energy
business
motion
h u p x
HUNGARIAN POWER EXCHANGE
1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

A HUPX Zrt.
Információbiztonsági szabályzata

Iktatószám:	HUPX-SZB-2019-0021
Adatbiztonsági besorolás:	Korlátozott hozzáférésű
Verzió:	1.1
Kiadás dátuma:	2019.05.27
Készítette:	Pépei László informatikai infrastruktúra szolgáltató információbiztonsági felelőse HUDEX Energiatőzsde Zrt.
Jóváhagyta:	Tóth Péter vezérigazgató

energy business motion
hupx HUNGARIAN POWER EXCHANGE
1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

Tartalom

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

1. Általános rendelkezések

1.1 A Szabályzat célja

Ezen Információbiztonsági Szabályzat (továbbiakban: IBSZ) célja a HUPX Zrt. számítógépes és vagyonvédelmi rendszerek biztonsági előírásainak részletes meghatározása, amely előírások lehetővé teszik az informatikai és vagyonvédelmi rendszerekre irányuló veszélyek, veszélyforrások, valamint az előre becsülhető problémák fellépésének megelőzését, illetve a zavartalan munkavégzés feltételeinek biztosítását. A Szabályzat az információbiztonság két alapterületével, az információvédelemmel és a megbízható működéssel kapcsolatos intézkedési rendszert hivatott rögzíteni.

1.2 A Szabályzat hatálya

Az IBSZ hatálya kiterjed a HUPX Zrt. érdekében működő valamennyi informatikai rendszerre.

Az IBSZ személyi hatálya alá tartozik a HUPX Zrt-vel munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban álló valamennyi munkavállaló, illetve a HUPX Zrt. bármely számítógépes rendszeréhez hozzáférési jogosultsággal rendelkező természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező egyéb társaság.

1.3 A Szabályzat elkészítéséért és karbantartásáért viselt felelősség

Jelen szabályzat kiadásáért a vezérigazgató viseli a felelősséget. A szabályzat kidolgozásával kapcsolatos operatív feladatokat, illetve annak karbantartását a vezérigazgató megbízásából az információbiztonsági felelős végzi, illetve koordinálja.

Az IBSZ-t legalább évente, illetve jelentős szervezeti, technológiai vagy üzleti változások, biztonsági incidensek bekövetkezése és új veszélyek megjelenése esetén felül kell vizsgálni.

1.4 Titoktartási kötelezettség és a felelősségi rendszer szempontjai

Titoktartási kötelezettség terhel minden, a HUPX Zrt. informatikai rendszereivel, illetve papír alapú dokumentumaival kapcsolatba kerülő személyt, tekintet nélkül arra, hogy a kapcsolat milyen jogviszonyból ered (pl. munkajogviszony, megbízási jogviszony stb.). A titoktartási kötelezettség kiterjed a HUPX Zrt. által üzemeltetett, illetve HUPX Zrt. által szolgáltatásként bérelt rendszereiben (továbbiakban: Rendszerek) kezelt „nyilvános” minősítésű adatok kivételével minden adatra, a Rendszerek felépítésére, működési rendjére vonatkozó adatokra, valamint a biztonsági rendszabályokra egyaránt. A titoktartási kötelezettség a minősítés hatályáig, egyéb esetben időkorlátra tekintet nélkül áll fenn és az érintett személy a mindenkor érvényes jogszabályok alapján tartozik ezen kötelezettségéért felelősséggel.

A külsős kivitelező, fejlesztő, illetve üzemeltető cégek képviselőivel a HUPX Zrt.-nek az IBSZ-t a feladat szempontjából adódó mértékben ismertetnie kell. A kivitelező, fejlesztő cég köteles az általa telepített, fejlesztett informatikai rendszert úgy konfigurálni, hogy annak minden eleme eleget tegyen a HUPX Zrt.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

IBSZ-ében előírtaknak.

1.5 A rendszerekért és adatokért viselt felelősség

A HUPX Zrt. informatikai rendszerei és az azokban tárolt és feldolgozott adatok tekintetében az egyes munkatársak által viselt felelősség az érintett rendszerhez/adathoz való viszonyától, jogosultságától függően kerül meghatározásra.

Ezek alapján meg kell különböztetni a rendszer/adat:

- Objektumfelelősét
- Megbízottját
- Informatikai felelősét
- Felhasználóját

a) A rendszer/adat Objektumfelelőse: az a munkatárs, aki felelős a felhasználás és a szükséges védelem körében meghozott döntésekért. Minden rendszernek, adatnak rendelkeznie kell objektumfelelőssel. Az objektumok és felelősök listáját a Jogosultság nyilvántartó rendszerben (Rights Management System, továbbiakban: RMS) kell nyilvántartani.

Az Objektumfelelős felelősséget visel:

- A rendszer/adat értékének meghatározásáért, a biztonsági koncepciók kidolgozása során a szakmai szempontok képviseletéért.
- A személyes adatokra vonatkozó követelmények érvényre juttatásáért.
- A rendszer-/adatbiztonsági követelményszintjének fenntartásáért, felhasználói gyakorlat felügyeletéért.
- Az adatok hitelességének, pontosságának, rendelkezésre állásának fenntartásáért.
- A rendszerre/adatra vonatkozó katasztrófaterv kidolgozásáért és karbantartásáért.
- A felhasználó, illetve a vezérigazgató kérése alapján a rendszer/adat hozzáférési jogosultságok kiadásának jóváhagyásáért és nyilvántartásáért.
- A rendelkezésre állási és katasztrófakezelési célokra készült adatmásolások biztosításáért.

b) Megbízott: Objektumfelelős távollétében objektumfelelősi szerepkörrel rendelkezik.

c) A rendszer/adat Informatikai felelőse: az a személy, aki a szakmai tevékenység támogatását szolgáló informatikai szolgáltatás nyújtásáért felelős, általában az alkalmazás rendszerfelelőse. Az informatikai felelősök listáját az RMS-ben kell nyilvántartani.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

Az informatikai felelős felelősséget visel:

- A biztonsági adminisztrációért az Objektumfelelős által meghatározottak szerint és a vonatkozó szabályozással összhangban,
- A hozzáférések és egyéb események felügyeletéért annak érdekében, hogy az adatok bizalmassága és sértetlensége kielégítse a támasztott követelményeket (a hozzáférések utólagos, naplók alapján történő ellenőrzése az Rendszerüzemeltető feladata),
- A rendelkezésre állási és katasztrófakezelési célokra készült adatmásolatok biztosításáért.

d) Felhasználó: aki a rendszerhez/adathoz hozzáférési jogosultsággal rendelkezik. A felhasználó lehet külső vagy belső.

A Felhasználó felelősséget visel:

- Az Objektumfelelős által meghatározott hozzáférési és egyéb biztonsági követelmények betartásáért.
- A jelszókezelési és egyéb biztonsági követelmények meghatározása szempontjából jelentőséggel bíró észrevételek, tapasztalatok továbbításáért az Objektumfelelős felé.

1.6 Meghatározások

Tűzfal (Firewall): Két hálózat (pl. Internet és egy LAN) közötti számítógépes alkalmazás, amely előre definiált feltételek szerint szabályozza a külső és a belső hálózatok közötti kommunikációt, hozzáféréseket.

LAN (Local Area Network): helyi hálózat, egy épületben vagy telephelyen, speciális, nagy sebességű csatlakozással hálózatba kötött személyi számítógépek együttese.

Internet: Különböző intézmények, vállalatok és egyedi felhasználók nyilvános számítógépes hálózata szolgáltatások, információk megosztása céljából.

Intranet: A vállalaton belüli számítógépes hálózaton szoftveresen kialakított információs felület adatok, előírások, közlemények megjelenítésére.

Számítógépes vírus: Számítógépes vírusnak tekinthető minden olyan, végrehajtható számítógépes kód (program, makró), amely azzal a szándékkal készült, hogy bekerülve egy informatikai rendszerbe ott kárt vagy zavart okozzon - megsemmisítve vagy használhatatlanná téve állományokat, terhelve vagy lassítva a rendszer működését, zavarva annak vagy a felhasználóinak a tevékenységét. Futásakor hozzákapcsolódik újabb és újabb programokhoz és ezáltal tovaterjed.

Rendszerüzemeltető: Egy informatikai rendszer szakmai üzemeltetéséért felelős személy, szervezet, szolgáltató, stb., aki figyelemmel kíséri a rendszer állapotát, technikailag kezeli a jogosultsági rendszert, elvégzi az üzemeltetési feladatokat, és a hibaelhárítást. A rendszerüzemeltetőket a vezérigazgató jelöli ki, külső

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

szolgáltató esetén a vezérigazgató felel a szolgáltatási szerződések meglétéért és az abban szereplő SLA-k betartatásáért.

Rendszerfelelős: Egy informatikai rendszer üzemeltetéséért felelős – többnyire belsős – személy, aki koordinálja a rendszerrel kapcsolatos üzemeltetési és fejlesztési feladatokat, a hibaelhárítást és a felhasználói igények kezelését. A Rendszerfelelősöket a vezérigazgató jelöli ki.

Helpdesk: Távoli informatikai támogatást végző, illetve incidensek és igények kezelését koordináló külső szolgáltató.

Servicedesk: a HUPX telephelyén informatikai támogatást nyújtó külsős kollégák.

1.7 Hatálybalépés

Jelen utasítás a kiadása napján lép hatályba.

2. Az információbiztonság személyi – szervezeti feltételei

2.1 Az információbiztonsági rendszer személyi feltételrendszere

2.1.1 Biztonsági Bizottság

A Biztonsági Bizottság (továbbiakban: „BB”) szerepe és felelősségi köre a HUPX Zrt. Biztonságpolitikájában, illetve a Biztonsági Bizottság ügyrendjében került meghatározásra.

2.1.2 Információbiztonsági felelős

Feladata a biztonsági követelmények érvényre juttatásának biztosítása, az alábbiak szerint:

1. Szakmai támogatással, közreműködéssel segíti a BB tevékenységét.
2. A BB által definiált biztonsági irányelveknek megfelelően irányítja a biztonsági rendszerrel kapcsolatos kiépítési és működtetési feladatokat. Feladata továbbá az informatikai biztonsági feladatok operatív irányítása és koordinálása, a HUPX Zrt. saját tulajdonú, illetve bérelt (a HUPX Zrt.-nek szolgáltatott) informatikai rendszerek biztonsági menedzselése.
3. Hozzájárul a biztonságot érintő események, tapasztalatok összegyűjtéséhez, részt vesz azok kiértékelésében.
4. Meghatározza és felügyeli a biztonsági követelmények betartását, a követendő biztonsági gyakorlatra, az alkalmazható speciális eljárásokra, eszközökre vonatkozó előírásokat.
5. Véleményezési joggal rendelkezik a felmerülő biztonsági koncepciók kialakítása

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

területén, valamint a használatbavétel jóváhagyásának kiadásával kapcsolatban.

6. Véleményezi az adatkapcsolat, hálózati csatlakozás kialakítása esetén a biztonsági intézkedések megfelelőségét.
7. Beszámolási kötelezettség terheli a BB felé biztonsági incidens esetén.
8. Az Információbiztonsági felelős felett a vezérigazgató rendelkezik utasítási jogkörrel.

2.2 Az információbiztonságért felelős személyek tevékenységi körének meghatározása

- A **Rendszerfelelős** feladata az adott rendszerrel kapcsolatos összes informatikai egység működésének, folyamatos monitorozásának biztosítása, az adott rendszerrel kapcsolatos fejlesztések támogatása, illetve a rendszerüzemeltetők koordinálása.

  Feladata továbbá az adott rendszerrel kapcsolatos mentési és jelszókezelési folyamatok kidolgozása és végrehajtásának folyamatos kontrollja, és a vírusvédelem biztosítása.

  Az Információbiztonsági felelős irányába általános együttműködési és tájékoztatási kötelezettség terheli minden biztonsággal kapcsolatos változást illetően.

- A **Rendszerüzemeltető** feladata az adott informatikai rendszer üzemeltetési, mentési és jelszókezelési feladatainak végrehajtása, illetve a vírusvédelmi eszközök telepítése, ellenőrzése.

- A **Helpdesk és Servicedesk** munkatársak feladata az ügyeletesi eljárásrendben meghatározott, szolgáltatás esetén a szerződésben vállalt feladatok elvégzése. Az ügyeletesi tevékenység ügymenetét az érvényben lévő ügyeletesi utasítások határozzák meg. Külső szolgáltató esetén ennek megfelelő kidolgozása és végrehajtása a szolgáltató feladata és felelőssége.

  Bármilyen meghibásodás esetén az ügyeletes köteles megtenni a szükséges intézkedéseket a hiba elhárítása érdekében. Amennyiben a meghibásodás olyan mértékű, hogy azt az ügyeletes nem tudja elhárítani, azonnal köteles értesíteni az illetékes rendszerfelelőst és a rendszerüzemeltetőt.

2.3 Az információbiztonság menedzseléséhez szükséges minimális személyi feltételrendszer meghatározása

A HUPX Zrt. informatikai alrendszerek működtetéséért felelős személyeket ki kell nevezni. Egy személy több informatikai alrendszerért is felelős lehet. A felelős személyek kinevezése az informatikai rendszerek üzemeltetésének biztosításáért felelős vezető jogkörébe tartozik.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

3. A jogosultsági rendszer adminisztrációja kialakításának folyamata, elvi szempontjai

Valamennyi információs vagyonelemhez való hozzáférési jogosultságot nyilván kell tartani. A nyilvántartás vezetése az informatikai terület felelőssége.

A jogosultságok felülvizsgálatát adott időközönként, de legalább évente egyszer, illetve nagyobb változás esetén el kell végezni. A felülvizsgálat az adott rendszerekben nyilvántartott ténylegesen kiosztott jogosultságok és az RMS alapján nyilvántartott hozzáférési jogosultságok összevetésével történik. Az eltérések kezelése az adott objektumfelelős felelőssége.

Minden munkavállaló és a külső felek összes felhasználója esetében a hozzáférési jogosultságokat vissza kell vonni a munkaviszony, a szerződés vagy a megállapodás megszűnésekor, illetve módosítani kell változás esetén. A fenti esetekben a hozzáférési jogosultságok szabályozása (visszavonása / módosítása) az adott objektumfelelős felelőssége.

A visszavont, vagy módosult hozzáférési jogosultságokat az RMS-ben adminisztrálni kell.

3.1 Felhasználó specifikus informatikai elemek védelme

A HUPX Zrt. informatikai rendszere jelszóval védett objektumok integrációja, melyek hardverre valamint felhasználói szinten definiált funkciókra vonatkoznak. Jelszóval védett objektumoknak tekintendő:

- a különálló számítógépek melyek a hálózaton keresztül kommunikálnak egymással,
- az aktív hálózati eszközök
- az egyéni felhasználói fiókok,
- az egyes rendszerfunkciókhoz létrehozott csoportok.

Az objektumok védelmét szolgáló jelszavak és felhasználói nevek biztonságos tárolása és menedzselése alapvető követelmény az illetéktelen behatolások elkerülése érdekében.

A felhasználók kezdeti (első) jelszavát a HUPX Zrt. hálózatához és a különböző informatikai rendszerekhez a felhasználó azonosítása után biztonságos módon, személyesen kell átadni, amelyet a felhasználónak a lehető legrövidebb időn belül meg kell változtatnia. Amennyiben a személyes átadás nem lehetséges, további kontrollok alkalmazásával (pl. egy megbízható, harmadik személy igazolja az igénylő személyi azonosságát) telefonon keresztül is át lehet adni a jelszót.

Egy hiba okának későbbi felderítése céljából az adminisztrátori jelszavak esetében követelmény a jelszókezelés változásmenedzselése és archiválása.

3.2 A jelszókezelés általános követelményei

Egy rendszer jelszókezelésének kialakítása során meg kell határozni a kapcsolódó objektumjelszavak változtatásának gyakoriságát, a jelszó szükséges karakterhosszát, valamint a jelszó összetételére (betűk és számjegyek kombinációja) és a korábbi jelszavak újrafelhasználásának kizárására vonatkozó elvárásokat.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

A jelszókezelési rendszer követelményei:

a) Az egységes jelszókezelési eljárást minden független informatikai rendszer esetén alkalmazni kell.

b) Az egységes jelszókezelésre vonatkozó előírástól eltérni csak megfelelő szakmai indoklás mellett az információbiztonsági felelős engedélyével lehetséges. A problémát és szakmai indoklását, valamint az információbiztonsági felelős döntését minden esetben írásban kell rögzíteni és tárolni.

c) Lehetőség szerint minden objektumot jelszóval kell ellátni.

d) Az egyes rendszerekhez tartozó jogosultságokat elektronikus formában az RMS-ben kell nyilvántartani. Szerverek esetében a rendszergazdai (admin / root) jelszavakat lezárt borítékban kell tárolni, és jelszókezelési táblázatban dokumentálni.

e) Az RMS-ben valamennyi funkcióhoz kiadott jogosultságot nyilván kell tartani. Új jogosultságok felvételét és meglévők megszüntetését adminisztrálni kell az RMS-ben.

f) A saját maga által üzemeltetett és a szolgáltatásként bérelt rendszerek esetében a HUPX Zrt. specifikus jogosultság nyilvántartó rendszerének és jelszókezelési táblázatának kidolgoztatása a vezérigazgató felelőssége.

g) Az érintetteket az RMS és a jelszókezelési táblázat megváltoztatásáról adminisztrációs úton tájékoztatni kell.

h) Azon estekben, amikor az előírások betartása központilag nem ellenőrizhető, illetve nem szabályozható, véletlenszerű ellenőrzést kell végezni.

i) Az objektumok jelszavait tilos - a szerverek rendszergazdai jelszavainak borítékos elhelyezésen kívül - bármilyen más formában (papír alapú vagy számítógépes adathordozón) tárolni.

j) Az objektum bárminemű adatának megváltozásáról az objektumfelelős (távolléte esetén a Megbízott) az objektum felhasználóit, valamint a Rendszerfelelőst köteles tájékoztatni. (A jelszó megváltoztatására vonatkozó előírásokat a 3.3.4. pont tartalmazza.)

k) Amennyiben a felhasználó úgy gondolja, hogy titkos jelszava nyilvánossá vált, úgy köteles azt megváltoztatni és az eseményről a Rendszerfelelőst tájékoztatni. Amennyiben a rendszer a felhasználó általi jelszómódosítást nem teszi lehetővé, úgy a felhasználó köteles új jelszót kérni a Helpdesken keresztül.

l) Azon jelszavakat, amelyeket több munkavállaló ismer és használ, azonnal módosítani szükséges, amint bármelyikük munkaviszonya megszűnik.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

3.3 A HUPX Zrt. jelszókezelési és az objektumokra vonatkozó titkos információ tárolási adminisztrációs rendszere

3.3.1 A HUPX Zrt. RMS tartalmi felosztása

Az adatbázis szerkezetének olyannak kell lennie, mely egyértelműen és világosan tartalmazza az egyes objektumokhoz tartozó személyek körét, illetve a személyek jogosítványait és jogosítványaik terjedelmét.

3.3.2 Az objektumokra vonatkozó titkos információk és jelszókezelés tárolásának követelmény rendszere

a) A jelszóval védett szerverek rendszergazdai felhasználói neveit és jelszavait, illetve titkosító kulcsokat – lezárt borítékban – lemezszekrényben kell tárolni. A borítékon fel kell tüntetni a jelszókezelési táblázatban szereplő rendszer és felhasználói nevet és a módosítás időpontját. A felhasználói fiókok jelszavait nem kell tárolni, tekintettel arra, hogy ezen jelszavak megfelelő jogosultságú felhasználók (pl. rendszergazda) által módosíthatóak.

b) Az olyan munkaállomások esetében, melyek működtetéséhez a számítógépház kulcsa szükséges, a kulcs másolatából a borítékban kell tárolni egy példányt.

c) A kiszervezett keretek között üzemeltetett rendszerekkel kapcsolatos szakmai dokumentációkat és bizalmas adatokat (accountok, jelszavak) az üzemeltető cég köteles a HUPX Zrt-nek bemutatni.

d) A borítékokat, illetve az információbiztonsági felelős által hitelesített jelszókezelési táblázat egy példányát lemezszekrényben kell tárolni.

e) A jelszavakat - illetve CD-ket, kulcsokat - tartalmazó borítékok elhelyezésére tűzbiztos lemezszekrényt kell használni.

f) A rekesz/lemezszekrény kulcsának biztonságos tárolásáért a titkárságvezető tartozik felelősséggel.

g) A titkosító kulcsok élettartamát a kockázattal arányos védekezés elve alapján kell megállapítani.

3.3.3 Az objektumokra vonatkozó titkos információk kiszolgáltatásának feltételrendszere

a) Egy adott objektumhoz tartozó boríték tartalmát csak az objektumfelelős, a Rendszerfelelős, illetve az Információbiztonsági felelős jogosult megtekinteni.

b) A Rendszerfelelős jogosult az objektum borítékolt adatait megváltoztatni, de erről a változtatásról az objektumfelelősét tájékoztatni köteles.

c) A titkos információhoz való hozzáférés jogosultsághoz kötött, hozzáférés a HUPX Zrt. Üzleti titkok védelmére vonatkozó szabályzata szerint történik.

d) A lemezszekrényben tárolt borítékok felbontásáról (a jelszavak megtekintése, változtatása esetén) naplót kell vezetni, amely naplót szintén a lemezszekrényben szükséges tárolni. A napló vezetése minden a jelszavak megtekintésére, megváltoztatására jogosult személy feladata. A változásokat oly módon kell feltüntetni, hogy a változások láncolatának egyes elemeit utólag is hiánytalanul

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

meg lehessen állapítani.

e) Naplónak tartalmaznia kell az alábbiakat:

- hozzáférés esetén: időpont, személy, ok rövid leírása;
- változtatás esetén: időpont, személy, ok rövid leírása.

Változtatás után a már nem érvényes jelszót tartalmazó borítékot és a hozzá tarozó jelszót meg kell semmisíteni, a változtatás dátumát az új, érvényes jelszót tartalmazó borítékra fel kell vezetni.

A változtatásról az érintetteket e-mailben tájékoztatni kell az objektum nevének, jelszóváltoztatás dátumának és a jelszóváltoztatás okának megadásával.

3.3.4 Az objektum jelszavának módosítására vonatkozó előírások

A jelszavak módosításának gyakoriságát lehetőség szerint az informatikai rendszeren ki kell kényszeríteni. Amennyiben ezt a rendszer nem támogatja, úgy a jelszóváltoztatás a felhasználó, rendszergazda jelszavak esetében pedig az adott Rendszerfelelős felelőssége.

Felhasználói jelszavak esetében, beleértve a rendszergazdai jelszavakat is, amennyiben az adott rendszerrel kapcsolatban más megkötés nincs, a rendszerhez tartozó jelszavakat 2 havonta meg kell változtatni. Minden olyan esetben, amikor bebizonyosodik, vagy csak annak gyanúja merül fel, hogy a jelszó kitudódott, úgy az adott felhasználóhoz tartozó jelszót a lehető legrövidebb időn belül meg kell változtatni. Rendszergazdai jelszavak esetében a jelszóváltoztatásért és dokumentálásáért az adott Rendszerfelelős, egyéb felhasználói jelszavak jelszóváltoztatásáért az adott felhasználó felelős.

Amennyiben az adott rendszer lehetőséget biztosít rá, úgy kell beállítani, hogy a rendszerre vonatkozó gyakorisággal kikényszerítse a jelszómódosítást. Rendszer jelszavak esetében a jelszavak változtatása csak abban az esetben szükséges, ha azok egyéb módon, pl. tesztelés, fejlesztés, hibajavítás, stb. során manuálisan alkalmazva lettek, illetve minden olyan esetben, amikor bizonyosságot nyer, vagy csak annak gyanúja merül fel, hogy a jelszó kitudódott. A rendszer jelszavak változtatása és dokumentálása az adott Rendszerfelelős felelőssége.

Telefonos vagy külső hálózaton keresztül történő hibaelhárítás esetén, amennyiben a hibaelhárítás nem titkosított hálózati kapcsolaton keresztül történt, a felhasználásra került objektumok jelszavait a lehető legrövidebb időn belül meg kell változtatni.

Törekedni kell arra, hogy az információs vagyonelemekhez való hozzáférés dedikált felhasználói fiókok használatával valósuljon meg. Amennyiben ez nem lehetséges, pl. külső szolgáltatáshoz tartozó hozzáférési jogosultság, akkor azon hozzáférés jelszavát, melyet több munkavállaló, szerződéses partner, szolgáltató, stb. ismerhet, azonnal meg kell változtatni, ha ezen személyek közül bárkinek megszűnik a munkaviszonya, illetve szerződéses kapcsolata a HUPX Zrt-vel. A jelszóváltoztatás valamennyi munkavállaló felelőssége. Amennyiben ezen csoportnak nem tagja HUPX munkavállaló, akkor a szerződésgazda felelőssége, hogy ebben az esetben gondoskodjon az adott jelszó megváltoztatásáról.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

3.3.5 A jelszóval védett objektumok kezelésére kialakított nyilvántartás változásmenedzselése és frissítése

A Jogosultság nyilvántartó rendszer csak az Informatikai terület számára lehet hozzáférhető.

3.3.6 A jelszókezelés gyakorlatára vonatkozó és a jelszavak minőségével kapcsolatos megkötések

A jelszavak minőségi követelményei:

- a jelszavak legalább 8 jelsorozatból, a rendszergazdai jelszavak legalább 12 jelsorozatból álljanak
- a jelszó ne tartalmazza a felhasználó bejelentkezési azonosítóját,
- tartalmazzon vegyesen kis- és nagybetűket, valamint számokat,
- az interaktív bejelentkezési jelszavak lejárata legfeljebb 90 nap legyen
- a legutoljára használt 5 jelszó ne legyen beállítható,
- a kezdeti jelszót az első belépés alkalmával kötelezően meg kell változtatni,
- legfeljebb 5 egymást követő sikertelen belépési kísérlet esetén a fiók kerüljön zárolásra 30 percig
- az egymást követő sikertelen belépések közötti időtartamok (time-out period) exponenciálisan növekedjenek.

A külső üzemeltető cégek képviselőivel a HUPX Zrt. Információbiztonsági Szabályzatát annak 1.4. pontja szerint ismertetni kell. A kivitelező cég köteles az általa telepített informatikai rendszert úgy konfigurálni, hogy annak minden eleme eleget tegyen a HUPX Zrt. IBSZ-ban előírtaknak.

3.3.7. A HUPX tagokra alkalmazandó informatikai kódok és azonosítók rendszere

A HUPX minden tagnak minden HUPX rendszerhez különböző felhasználói azonosítót és jelszót ad meg. A felhasználók kezdeti (első) jelszavát a HUPX Zrt. hálózatához és a különböző informatikai rendszerekhez a felhasználó azonosítása után biztonságos, dokumentált módon, személyesen kell átadni. Amennyiben a személyes átadás nem lehetséges, további kontrollok alkalmazásával (pl. egy megbízható, harmadik személy igazolja az igénylő személyi azonosságát) telefonon keresztül is át lehet adni a jelszót. Amennyiben az adott rendszer lehetőséget biztosít rá, úgy kell beállítani, hogy a kezdeti jelszó megváltoztatását megkövetelje az adott felhasználó rendszerbe való első bejelentkezése után.

Amennyiben az adott rendszer nem teszi lehetővé a felhasználónak a jelszómódosítást, mint pl. SFTP rendszer, abban az esetben felhasználói kérésre, vagy amennyiben a HUPX úgy ítéli meg, pl. információbiztonsági incidens esetén, a HUPX gondoskodik az új jelszó generálásáról és eljuttatásáról az adott felhasználónak a fent említett biztonságos és dokumentált módon.

Nem szükséges elvégezni a rendszeres jelszómódosítást azon felhasználói azonosítók esetében, amelyek a HUPX rendszereihez kapcsolódó külső rendszerek

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

azonosítására szolgálnak és az azonosítási folyamatban nem történik emberi beavatkozás.

A felhasználói azonosítót és a jelszót minden esetben külön csatornán kell eljuttatni az adott HUPX tag részére. Az ebben a pontban nem szabályozott kérdésekben a jelen szabályzatban megfogalmazott jelszókezelés általános követelményei irányadóak a HUPX tagok részére létrehozott jelszavak esetében is.

4. Mentési és archiválási rend

Az adatvédelem az egyik legérzékenyebb pontja a jól megtervezett számítógépes rendszereknek. Az adatvédelem kiterjed az adathozzáférés jogosultsági rendszerének kialakítására, illetve az adatok rövid és hosszú távú tárolására (archiválására).

A mentési rendszerrel szemben támasztott általános elvárások:

a) A rendszerszolgáltatással kapcsolatos eseményeket rögzítő naplóállományok mentéseivel, illetve a kritikus archivált állományokkal kapcsolatban is követelmény a hozzáférési jogosultságrendszer kidolgozása, valamint a hozzáférések regisztrálása.

b) Szolgáltatásként igénybe vett rendszerek esetében az üzemeltető feladata a hozzáférési jogosultságrendszer kidolgozása.

c) A mentéssel és archiválással kapcsolatos részletes szabályokat az egyes rendszerek üzemeltetési leírása tartalmazza.

Rögzített hang- és kamerafelvételek megőrzése

A 2005.évi CXXXIII. törvény alapján a Társaság jelen szabályzatban rendelkezik a vagyonvédelemmel kapcsolatos rögzített hang- és kamerafelvételek megőrzéséről, valamint archiválásáról.

Az üzleti céllal rögzített hanganyag bejelentési kötelezettség alá eső adatkezelésnek minősül, emiatt arra az Adatvédelmi törvény és a Társaság Adatvédelmi Szabályzat dokumentuma vonatkozik.

Általános követelmények a vagyonvédelmi okból rögzített hang- és kamerafelvételek tárolására vonatkozóan:

- A rögzített kép-, hang-, valamint kép- és hangfelvételt felhasználás hiányában legfeljebb a rögzítéstől számított három munkanap elteltével meg kell semmisíteni, illetve törölni kell.
- A rögzített kép-, hang, valamint kép- és hangfelvételt felhasználás hiányában legfeljebb a rögzítéstől számított hatvan (60) nap elteltével meg kell semmisíteni, illetve törölni kell, ha a rögzítés célja
    - a pénzügyi szolgáltatást, kiegészítő pénzügyi szolgáltatást,
    - befektetési szolgáltatási, tőzsdei tevékenységet,
    - elszámolóházi tevékenységet folytatóknak a feladataik ellátásához szükséges, nyilvános magánterületének védelme.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

Felhasználásnak az minősül, ha a rögzített kép-, hang-, vagy kép- és hangfelvételt, valamint más személyes adatot bírósági vagy más hatósági eljárásban bizonyítékként felhasználják.

Az, akinek jogát vagy jogos érdekét a kép-, hang-, vagy a kép- és hangfelvétel, illetve más személyes adatának rögzítése érinti, a kép-, hang-, valamint kép- és hangfelvétel, illetve más személyes adat rögzítésétől számított három munkanapon, illetve hatvan napon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot a Társaság ne semmisítse meg, illetve ne törölje.

Bíróság vagy más hatóság megkeresésére a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni.

Amennyiben megkeresésre attól számított harminc napon belül, hogy a megsemmisítés mellőzését kérték, nem kerül sor, a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell, kivéve, ha a fent említett 60 napos határidő még nem járt le.

A rögzített felvételt, valamint más személyes adatot a vezérigazgató által kijelölt egy vagy több olyan személy jogosult megismerni, aki megfelelő kompetenciával rendelkezik a szervezeten belül ahhoz, hogy döntsön az esetleges felhasználásról.

A rögzített felvétel megismerésére jogosult nevét, az adatok megismerésének okát és idejét jegyzőkönyvben kell rögzíteni.

5. Informatikai egységek védelmi ellenőrzése

A HUPX Zrt. mindent elkövet annak érdekében, hogy a kommunikációs, informatikai, és vagyonvédelmi rendszerét megóvja a jogosulatlan hozzáférésektől. Amennyiben mindezek ellenére a HUPX Zrt. olyan jogosulatlan hozzáférést észlel – vagy annak akár csak a gyanúja felmerül –, amely a bizalmas adatok, illetve információk nyilvánosságra kerülését is eredményezheti, a HUPX Zrt. haladéktalanul köteles a Magyar Energetikai és Közmű-szabályozási Hivatalt (MEKH) írásban tájékoztatni. Az üzemzavarokat előidéző kockázatok fajtáit és azok bekövetkezésekor végrehajtandó akciókat a HUPX Zrt. Üzletfolytonossági stratégiája és Üzletfolytonossági terve tartalmazza.

A HUPX Zrt. az átláthatóság biztosítása érdekében a különböző célú alrendszereit úgy alakítja ki, hogy azok egyértelműen elválaszthatók legyenek egymástól, továbbá a bizalmas adatok és információk védelme érdekében az alábbi intézkedéseket hajtja végre.

5.1. Vírusvédelem

A számítógépes vírusok által okozott adatvesztés és az informatikai rendszerek működésének akadályozása, illetve ellehetetlenítése ellen az informatikai vagyon megóvása érdekében védekezni kell. A számítógépes vírusok által okozott károk elleni összehangolt védekezés szabályait és az ehhez kapcsolódó felelősségi köröket a HUPX Zrt. Vírusvédelmi szabályzata tartalmazza.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

5.2. Hálózati adatforgalom

a) Bizalmas adatok Interneten keresztül a lehetőségek szerint kriptográfiai támogatás mellett továbbítandók a HUPX Zrt. és külsős partnerek között.

b) Saját vagy bérelt iparági vonalon a titkosítás nem feltétlenül szükséges, kiváltképp, ha a titkosító algoritmusok alkalmazása az üzemeltetés követelményrendszeréhez nem illeszthető.

c) A HUPX Zrt. belső hálózatának rendszeres – lehetőleg évenkénti – átvilágítását el kell végezni, az adatforgalom és jelszóval védett objektumok biztonsága érdekében.

d) Kerülni kell a kódolás nélküli kapcsolatteremtést az informatikai egységek között. Jelszóval ellátott applikációk titkos adatai lehetőség szerint kódolás mellett áramoltathatók az informatikai rendszerben.

e) A felhasználóknak tilos a HUPX Zrt. hálózati konfigurációjának illetéktelen megváltoztatása, ami magába foglalja a munkaállomásuk hálózati beállításait (IP cím, stb.).

f) A nyilvános hálózatokon nyújtott alkalmazásszolgáltatások megtervezésénél kockázattal arányos védelmi mechanizmusokat kell beépíteni az alkalmazásszolgáltatások által nyilvános hálózatokon átvitt információk védelme érdekében. A védelmi mechanizmusokat úgy kell kialakítani, hogy védelmet nyújtson a tisztességtelen tevékenységekből eredő esetleges adatvesztések, adattorzulások, jogosulatlan közzététel, illetve üzenetismétlés, vagy -újraküldés által okozott károk ellen.

5.2.1. Külső egységekkel folytatott adatkommunikáció audit és monitoring támogatása

a) A HUPX Zrt. külső egységekkel folytatott, biztonságos adatkommunikációjának megvalósítása érdekében az egyes eseményeket audit és monitoring funkciókkal kell ellenőrizni.

b) A rendszerek közötti átjárhatóságot szigorú szűréssel kell megvalósítani. A szűrés IP cím, protokoll és port alapján kell megvalósuljon.

c) A keletkezett log-file-ok mentése, tárolása és kiértékelése a Rendszerüzemeltető feladatköre.

d) Amennyiben a tűzfal üzemeltetését nem a HUPX Zrt. szakemberei végzik, úgy a szabályzatban rögzített előírások megvalósítása az üzemeltető céget terhelik.

5.3 A jogosultsági rendszer biztonsági előírásai az alrendszerek specifikus tulajdonságai alapján

a) A HUPX Zrt. a jogosultságok kezelését egy jogosultság nyilvántartó rendszerben tartja nyilván. A változtatási igényeket dokumentált módon nyilván kell tartani.

b) A rendszerekben nyilvántartott felhasználók jogosultságait minimalizálni kell; kizárólag olyan jogosultságot szabad megadni, melyek a munkavégzéshez

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

feltétlenül szükséges. A felhasználói jogok igénylésével, engedélyezésével, és kiadásával, illetve visszavonásával kapcsolatos folyamatokat, szerepköröket és mindezek dokumentálását szabályozni kell. Nem engedélyezett a fejlesztői rendszerből az éles rendszerbe való jelszó nélküli átjelentkezés.

c) A központi szerepet betöltő rendszerek alapbeállítása szerint az alábbi naplóvezetési funkciók automatikus működtetése kötelező:

- sikeres bejelentkezések;
- sikertelen bejelentkezések;

d) A keletkezett log file-ok tárolását legalább hat hónapig kell biztosítani.

5.4 Betörésvédelmi tesztek végrehajtása

a) A számítógépes objektumok védelmének fokozása érdekében alkalmazni kell betörésvédelmi teszteket, amely ellenőrző tesztek a különböző operációs rendszerek és hálózati elemek konfigurálásaiból, illetve rendszer specifikus alkalmazások beállításaiból adódó biztonsági rések felderítésére irányulnak, így a monitoring funkciók alkalmazása mellett fokozott biztonság érhető el.

b) A betörésvédelmi tesztek lefuttatását rendszeresen, évente el kell végezni a HUPX Zrt. tulajdonát képző, illetve – előzetes értesítés mellett – a HUPX Zrt-nek szolgáltatott, a társaság érdekében üzemeltetett informatikai rendszerekre.

c) A betörésvédelmi teszteket a HUPX Zrt. szakképzett külső erőforrás bevonásával végzi el.

d) A betörésvédelmi teszt végrehajtásának ügymenete:

A betörésvédelmi tesztek végrehajtására az információbiztonsági felelős adhat engedélyt. A teszthez szükséges technikai paraméterek (pl. hálózati cím) megadása ezen engedély alapján történhet.

A tesztet végrehajtó egységet a rendszer alhálózatára kell csatlakoztatni. Több hálózati csatolóval rendelkező tesztelt egység esetében a teszteket minden kapcsolódó alhálózaton el kell végezni.

A teszttel kapcsolatos kockázatok miatt a végrehajtás során a tesztelt egység Rendszerüzemeltetője jelen kell, hogy legyen (illetve külső rendszer esetén elérhetőnek kell lennie úgy, hogy adott esetben be tudjon avatkozni). A tesztről naplófájlt kell készíteni, majd ez alapján biztonsági elemzést kell készíteni. A naplófájlt és az elemzést az információbiztonsági felelősnek kell átadni.

e) A biztonsági rés elhárításáról az információbiztonsági felelős javaslata alapján, valamint a HUPX Zrt. kockázatkezelési eljárásainak figyelembevételével a rendszer Rendszerfelelőse dönt.

f) A tesztelés során keletkezett naplóállományokat minimum egy évig tárolni kell. Az állományok tárolásáért az információbiztonsági felelős felel.

g) A rendszerek adminisztrátori karbantartására jogosult felhasználókon kívül más személy számára nem engedélyezett a különböző rendszer segédprogramok (pl.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

Registry editor, User manager) használata. Az információbiztonsági felelős által jóváhagyott audit programok használata engedélyezett a betörési tesztet végrehajtó személyek számára. Ezek a programok jelentős kockázatokat hordoznak, mert képesek a rendszerből érzékeny adatokat kinyerni, illetve a használójuk képes lehet a rendszer kontrolljait áthágva módosításokat tenni, ami a rendszerek rendelkezésre állását veszélyeztetheti. A segédprogramokat csak a jogosult felhasználók használhatják, megfelelő autentikációt követően a tesztek és a karbantartás elvégzéséhez szükséges feladatok és időtartam erejéig. A segédprogramok használatát naplózni kell, és rendszeres ellenőrzéseket kell végezni annak felderítésére, hogy történt-e jogosulatlan használat.

5.5 Elektronikus levelezés

a) A HUPX Zrt. saját tulajdonú vagy bérelt hálózatán keresztül történő elektronikus levelezéssel kapcsolatos feltételrendszer kialakítása teljes mértékben a HUPX Zrt. hatáskörébe tartozik.

b) A HUPX Zrt. fenntartja az elektronikus levelek vírus szűrésének jogát.

c) Amennyiben az elektronikus levelezés kódolatlan formában történik, a hálózatra csatlakozva a levél tartalma bárki által olvasható, ezért a visszaélések elkerülése érdekében a HUPX Zrt. informatikai rendszerének titkos adatait (pl. számítógép- vagy felhasználó-specifikus adatok) vezetői engedélyeztetés nélkül tilos bárminemű, titkosítás nélküli átvitelt használó elektronikus úton (e-mail, FTP, Internet) kiáramoltatni a HUPX Zrt-ből.

d) A HUPX Zrt. saját tulajdonú, vagy bérelt rendszerein biztosított elektronikus levelezés csak és kizárólag a céggel kapcsolatos üzleti levelezésre, valamint a kollégákkal történő kapcsolattartás céljából használható, magán célra nem vehető igénybe.

e) A cégtől kilépett kollégák postafiókjához az illetékes területi vezető adhat hozzáférési jogosultságot maximum 3 hónap időtartamra. Az adott kolléga kilépésétől számított 3. hónap elteltével a kilépett kolléga postafiókját archiválás után törölni kell.

5.6 Távoli bejelentkezés

A HUPX Zrt. távoli hozzáférést biztosít a munkatársak számára az informatikai rendszerei (pl. levelező és file szerver) távoli elérésére, valamint üzemeltetői feladatok ellátásához külső Rendszerüzemeltetők részére. A HUPX hálózat külső elérése jelszavas kétfaktorú autentikáció után történhet. Az eléréséhez a felhasználók csak a HUPX Zrt. saját tulajdonú, és a HUPX Zrt. által a HUPX működése érdekében bérelt eszközeit, illetve a Servicedesk által bevizsgált és az információbiztonsági felelős által engedélyezett eszközöket vehetik igénybe, azonban szigorúan tilos a munkaállomás merevlemezére a HUPX Zrt. korlátozott hozzáférésű és üzleti titoknak minősülő adatainak titkosítás nélküli lementése.

Üzleti alkalmazások, a telephely és a szolgáltató közötti „site to site” VPN kapcsolat és az egyedileg létrehozott VPN kapcsolatok biztonság szempontjából nem

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

különbözhetnek.

5.7 Internet elérés

a) A HUPX Zrt. saját tulajdonú vagy bérelt hálózatán keresztül történő Internet eléréssel kapcsolatos feltételrendszer kialakítása teljes mértékben a HUPX Zrt. hatáskörébe tartozik.

b) A HUPX Zrt. fenntartja az erőforrások feletti rendelkezési jogát.

c) A HUPX Zrt. fenntartja az Internetes oldalak elérhetőségének korlátozási jogát.

d) A HUPX Zrt. fenntartja az Internetes alkalmazások ellenőrzésének és tartalomszűrésének jogát.

e) A HUPX Zrt. fenntartja az Internetes adatforgalom korlátozásának jogát.

5.8 A munkaállomások zárolása

Abban az esetben, amikor a felhasználók munkaállomásaikat felügyelet nélkül hagyják, kötelesek a munkaállomást zárolni úgy, hogy a zárolás csak az arra jogosult által legyen feloldható. A munkaállomás használatát nem szabad senkinek átengedni úgy, hogy eközben a munkaállomás funkcióinak illetéktelen használatával az informatikai biztonság sérülhessen.

5.9 Egyéb felhasználói felelősségek

A jelen szabályzat alapján a HUPX informatikai rendszeréhez kapcsolódó valamennyi felhasználó kötelessége erős jelszavak használata.

A beállított inaktivitás után (15 perc) a munkaállomás automatikusan lezáródik.

5.10 Beléptető-rendszer (fizikai határzóna)

A HUPX Zrt. irodáinak és szervertermének belépési pontjain, önálló az irodaháztól független kártyás beléptető-rendszert üzemeltet. Az adott belépési pontokon csak az adott jogosultsággal rendelkező kártya birtokosa léphet be, mely belépés regisztrálásra kerül.

Biztonsági területként kerül meghatározásra a HUPX székhelyén lévő, a HUPX irodai infrastruktúráját kiszolgáló szerverterem. A szerverterembe való bejutáshoz rendelkezni kell az adott biztonsági területre vonatkozó jogosultsággal, így a szerverterembe csak az adott jogosultsággal rendelkező személyek léphetnek be. Amennyiben szükséges (pl. karbantartási munkálatok miatt) jogosultsággal nem rendelkező személyek bejutása, abban az esetben a munkavégzés csak egy arra jogosult személy felügyelete mellett történhet. Az adott jogosultsággal nem rendelkező személyek a szerverteremben felügyelet nélkül nem hagyhatók.

5.10.1. Belépésre jogosultak nyilvántartása

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

A beléptető rendszerhez szükséges kártyák és az egyes belépési pontokon való bejutási engedély kérelmet a Jogosultságok kezelése folyamat szabályai szerint kell benyújtani. A belépőkártya jogosultságok engedélyezése a vezérigazgató jogkörébe tartozik. A kártyák kiadásáról átadás-átvételi bizonylat készül.

A HUPX telephelye riasztóval védett, melynek élesítéséért a munkanap végén utolsóként távozó munkavállaló felelős. A riasztó kódjának kiadásáért a titkárságvezető felelős.

5.10.2. Kilépések kezelése

Kilépéskor a Társaság a következők végrehajtásáról gondoskodik, melyről jegyzőkönyvet készít:

- Kilépő hozzáféréseinek megszűntetése
- A társaság tulajdonát képező, vagy a társasággal szerződéses viszonyban álló szolgáltatóktól bérelt eszközök visszavétele
- Hitelesítő eszközök visszavétele
- Kilépő feladatainak átadása/átvétele
- Amennyiben szükséges, fokozottan gondoskodik arról, hogy a kiléptetés az informatikai rendszerek biztonságát ne veszélyeztesse

5.11 Berendezések karbantartása

A berendezések karbantartása lehetőség szerint a helyszínen történik. A karbantartást csak megfelelő képzettséggel és hozzáférési jogosultsággal rendelkező személy végezheti.

5.12 Selejtezés, újrafelhasználás, vagyontárgyak eltávolítása

A berendezések, adathordozók selejtezése esetén az érintett Rendszerüzemeltető, asztali, mobil eszközök és adathordozóik, illetve cserélhető és külső adathordozók (pl. pendrive) esetében a Servicedesk-es kollégák gondoskodnak az adatok biztonságos eltávolításáról, az információbiztonsági felelős előzetes tájékoztatása és engedélye mellett.

Az adathordozók biztonságos megsemmisítése érdekében a felhasználók a feleslegessé vált adathordozókat az információbiztonsági felelősnek adják át selejtezésre, melyről jegyzőkönyvet kell felvenni.

Berendezések, illetve szoftverek csak az információbiztonsági felelős előzetes engedélyével vihetők ki a telephelyről. Ezen szabályozás nem vonatkozik a személyes használatra átadott eszközökre (pl. laptop).

5.13 Naplózási feladatok

A hozzáférések utólagos, naplók alapján történő ellenőrzése a Rendszerüzemeltető felelőssége. A rendszerszolgáltatással kapcsolatos eseményeket rögzítő

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

naplóállományok mentéseivel, illetve a kritikus archivált állományokkal kapcsolatban is követelmény a hozzáférési jogosultságrendszer kidolgozása, valamint a hozzáférések regisztrálása.

A rendszeradminisztrátori tevékenység naplózása a szolgáltató nyilvántartó rendszerében történik.

A hibák naplózása a hibabejelentő rendszerben történik.

6. Szoftver specifikus előírások

a) A HUPX Zrt. tulajdonát képző informatikai egységekre kizárólag jogtiszta szoftvereket szabad telepíteni, azokról csak a licencszerződésben megengedett számú másolat készülhet.

b) A HUPX Zrt. minden indokolt szoftverigény kielégítésére megfelelő mennyiségű jogtiszta szoftvert biztosít. A HUPX Zrt. számítógépein indokolt esetben, a számítógép felhasználója vezetőjének engedélyével, és az információbiztonsági felelős hozzájárulásával nem HUPX Zrt. által beszerzett, de legális szoftver (pl. üzleti használat esetén is ingyenes) free software, shareware (a próbaidőszakon belül), a munkavállaló saját licence, stb. is használható. Ezen szoftverek használatát az információbiztonsági felelőssel írásban véleményeztetni, illetve engedélyeztetni kell. Az ilyen szoftverek forrását és legalitását a felhasználó bizonyítani köteles.

c) A megvásárolt felhasználói programokkal és licence jogokkal kapcsolatos adatokról a HUPX Zrt. nyilvántartást vezet.

d) Új programok beszerzése vagy frissítése esetén a licence nyilvántartást is frissíteni kell.

e) A HUPX Zrt. számítógépei és egyedi számítógépes rendszerei munkaeszközök, amelyek megfelelő működését biztosítani kell. A számítógépek konfigurációjának változtatását, szoftverek telepítését vagy azok eltávolítását csak megfelelő szakértelemmel és jogosultsággal szabad végezni. Ilyen tevékenység végzésére az illetékes Rendszerüzemeltetők, a Servicedesk kollégák, illetve az információbiztonsági felelős által arra feljogosított személyek jogosultak.

f) Az egyéni felhasználóknak joguk van információért fordulniuk a Servicedesk kollégákhoz, amennyiben új alkalmazás telepítése során kérdés merül fel a szoftver jogtisztaságát illetően.

g) A Servicedesk kollégák jogosultak ellenőrzést végezni a személyes felhasználásra átadott informatikai eszközökön az azokon található szoftverek legalitására vonatkozóan. Amennyiben a Servicedesk kolléga illegálisan feltelepített alkalmazást talál, úgy köteles írásban tájékoztatni az egység felhasználóját, a felhasználó közvetlen felettesét és a vezérigazgatót.

h) A Servicedesk kolléga tevékenysége nem irányulhat jogosulatlan információ megszerzésére.

i) A telepített alkalmazásokhoz, a felhasználói segédlet hozzáférését biztosítani kell a felhasználók számára.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

j) A forráskódokhoz csak az arra feljogosítottak – rendszerüzemeltetők és rendszerfelelősök –, valamint a szerződésben rögzített külső támogatók és fejlesztők férnek hozzá.

7. Az informatikai rendszerek HUPX tagokkal történő tesztelése

A kereskedési rendszerek fejlesztéseinek tagokkal történő tesztelése az alábbi lépések mentén történik:

a) A teszt célja írásban meghatározásra kerül, ami alapján vezetői döntés születik a teszt elindításáról és pontos időpontjáról.

b) Ezután ki kell dolgozni a tesztforgatókönyvet, előkészíteni a teszt rendszert a teszt hozzáférések nélkül.

c) Össze kell állítani a tesztelésre meghívandó partnerek listáját, és a meghívót a tesztelésre. A tesztelés megkezdése előtt két héttel kiküldésre kerül a meghívó a regisztráció részleteivel. Kevés regisztráló esetén a határidő lejárta előtt újabb üzenetben kell emlékeztetni a tagokat a regisztrációra.

d) A regisztrációk alapján elkészülnek a teszt hozzáférések. Tájékoztató készül és kerül kiküldésre a teszt részletes menetéről, aminek része a tesztforgatókönyv is. A teszt megkezdése előtt egy munkanappal kapják meg a regisztrációban megjelölt kontaktszemélyek a teszt során használandó felhasználónevet és jelszót. A felhasználói azonosító és jelszó átadását a jelen szabályzat 3.3.7. pontjában megfogalmazottak alapján kell elvégezni.

e) A teszt során annak monitorozása, illetve a helpdesk ügyelet biztosított. A teszt lezárásakor a teszt rendszer elérhetőségét meg kell szűntetni.

f) A teszt részvevőitől a visszajelzéseket, észrevételeket be kell kérni, amennyiben azt maguktól nem küldik. A visszajelzések és a monitorozás során összegyűjtött HUPX tapasztalatokból tesztjegyzőkönyv készül, ami alapján döntés születik az új rendszer/rendszerelem bevezetéséről.

Mivel a tesztelés külön e célra létrehozott teszt környezetben zajlik fiktív adatokkal, így a tagok tényleges kereskedelmi adatai nem kerülhetnek illetéktelenek birtokába a tesztelés során. Teszt környezethez adott hozzáférésekkel nem lehet az éles környezetbe belépni, ott adatokhoz, kereskedelmi funkciókhoz hozzáférni.

8. Az Informatikai elemek dokumentációkezelése

Dokumentációnak számít minden papír alapú dokumentáció és adathordozón tárolt információ is, amelyek lehetnek maguk a HUPX Zrt.-ben feltelepített alkalmazások vagy azok felhasználó segédletei.

8.1 Az Informatikai elemek dokumentálása

a) A HUPX Zrt. hálózatára telepített minden informatikai elem (független informatikai alrendszer, eszköz, alkalmazás) mellé átadáskor csatolni kell az informatikai

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

elemmel kapcsolatos dokumentációkat.

b) A dokumentációk elkészítése az informatikai elem telepítésével megbízott kivitelező feladatköre.

c) Egy telepített informatikai elem átvétele kizárólag a mellékelt dokumentációk átadása esetén engedélyezett.

d) A csatolt dokumentációknak tartalmazniuk kell az új rendszer eszköz vagy alkalmazás

- telepítésének ügymenetét,
- a telepítéssel kapcsolatos konfigurációs beállításokat,
- az eszköz hardver és szoftver dokumentációit,
- az eszköz/alkalmazás felhasználói segédletet,
- az eszköz menedzselésére vonatkozó útmutatásokat.

e) Az új informatikai elem átvétele után a mellékelt dokumentációkról másolatot kell készíteni két példányban, amely az átvételért felelős személy feladata.

8.2 Az Informatikai elemek dokumentációinak tárolása

a) Minden dokumentációból másolati példányt kell készíteni. Egy eredeti példányt a HUPX Zrt. székhelyén zárható, megfelelő objektumvédelemmel ellátott helyen, egy másolati példányt pedig elektronikusan megfelelő hozzáférési jogosultságok kialakítása mellett a HUPX file szerverén, vagy DMS rendszerében kell elmenteni.

b) Az eredeti példány nem adható ki.

c) Minden dokumentációhoz, ún. fedőlapot kell készíteni, mely tartalmazza a dokumentum:

- nevét,
- azonosítóját,
- verzió számát,
- minősítését

e) A dokumentumokról összesített nyilvántartást kell készíteni. A nyilvántartásban fel kell tüntetni a meglévő valamennyi dokumentum:

- nevét,
- azonosítóját,
- verzió számát,
- minősítését,
- az adathordozó típusát.

8.3 Az Informatikai elemek dokumentációinak ellenőrzése

a) A HUPX Zrt. informatikai elemeinek dokumentációiról készített leltár alapján, év

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

végén ellenőrizni kell a tárolt dokumentációkat.

b) A leltár elvégzése az egyes informatikai eszközökért felelős Rendszerfelelősök feladatkörét képzi.

c) A leltár során feltárt hiányosságokról értesítendő az információbiztonsági felelős.

9. Külső szolgáltatók és a HUPX Zrt. informatikai elemeinek kapcsolata

A HUPX Zrt. funkcionalitás szempontból egymástól elkülönülő informatikai rendszereinek telepítését, üzemeltetését nagyrészt külső szolgáltató cégek végezik, ezért számukra biztosítani kell az általuk támogatott IT-egységekbe való bejelentkezés lehetőségét az adott fejlesztési, támogatási és üzemeltetési időszak alatt. A telepítést végző cégek a garanciális karbantartási munkákat, valamint a szakmai támogatást – amennyiben az lehetséges – ún. távoli bejelentkezés révén végzik. Ennek megvalósítása érdekében engedélyezni kell a cégek távoli bejelentkezését a HUPX Zrt. informatikai hálózatába, bizonyos esetben akár szuperfelhasználói jogosultsági szint mellett is.

A külső cégekkel kötött – az informatikai biztonságot lényegesen érintő – informatikai vonatkozású szerződések műszaki tartalmát véleményeztetni kell az információbiztonsági felelőssel. A kiszervezés keretében külső szolgáltatókkal történő szerződéskötéskor érvényre kell juttatni HUPX Zrt. vonatkozó előírásait.

9.1 Külső szolgáltatók által telepített rendszerre vonatkozó előírások

a) Amennyiben a HUPX Zrt. informatikai rendszereinek fejlesztése során bizonyos feladatok elvégzése külső szolgáltatók bevonásával történik, úgy a fejlesztésben részvevő szolgáltatók kötelesek a HUPX Zrt. Információbiztonsági szabályzatának 1.4 pontjában foglaltaknak megfelelően eljárni a kivitelezési munkák elvégzése során.

b) A kivitelezőnek a rendszer telepítése során el kell készíteni a rendszer dokumentációit, az ide vonatkozó szabályzati pontnak megfelelően.

c) A kivitelezőnek a rendszer konfigurálása esetén eleget kell tennie az IBSZ-ben foglaltaknak.

9.2 Külső üzemeltetésre vonatkozó előírások

a) A külső üzemeltetési szerződések megkötésekor figyelembe kell venni a HUPX Zrt. előírásait.

b) A kiszervezés keretében üzemeltetett rendszerek üzemeltetői kötelesek meghatározott időközönként jelentést készíteni a HUPX Zrt. számára az üzemeltetés eseményeiről, illetve azonnali intézkedést igénylő és/vagy rendkívüli események fellépése esetén, soron kívüli jelentést küldeni.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

9.3 Karbantartási feladatok elvégzése helyi bejelentkezés révén

a) A kivitelező a karbantartási munkák elvégzéséhez adminisztrátori jogosultsággal is bejelentkezhet a HUPX Zrt. telephelyén az erre a célra meghatározott informatikai eszközökön.

b) A karbantartási munkák során végzett változtatásokat a karbantartó köteles dokumentálni és azt a rendszer felelősének (Rendszerfelelősnek) átadni.

c) A karbantartási munkák során készített naplóállománynak tartalmaznia kell

- a karbantartást végző személy nevét,
- a bejelentkezés módját,
- a munkafolyamat rövid leírását,
- a munkafolyamat révén elért IT egységek listáját,
- a munkafolyamat során módosított konfigurációs file-ok listáját.

9.4 Karbantartási feladatok elvégzése távoli bejelentkezés révén

a) A külső cégek távoli bejelentkezésére vonatkozó előírások:

- A HUPX Zrt. informatikai rendszereibe a távoli bejelentkezés csak 2 faktorú autentikáció útján történhet.
- a bejelentkezés kizárólag a HUPX Zrt. szakemberének és információbiztonsági felelősének előzetes engedélyezése esetén valósulhat meg,
- Az engedély kérelem során fel kell tűntetni az igénylő nevét, igénylés okát és a hozzáférés időtartamát,
- a bejelentkezéseket szigorúan naplóállományban rögzíteni kell,
- root/adminisztrátori jogosultságot kizárólag HUPX Zrt. szakembere adhat ki az Rendszerüzemeltetők számára.

b) Amennyiben szükség van az eszközökhöz a távdiagnosztikai portokon keresztüli csatlakozásra a HUPX Zrt. erre jogosult Rendszerfelelősei aktiválhatják azokat.

10. Információbiztonság a projektvezetésben

A projektvezetés során a projektvezető felelőssége, hogy az adott projekttel kapcsolatban keletkezett információs vagyonelemek minősítéséről gondoskodjon és meghatározza a hozzáférési jogosultságokat, különös tekintettel a keletkezett eredménytermékekre, pl. rendszer dokumentációk, forráskódok, stb. A hozzáférési jogosultságok kiosztása és adminisztrálása a jelen szabályzatban foglaltak mellett a Jogosultságok kezelése (IT.7.) folyamatban meghatározottak szerint kell történnie.

A projekt zárását követően a projektvezető felelőssége, hogy a projekt során kiosztott a projekt végrehajtásához szükséges ideiglenes hozzáférési jogosultságok visszavonásáról gondoskodjon.

A fejlesztési projektekkel kapcsolatos információbiztonsági előírásokat a HUPX Zrt.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

Informatikai fejlesztési szabályzata tartalmazza.

11. Emberi erőforrások biztonsága

A HUPX Zrt. az információs vagyonelemei védelme érdekében az egyes munkakörök betöltésére megfelelő kompetenciákkal, ugyanakkor megfelelő erkölcsi normákkal rendelkező személyek kiválasztására törekszik, ezért a szakmai kompetenciák meglétén túl a munkakör betöltésének előfeltétele, hogy a HUPX Zrt. leendő munkavállalója büntetlen előéletét igazolja a munkaviszony megkezdése előtt a büntetlen előéletet igazoló nyilatkozat aláírásával. Ezen felül a HUPX Zrt. valamennyi állásra pályázó esetében a működése által megkívánt mértékben és a törvényi, szabályozási, etikai előírásoknak megfelelően, háttérellenőrzéseket végezhet.

A belépés alkalmával a munkavállalók információbiztonsági képzésben részesülnek, ahol jelenléti ív aláírásával kell igazolniuk részvételüket és az elhangzottak tudomásul vételét. Emellett évente fókuszált biztonsági továbbképzésben részesül a HUPX Zrt. valamennyi munkavállalója, melyet követően 50 kérdésből álló ellenőrző teszt kitöltésével történik a visszaellenőrzés.

A kilépő munkavállaló felettese köteles legkésőbb az adott munkavállaló kilépésének napján gondoskodni az adott munkavállaló információs vagyonelemekhez való hozzáférési jogosultságainak visszavonásáról. A HUPX Zrt. szabályzatai, utasításai, illetve általános erkölcsi normák megsértése miatt távozni kényszerülő munkavállalók információs vagyonelemekhez való hozzáférési jogosultságainak visszavonásáról a lehető leghamarabb gondoskodni kell. Ez valamennyi vezető felelőssége.

12. Adathordozók kezelése

A HUPX Zrt. mindent elkövet annak érdekében, hogy a rendszerein tárolt adatokhoz illetéktelenek ne férhessenek hozzá. Ennek érdekében adattároló eszközeit fizikai védelemmel, a rajtuk tárolt adatokhoz való hozzáférést pedig szabályzatok és jogosultsági rendszerek kialakításával és üzemeltetésével biztosítja.

Az adathordozók szállítása előtt gondoskodni kell az adott adathordozón tárolt adatok biztonságos mentéséről és szállítás közben a kockázattal arányos védelem biztosításáról.

13. Berendezések védelme

Kritikus, kulcsfolyamatokat kiszolgáló infrastruktúra tervezésekor szem előtt kell tartani az áramkimaradások és közműszolgáltatások hibáiból, esetleges kiesésükből származó az adott infrastruktúrát érintő fenyegetéseket is. A kritikus, kulcsfolyamatokat támogató infrastruktúrát úgy kell kialakítani, hogy az ilyen hibák, kiesések esetén is biztosítsa a folyamatos üzemet az üzletfolytonossági elvárásoknak megfelelően.

Az energiaellátási, valamint az adatátviteli vagy információszolgáltatásokat támogató távközlési kábeleket védeni kell a lehallgatástól, a zavarásoktól vagy a károsodástól.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

A berendezések elhelyezésekor biztosítani kell a kockázattal arányos fizikai védelmet.

14. Tiszta asztal szabálya

A HUPX Zrt. telephelyén dolgozó valamennyi munkavállaló felelőssége, hogy céges információkat tartalmazó papír alapú dokumentumokat, külső adattároló eszközöket (pl. pendrive, külső merevlemez), valamint mobil eszközöket (pl. mobil telefon, notebook) ne hagyjanak őrizetlenül. A munka végeztével valamennyi külső adathordozót, mobil eszközt és minden nem nyilvános adatot tartalmazó dokumentumot, biztonságosan el kell zárni.

15. Fejlesztési és tesztelési környezetek

A fejlesztési és tesztelési környezetet el kell különíteni az éles üzemi környezettől. A jogosulatlan hozzáférések elkerülése érdekében törekedni kell arra, hogy a tesztelési környezetekben az éles adatoktól eltérő, tesztelési célra létrehozott fiktív adatokkal történjen a tesztelés.

Amennyiben a sikeres teszteléshez ezen adatok megléte elkerülhetetlen, akkor az adatok éles környezetből a teszt környezetbe történő másolása és a tesztelés alatti felhasználása során a megfelelő szintű védelmét biztosítani kell.

16. Óraszinkronizálás

Egy szervezeten, vagy biztonsági tartományon belül az összes érintett információ feldolgozó rendszer óráját szinkronizálni kell egyetlen órajel forrással, mint viszonyítási alappal.

17. Incidensek kezelése

A HUPX Zrt. valamennyi munkavállalója köteles a HUPX Zrt. információs és vagyonelemeit érintő incidenseket, gyanús jelenséget (minden, ami eltér a megszokott működéstől) késlekedés nélküli jelenteni a Helpdesk felé. Amennyiben akár csak a gyanúja felmerül, hogy információbiztonságot fenyegető incidens történt, akkor az információbiztonsági felelőst is értesíteni kell. Az információbiztonsági felelős hatásköre eldönteni, hogy az adott eseményt információbiztonsági incidenssé nyilvánit-e. Amennyiben igen, abban az esetben incidens jelentés készül róla. Az incidensről az információbiztonsági felelős tájékoztatja a Biztonsági Bizottságot, sürgős esetben pedig rendkívüli ülést hívhat össze.

A Biztonsági Bizottság tervet dolgoz ki az információbiztonsági incidens elhárítására és az esetlegesen okozott kár minimalizálására. Ezzel egy időben az információbiztonsági incidens jövőbeni kivédésére irányuló kockázattal arányos védelmi tervet dolgoz ki és hajt végre.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

18. Biztonság a fejlesztési és támogatási folyamatokban

A informatikai rendszerekkel kapcsolatos fejlesztéseket és változásokat a különböző szervezeti egységek a Fejlesztési és változás igénylő dokumentum (FID) Informatikai terület felé történő benyújtásával igényelhetnek. A FID-et az Intranet erre a célra kialakított dokumentumtárába szükséges feltölteni.

A benyújtott igényeket az informatikai terület megvizsgálja, az igény jellegétől függően fejlesztési projektet indít, vagy módosítási feladatként kezeli. Fejlesztési projekt esetén a Fejlesztési szabályzatban meghatározottak alapján kell eljárni.

Mindkét esetben a jelen szabályzatban megfogalmazott információbiztonsági előírásoknak megfelelően szükséges elvégezni az adott fejlesztés, vagy változás megvalósítását.

A működtető környezet bárminemű változtatása esetén csak a szállító és az üzleti terület által egyaránt tesztelt változtatásokat lehet telepíteni.

Az operációs rendszerek esetében csak a releváns sérülékenységek kezelését szolgáló, tesztelt javítások telepíthetők.

Az információs rendszereket az IBIR irányelveinek megfelelően úgy kell megtervezni, hogy a rendszer által nyújtott védelmi mechanizmusok és a használatához köthető folyamatok szabályozása révén biztosítsák az adott rendszerben tárolt információk bizalmasságát, sértetlenségét és rendelkezésre állását.

19. Az IBSZ rendszeres felülvizsgálata és változáskezelése

19.1 Az Információbiztonsági Szabályzat automatikus felülvizsgálatát eredményező változások

a) Az IBSZ a (szabályzat elkészítésekor) fennálló informatikai rendszer hardver, szoftver és humán erőforrások alapján került kialakításra.

b) Mivel egy informatikai rendszer egymással szorosan összefüggő részrendszerek integrációjaként jelenik meg a valóságban, ezért a rendszerben történő bárminemű topológiai változás esetén a szabályzatrendszert felül kell vizsgálni és szükség esetén változtatásokat kell bevezetni.

19.2 Az Információbiztonsági Szabályzat érvénybe léptetésének ügymenete

a) Az IBSZ változáskezelésének ügymenete: az IBSZ-ben szükségessé vált változtatások esetén dokumentum új iktatószámot kap, ez biztosítja annak visszakereshetőségét.

b) Szükség esetén az ellenőrzési feladatba külső szakértők bevonása lehetséges. Ez esetben a külső szakértőt titoktartási kötelezettség terheli, melyet a szerződéskötéskor érvényesíteni kell.

c) Vezetői szintű konzílium során az információbiztonsági felelős terjeszti elő a változtatási javaslatokat és engedélyezteti a BB-vel.

1134 Budapest, Dévai utca 26-28.
Telefon: (+36-1) 304-1090
Fax: (+36-1) 304-1099
Web: www.hupx.hu

d) Új Információbiztonsági Szabályzati pont érvénybe léptetése a vezérigazgató engedélyéhez kötött. Az engedélynek ki kell terjednie arra, hogy az új szabályzati pont mikortól kezdve lép életbe, illetve, hogy milyen ütemben kerül sor megvalósítására.

e) Az IBSZ megváltozásáról – körlevélben, elektronikus levélben – értesíteni kell az érintetteket.

20. Hivatkozott szabályozók

A HUPX Zrt. Biztonságpolitikája
A HUPX Zrt. Üzletfolytonossági stratégiája
A HUPX Zrt. Üzletfolytonossági terve
A HUPX Zrt. Vírusvédelmi szabályzata
A HUPX Zrt. Üzleti titkok védelmére vonatkozó szabályzata
A HUPX Zrt. Informatikai fejlesztési szabályzata
Jogosultságok kezelése (IT.7.)