gazdaságossági követelmények mellett alapvető elvárás a megbízható működés és a karbantarthatóság.
- A szoftverek minőségbiztosítását, biztonságának vizsgálatát szabályozott keretek között kell biztosítani.
- A fenti elvárások alapján a WebDreamnél két kategória kerül meghatározásra: az engedélyezett illetve a nem engedélyezett szoftverek. Az engedélyezett szoftverek azok, amelyek a WebDream működéséhez szükséges és az engedélyezett szoftverek nyilvántartásában (iTop) felvett rendszerek. Minden egyéb szoftver, amely az engedélyezett szoftverek listáján nem szerepel, az nem engedélyezett és használata tiltott.

Abban az esetben, ha egy vagy több szoftver belső hálózaton történő használata biztonsági kockázatot jelent, és/vagy a licenc költsége nincs arányban annak üzleti hasznával, és/vagy sem üzleti, sem IT vagy biztonsági szakmai szempontból nem támogatott, akkor NEM használható a WebDream által biztosított informatikai eszközein.

Ezek alatt az alábbi típusú szoftverek értendők:

- Szabad szoftver
  A nyílt forrású szoftver egy speciális fajtája, amely a program forráskódjához történő hozzáférés mellett, annak szabad módosítását, terjesztését, valamint ugyanezen jogok továbbadását is biztosítja és megköveteli a jogos felhasználók számára és azokkal szemben.
- Ingyenes szoftver, Szabadon terjeszthető és felhasználható szoftverek
  A freeware licencek lényege, hogy azokban a tulajdonos korlátozás és díjfizetési kötelezettség nélküli terjesztési és felhasználási jogot biztosít mindenki számára, bizonyos értelemben „közkinccsé" téve azt. Ugyanakkor a freeware szoftverek legtöbbjéhez alkotója nem mellékeli a program forráskódját, illetve nem engedélyezi módosított, derivált változatok létrehozatalát és terjesztését sem.
- Korlátozott használatú szoftver
  Csak korlátozott mértékben és/vagy ideig terjeszthető, birtokolható és felhasználható szoftver.

A kiválasztott szoftvert a bevezetés/letöltés előtt, de legkésőbb vásárlást követően a végfelhasználó állomásra történő telepítés megkezdése előtt minden esetben elővizsgálat alá kell vetni. Az elővizsgálat során

- ellenőrizni kell a szoftver(verzió) sérülékenységét;
- el kell végezni a kompatibilitás vizsgálatot;
- meg kell győződni arról, hogy az igényelt funkciók teljes körűen elérhetők vagy sem;
- a zavartalan jövőbeli működés biztosítás érdekében fel kell ismertetni *(false positive)* a WebDream által üzemeltett vírusvédelmi / IPS rendszerekkel.

A(z) (elő)vizsgálat kimenetelétől függően kell a beszerzési, telepítési folyamatot folytatni vagy megállítani.

WebDream által a belső hálózaton elérhető szerverek/munkaállomások, notebookra vonatkozó TILTOTT szoftver típusok / kategóriák / funkciók felsorolása:

- Torrent,
- Webcast,
- Game,
- P2P,
- Gambling,
- File/Network sharing,
- Cracking / Hacking (kivéve külön engedéllyel ethical hacking, terheléses tesztek elvégzésére),
- Daemon.

Programot a WebDream kezelésében lévő számítógépre csak a Rendszergazda telepíthet, függetlenül attól, hogy adott esetben technikailag erre más is képes-e!

12 INFORMÁCIÓS RENDSZEREK BESZERZÉSE, FEJLESZTÉSE ÉS FENNTARTÁSA

Az üzleti folyamatokat támogató alkalmazások fejlesztését alapvetően külső fejlesztések útján valósítja meg. A WebDream működéséhez fejlesztett alkalmazások üzemeltetésére a következő pontok vonatkoznak:

- A fejlesztési, a teszt és az éles környezetnek élesen el kell különülnie.
- A három környezetnek egymástól független gépeken/partíciókon (virtuális gépeken) kell futnia.
- Minden alkalmazásnak kell, hogy legyen egy üzemeltetésért felelős alkalmazásgazdája (a Rendszergazda is elláthatja ezt a feladatot), továbbá az üzleti területről delegált adatgazdája.
- A fejlesztőknek nem lehet jogosultsága az éles alkalmazásokra.
- Ha egy rendszert futtató szerver alap szoftvereiben, hardver-komponenseiben speciális javításokat, módosításokat kell végrehajtani, ezt csak az Ügyvezető engedélyével, írásbeli dokumentáltság mellett végezgeti el a Rendszergazda.
- Amikor a javítások, módosítások, változások végrehajtásra kerülnek, akkor azokat dokumentálni kell, amelynek felelőse a Rendszergazda. A verzióváltások rendjét a „Fejlesztési és változáskezelési szabályzat” tartalmazza.
- Amennyiben szükséges, a változásokról az érintett felhasználókat tájékoztatni kell, továbbá meg kell velük ismertetni a fejlesztés gyakorlati alkalmazásainak használatát és új lehetőségeit. A további, részletes útmutatásokat és irányvonalakat a „Fejlesztési és változáskezelési szabályzat” tartalmazza.

12.1 BIZTONSÁGI KÖVETELMÉNYEK ELEMZÉSE ÉS MEGHATÁROZÁSA

Alapvető biztonsági követelmény, hogy a WebDream informatikai rendszereiben minden változtatás esetben készüljön visszaállítási pont, mely által visszaállíthatóvá kell tenni a legutolsó helyes állapotot. Az információs rendszerekben történő bármilyen változás esetén az üzleti terüle-

tek munkavégzését minden esetben biztosítani szükséges. Amennyiben szükséges, úgy az üzleti területek bevonásával kell történnie a rendszerekben történő változások bevezetésének. A követelmények betartásáért azt IBF felel.

12.2 HELYES INFORMÁCIÓ FELDOLGOZÁS AZ ALKALMAZÁSOKBAN

Az információ feldolgozási folyamat ellenőrzését a folyamatba épített kontrollok és a több szem elvén alapuló kontrollok megvalósításával kell biztosítani. A kontrollok megvalósítását a folyamat ügyrendekbe dokumentálni szükséges. Fontos, hogy a tranzakciót indító és engedélyező személye minden esetben elkülönítésre kerüljön. A tevékenység ellenőrzése a WebDream Belső Ellenőrének a feladata.

12.3 RENDSZERFÁJLOK BIZTONSÁGA

12.3.1 ÜZEMELŐ SZOFTVEREK ELLENŐRZÉSE

Az engedélyezett szoftverek nyilvántartását a szoftver leltárban (iTop rendszerben) naprakészen kell vezetni. Az eljárásban meg kell fogalmazni a feladat- és felelősségi köröket, továbbá az ellenőrzési jogkört. Az ellenőrzések előírás szerinti végrehajtásáért az Ügyvezető Igazgató felel.

12.3.2 RENDSZERVIZSGÁLAT ADATAINAK VÉDELME

A vizsgálat reprodukálhatóságának érdekében a bázis adatokat minden esetben biztos helyen szükséges elérhetővé tenni. A vizsgálati adatokat gondosan kell kiválasztani, valamint azokat védeni és ellenőrizni kell. A tevékenység végrehajtásáért az Ügyvezető felel.

12.3.3 PROGRAMOK FORRÁSKÓDJÁHOZ VALÓ HOZZÁFÉRÉS ELLENŐRZÉSE

A programok forráskódjához a fejlesztőkön kívüli hozzáférést dokumentálni szükséges, továbbá az azokhoz való hozzáférés csak az Ügyvezető Igazgató engedélyével lehetséges. Az adathordozókat biztos helyen kell tárolni. Az IBF feladata ellenőrizni az előírások betartását.

12.4 BIZTONSÁG A FEJLESZTÉSI ÉS TÁMOGATÓ FOLYAMATOKBAN

12.4.1 VÁLTOZÁS-SZABÁLYOZÁSI ELJÁRÁSOK

A fejlesztés során felmerülő változási igényeket és az adott megoldásokat minden esetben kötelező írott formában dokumentálni. A változáskezelés hiteles dokumentumait csatolni kell a fejlesztés teljes dokumentációjához. A fejlesztésekkel kapcsolatos adminisztrációs feladatok a következők:

- tárolni kell a rendszer specifikációt,
- tárolni kell a tesztelési dokumentációkat,
- tárolni kell a szükséges engedélyeket, követelményeket.

A fejlesztésekkel kapcsolatos előírások betartását az IBF feladata ellenőrizni.

12.4.2 ALKALMAZÁSOK MŰSZAKI ÁTVIZSGÁLÁSA A RENDSZEREK MEGVÁLTOZTATÁSÁT KÖVETŐEN

Amikor üzemelő rendszerekben történik változtatás, a működés szempontjából kritikus alkalmazásokat át kell vizsgálni annak biztosítása érdekében, hogy a változtatás ne legyen hátrányos hatással a szervezet működésére, illetve a biztonságra.

Azokon a rendszereken, ahol már történtek korábban tesztelések, a hatálybaléptetést követően érvényesíteni szükséges a fenti intézkedéseket. Azokon a rendszereken, ahol még nem történtek tesztelések, meg kell teremteni annak a lehetőségét, hogy a fenti követelményeknek képes legyen helytállni a folyamat.

12.5 MŰSZAKI SEBEZHETŐSÉG KEZELÉSE

Az alkalmazásban lévő információs rendszerek műszaki sebezhetőségeiről aktuális információkat kell beszerezni, elemezni kell a szervezetnek az ilyen sebezhetőségekkel szembeni kiszolgáltatottságát, és megfelelő intézkedéseket kell hozni az ezzel járó kockázatok kezelésére.

13 INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE

13.1 INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK ÉS GYENGESÉGEK JELENTÉSE

A WebDream minden alkalmazottjának és partnerének kötelessége az általa tapasztalt biztonsági eseményt vagy általa feltárt biztonsági sebezhetőséget haladéktalanul jelenteni az IBF-nek és a Rendszergazdának. A Rendszergazdának külön kötelessége a számára bejelentett incidenst jelenteni az IBF-nek attól függetlenül, hogy a bejelentő esetleg az IBF-et is értesítette már. A bejelentés formai követelményeit, kezelésének módját az Ügyvezető Igazgató határozza meg.

13.2 ESEMÉNYEK, GYENGESÉGEK KIÉRTÉKELÉSE, INCIDENSEK KEZELÉSE

A biztonsági események kiértékelése, incidensek kezelése elsődlegesen az IBF feladata, mely tevékenységbe a rendszergazdát is be kell vonnia. Sürgős intézkedést igénylő esetben, az IBF akadályoztatása, elérhetetlensége esetén a rendszergazdának önállóan is meg kell kezdenie az incidensek kezelését. A biztonsági események kezelésekor az IBF-nek, mint szakértőnek be kell tartatni a jelen IBSZ-ben rögzítetteket. Ugyancsak ezen szabályzat előírásai szerint kötelessége a bejelentés dokumentálása, valamint a kiértékelés elvégzése és átadása az Ügyvezető Igazgatónak.

Az ismertté vált gyengeség, sebezhetőség kezelését a lehető legrövidebb időn belül, de legkésőbb az ismertté válást követő 2 munkanapon belül meg kell kezdeni. Az incidensek kezelését a bejelentést, ismertté válást követően haladéktalanul meg kell kezdeni.

A biztonsági esemény kiértékelése az IBF feladata, melyet az alábbi szabályok szerint kell elvégeznie:

- meg kell határoznia, hogy a biztonsági esemény
  - az informatikai rendszer kiesésével, vagy meghibásodásával,
  - a szolgáltatás megtagadásával,
  - az adatok megsérülésével, pontatlanságával,
  - vagy biztonságsértéssel kapcsolatos;
- meg kell határoznia a biztonsági esemény okát;
- meg kell határoznia a javító intézkedést az előzetesen gyűjtött adatok felhasználásával;
- értesítenie kell az Ügyvezető Igazgatót a foganatosított intézkedésekről;
- ha az intézkedés csak a hasonló biztonsági esemény kizárását célozza, akkor jeleznie kell az Ügyvezető Igazgató felé a hiányosságot, akinek kötelessége munkacsoport összehívása a megfelelő védelmi intézkedés kidolgozására;
- meg kell határoznia a biztonsági esemény elhárításának végső határidejét.

Az IBF köteles negyedévente

- a beérkező biztonsági eseményekről statisztikát készíteni;
- a biztonsági eseményekből közvetlenül származtatott kárt megbecsülni;
- a jellemző információbiztonsági sérüléseket azonosítani, dokumentálni;
- a felülvizsgálatokkal összhangban, a védelmi intézkedésekkel együtt előterjesztést készíteni a vezetői értekezlet elé.

14 MŰKÖDÉS FOLYTONOSSÁGÁNAK IRÁNYÍTÁSA

A működés folytonosság menedzselésére vonatkozó előírásokat az „Üzletmenet folytonossági- és katasztrófa elhárítás menedzselése szabályzat” dokumentumban kell szabályozni.

15 KÖVETELMÉNYEKNEK VALÓ MEGFELELÉS

15.1 JOGI KÖVETELMÉNYEKNEK VALÓ MEGFELELÉS

15.1.1 AZ ALKALMAZANDÓ JOGSZABÁLYOK MEGÁLLAPÍTÁSA

A WebDream informatikai tevékenységére az alábbi főbb jogszabályok vonatkoznak:

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Avtv)
- az elektronikus közbeszerzés részletes szabályairól szóló a 424/2017. (XII. 19.) Korm. rendelet.
- az Általános Adatvédelmi Rendelet (Az Európai Parlament és az Európai Tanács (EU) 2016/679 Rendelete).

A WebDreamre vonatkozó jogszabályi követelmények folyamatos figyelemmel kíséréséről és az annak megfelelő tevékenység végzésről a megfelelőségi felelősnek kell gondoskodni.

15.1.2 SZELLEMI TULAJDONJOGOK (ANGOL RÖVIDÍTÉSSEL: IPR)

A WebDream által létrehozott, vagy részére külső szerződéses partner által leszállított dokumentációk tulajdonjogának a WebDream birtokába vagy ügyvédi letétbe kell kerülnie. Amennyiben ez nem lehetséges, azt a szerződésben szerepeltetni kell.

15.1.3 SZERVEZETI FELJEGYZÉSEK VÉDELME

A WebDream információs vagyonát, üzleti titkokat, egyéb feljegyzéseket az adatvagyon leltárban megfogalmazott irányelvek szerint kell besorolni, kezelni.

15.1.4 ADATVÉDELEM ÉS A SZEMÉLYES ADATOK TITKOSSÁGA

A WebDream „Adatvédelmi szabályzat” megtételével érvényesíti a vonatkozó előírások alapján rá vonatkozó kötelezettségeket.

15.1.5 INFORMÁCIÓ-FELDOLGOZÓ BERENDEZÉSEKKEL VALÓ VISSZAÉLÉSEK MEGELŐZÉSE

A felhasználók csak a munkakörükhöz szükséges rendszerekhez kaphatnak hozzáférési jogokat előzetes igényjogosultság megítélése alapján. Az igényjogosultság megítélésének első szintje a közvetlen vezető felelőssége. Az IBF feladata ellenőrizni a hozzáférési folyamat előírásainak betartását.

15.1.6 TITKOSÍTÁSI ELJÁRÁSOK SZABÁLYOZÁSA

Titkosítási eljárás bevezetésére a WebDream nem kötelezett.

15.2 BIZTONSÁGI SZABÁLYOKNAK VALÓ MEGFELELÉS ÉS MŰSZAKI MEGFELELŐSÉG

A WebDream informatikai rendszerei fejlesztéséhez és működtetéséhez a COBIT nyílt szabvány útmutatásait veszi figyelembe.

15.3 INFORMÁCIÓS RENDSZEREK AUDITÁLÁSÁNAK SZEMPONTJAI

15.3.1 INFORMÁCIÓS RENDSZEREK AUDITJÁVAL KAPCSOLATOS INTÉZKEDÉSEK

Azokat az eszközöket, amelyekben támogatott az audit szolgáltatás beállításának lehetősége, alkalmazni kell a jelen szabályzatban megfogalmazott irányelvek alapján.

15.3.2 INFORMÁCIÓS RENDSZEREK AUDITESZKÖZEINEK VÉDELME

Az információs rendszerek auditálására szolgáló eszközök a Kiemelt biztonsági szint szerinti besorolásba tartoznak és így ennek megfelelő védelemmel kell ellátni. A védelmi intézkedések ellenőrzése az IBF feladata.