PÁZMÁNY

1635

Pázmány Péter Katolikus Egyetem Információbiztonsági Szabályzata (IBSZ)

PÁZMÁNY
Pázmány Péter Katolikus Egyetem
1635

2023.

Változások, felülvizsgálatok jegyzéke:

Verzió	Dátum	Rövid összefoglaló
1.0	2022.09.06.	Eredeti változat
1.1	2022.10.13.	Módosítások
1.2	2022.11.19.	Osztálybesorolások
1.3.	2022.12.02.	Szervezeti felépítés
1.4	2023.04.17.	Kiegészítések

Dokumentum felülvizsgálata:

Következő tervezett felülvizsgálat dátuma:	Felelős

Jóváhagyta:

Dátum:	Felelős	Aláírás
2022.xx.xx		

PÁZMÁNY
Pázmány Péter Katolikus Egyetem
1635

Dokumentum elektronikus adatai:

Elektronikus tárolás:	Érvényes
PPKE_Informatikai_Szabályzat	2023
Elektronikus verzió tárolási helye:	

Tartalom

1. Általános rendelkezések

1.1. A PPKE IBSZ célja

A **Pázmány Péter Katolikus Egyetem** (a továbbiakban: **PPKE**) feladatai megvalósulásának elősegítése érdekében folyamatait informatikai eszközök használatával teszi hatékonyabbá, gazdaságosabbá és biztonságosabbá. Az informatikai eszközök egyre szélesebb körű használatával azonban új, eddig nem tapasztalt, változó és mindig megújuló kockázatot jelent a **PPKE** számára, ezért jelen információbiztonsági szabályzat célja egységes keret szabályokat, értelmezéseket, iránymutatásokat, biztonsági ajánlásokat adni az adatgazdák, az informatikai eszközök üzemeltetői, fejlesztői, felhasználói számára, rögzítve azokat a szabályokat, amelyeket a munkakörükhöz és jogosultságukhoz rendelt adatok során követniük kell.

A jelen **PPKE Információbiztonsági Szabályzat** (továbbiakban: IBSz) szabályzat célja:

- egységes szemléletben meghatározni a felhasználók és az információtechnológiai rendszerek viszonyát az informatikai rendszerek által kezelt **adatokat, információk bizalmasságának, sértetlenségének, rendelkezésre állásának megőrzése** érdekében;
- azon alapvető biztonsági normák és működési keretek meghatározása, illetve a széles körben elfogadott ajánlások, iránymutatások érvényesítésével a **PPKE** az elfogadható minimumra csökkentheti az adatkezelés és adatfeldolgozás kockázatait, beleértve a hatályos jogszabályi feltételek betartását is;
- a **PPKE**-be bekerülő, illetve ott keletkező adatok, információk informatikai rendszere(ke)n történő adatfeldolgozásával szemben támasztott biztonsági követelmények rögzítése;
- egyértelműen meghatározni a **PPKE**-n igénybe vehető szolgáltatásokat, ezen szolgáltatások határait és a hozzá tartozó, illetve kapcsolódó felelősségeket;
- az informatikai berendezések, halózati eszközök (hardver) és alkalmazási rendszerek (szoftver) biztonságának elősegítése.

1.2. A PPKE Információbiztonsági szabályzat hatálya

A PPKE IBSz hatálya kiterjed a PPKE minden információkezeléssel és -feldolgozással kapcsolatos folyamatára és tevékenységére vagy támogatásukban résztvevő informatikai eszközökre, személyekre, illetve ezek elhelyezésére szolgáló létesítményekre.

A jelen szabályzat felhasználók számára készült kivonata a PPKE Informatikai Felhasználói Szabályzata.

Jelen szabályzat a következő jogszabályokkal összhangban kerül alkalmazásra:

- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info tv.);
- az EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (a továbbiakban: GDPR);
- a minősített adat védelméről szóló 2009. évi CLV. törvény;

Jelen szabályzat az alábbiakban felsorolt figyelembe veendő szabványokkal összhangban kerül kialakításra:

- MSZ EN ISO 9000:2015 Minőségirányítási rendszerek, alapok és szótár;
- MSZ EN ISO 9001:2015 Minőségirányítási rendszerek, alapok és követelmények;
- ISO/IEC 27000:2014 Information Technology – Security Techniques – Information Security Managements Systems. Overview and Vocabulary;
- MSZ ISO/IEC 27001:2014 Infromatika, Biztonságtechnika. Információbiztonsági – irányítási rendszerek. Követelmények;
- ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems;
- MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap és Irányelvek;

- ITIL v4 (Information Tecnhology Infrastructure Library) – Informatikai rendszerek üzemeltetésére és fejlesztésére szolgáló ajánlás „de facto" szabvány;

1.2.1. A PPKE Információbiztonsági szabályzat személyi hatálya

A PPKE IBSz szabályzat személyi hatálya kiterjed:

- A PPKE valamennyi Informatikát alkalmazó vagy az informatikai környezetében működő szervezeti egységre (Intézmények-re / Karok-ra).
- A PPKE valamennyi munkavállalójára és felhasználójára (oktatók, óradók, kutatók, hallgatók, adminisztratív dolgozók, üzemeltetők, stb.)
- A PPKE informatikai rendszerével, szolgáltatásaival kapcsolatban a PPKE szerződéses jogviszonyban álló természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban: külső személy), a velük kötött szerződésben, illetve a titoktartási nyilatkozatban rögzített mértékben. A PPKE-vel szerződéses kapcsolatban álló olyan szervezetekre is, mely információcserét (küldés / fogadás, tárolás / továbbítás) folytat, függetlenül a szervezet betöltött szerepétől, szervezeti elhelyezkedésétől és a PPKE-hez fűződő kapcsolatától.
- A PPKE-vel felhasználói (ideértve a hallgatói) jogviszonyban lévő regisztrált, informatikát használó felhasználójára.

1.2.2. A PPKE Információbiztonsági szabályzat tárgyi hatálya

A PPKE IBSz szabályzat tárgyi hatálya kiterjed:

- A PPKE: adataira, adathordozóira, alkalmazásaira, folyamataira és a szoftverekre. Ezen felül a PPKE IT rendszerére, az infrastrukturális környezetére, az informatikai eszközökre (notebook, desktop, stb.), ezen felül a jogszabályoknak és a külső követelményeknek való megfelelésre.

- A PPKE információkezeléssel és feldolgozással kapcsolatos folyamataiban résztvevő informatikai eszközökre, nyilvántartó rendszerekre, mely az PPKE területén, illetve intézményeiben megtalálhatóak. Valamennyi informatikát alkalmazó és / vagy informatikai környezetben működő szervezeti egységre.
- Ezen felül a PPKE tulajdonában és / vagy használatában lévő informatikai eszközökre és ezen informatikai eszközök által kezelt, illetve tárolt vagy továbbított információira. A PPKE informatikai rendszerére / hálózatára csatlakozó, de nem a PPKE tulajdonában levő eszközökre is, függetlenül ezen eszközök földrajzi elhelyezkedésétől.

1.2.3. A PPKE Információbiztonsági szabályzat területi hatálya

A PPKE IBSz szabályzat területi hatálya kiterjed az informatikai erőforrások üzemelési helyszíneire:

- A PPKE intézményeire és telephelyeire,
- A külső szolgáltatók által, a PPKE-nek nyújtott szolgáltatásaiban érintett helyszíneire.

1.2.4. A PPKE Információbiztonsági szabályzat időbeli hatálya

Jelen PPKE IBSz szabályzat a PPKE Egyetemi Tanács (továbbiakban: ET) által történő elfogadásával lép hatályba, a dokumentumban foglalt feladatok, folyamatok és szabályok ezen időponttól alkalmazandóak. Mindaddig hatályos, amíg új verziót nem fogad el az ET vagy visszavonásra nem kerül. Jelen PPKE IBSz szabályzatot az ET módosíthatja.

Jelen PPKE IBSz szabályzat felülvizsgálatára az Informatikai Osztályvezető (Továbbiakban: ITO) irányításával évente egyszer kötelező jelleggel sor kerül. Minden évben felül kell vizsgálni, annak betarthatósága és aktualizálása szempontjából és értékelni kell, hogy megőrizte-e azon biztonsági fokozatát, amelyet előirányozott. Jelen szabályzatot módosítani kell, ha a felülvizsgálat eredménye, annak betarthatatlanságát vagy aktualizálatlanságát állapította meg, illetve a vizsgálaton kívül olyan külső vagy belső környezeti változás történt, amely szükségessé

teszi azt. Ezek a változások ugyancsak vizsgálatot vonhatnak maguk után, amennyiben nem egyértelmű a kivitelezendő változtatás a PPKE IBSz-re vonatkozó hatása. A szabályzat aktualizálásáért az ITO a felelős. A PPKE IBSz-ben bekövetkezett módosításokról a hatályba lépést követő 14 napon belül minden szabályzat hatálya alá tartozó személyt értesíteni kell.

1.2.5. A PPKE Információbiztonsági szabályzat vezetői elkötelezettség

A Pázmány Péter Katolikus Egyetem minden egyetemi szervezeti egység vezetője közreműködik az információbiztonság megfelelő, hatékony kialakításában és fenntartásában. Ezen felül a PPKE elkötelezett, hogy olyan informatikai biztonsági rendszert épít ki, ami a folyamatszemléletű megközelítésen alapul és a jelenkor ajánlásait is figyelembe veszi. Az informatikai biztonság rendszer alapján a PDCA ciklus és a kockázatmenedzsment alapú gondolkodásmód képezi, így könnyebbé válik a szükséges biztonsági követelmények megértése és alkalmazása, így a folyamatok kialakítása, átgondolása, tovább fejlesztése, és ezeknek a folyamatoknak, a folyamatos korrekciója az eredményes működés alapja.

2. Az Információbiztonság szervezete

2.1. A vezetés elkötelezettsége az információbiztonság ügye iránt

A PPKE IT-SZ és a PPKE IBSz által meghatározott követelményrendszeren keresztül teljesül 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 információbiztonság területén alkalmazandó védelmi alapelveket, amelyeket a teljes körűségre, a zártságra, a kockázatarányosságra, a védelem szintjének folytonos biztosítására, a szabályozást zárt folyamatára és az informatikai rendszer teljes életciklusára vonatkoznak. Alapot teremt az informatikai stratégia részét képező biztonsági stratégia kialakításához.

A pro-aktív, azaz megelőzésre törekvő magatartást tartja szem előtt, elősegíti az információbiztonsággal összefüggő szabályoknak, intézkedéseknek a PPKE szintjén egységes értelmezését. Biztosítja, hogy a rendszerek védelme a jogszabályi előírásoknak eleget tegyen, valamint a védelem hiányából eredő kockázatokkal legyen arányos. Elősegíti, hogy a PPKE kiszolgáló kommunikációs és informatikai rendszereket az adatok titkosságára, bizalmas jellegére és biztonságára vonatkozóan (pl. adatvédelmi törvényeknek megfelelően) üzemeljenek.

2.2. Az információbiztonság koordinálása

Az információbiztonsági tevékenységek koordinálására a PPKE Információbiztonsági Felelőst (IBF) alkalmaz, akit egyben az Informatika Osztály Vezető (ITO) nevezett ki. Hatásköre alá tartozik az információbiztonsági eljárások betartásának ellenőrzése, továbbá az eljárással kapcsolatos folyamatok kontrollálása. Az IBSz kidolgozásának, rendszeres aktualizálásának és a benne foglaltak érvényre juttatásának elsődleges felelőse az IBF és ITO. A Gazdasági Főigazgató felé jelentési kötelezettsége van, aki köteles elbírálni a felé intézett igényeket és azt jóváhagyni, illetve elutasítani.

Az információbiztonsági felelősségi körök kijelölése

Felelős	Tevékenység
Rektor	Biztosítja a munkavégzéshez szükséges személyi és tárgyi feltételeket. A PPKE teljes működéséért felelős, feladata az egyetem szabályozása, operatív tevékenységek koordinálása és ellenőrzése.
Gazdasági Főigazgató	Az informatikai üzemeltetési feladatok koordinálásáért, és felügyeletéért felelős.
Információbiztonsági Felelős (IBF) – (ITO)	Az információbiztonsági tevékenységek meghatározásáért, szabályozásáért, ellenőrzéséért és betartásáért felelős.
Változásmenedzser	A felügyelete alá helyezett alkalmazással kapcsolatos változások nyomon követése, ütemezése továbbá közvetett felelősség a változások végrehajtásáért.
Adatgazda	A meghatározott adatokon adatkezelést végez vagy végeztet, e tevékenységért felelősséggel tartozik, továbbá a munkakör leírásában, mint kinevezett megjelenik a felelősségek megfogalmazása.
Szerverüzemeltető/Hálózat mérnök	Mindenkori közvetett 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 ezen rendszerek működtetéséért Jelentési kötelezettsége van az IBF felé.
Fejlesztő	Az PPKE folyamatait támogató fejlesztések megvalósítása.

Adatbázis adminisztrátor	Adatbázisokkal kapcsolatos rendszeradminisztrációs tevékenységek ellátása, kivéve a biztonsági adminisztrálás feladatait. Rendszeres adatbázis karbantartás, adat leválogatások elvégzése.

2.3. Titoktartási megállapodások

Minden alkalmazottnak / munkatársnak és a PPKE-vel kapcsolatba kerülő külső személynek titoktartási (munkavállalói / alkalmazotti / külsős) nyilatkozatot kell aláírnia, melyben nyilatkozik arról, hogy a munkája során tudomására jutott, a PPKE számára értéket jelentő információt sem a munkavégzése, sem annak vége után nem hozza harmadik fél tudomására.

A Titoktartási (munkavállalói / alkalmazotti) nyilatkozat tartalmi szempontból, a munkavállalók / alkalmazottak felvételét is intéző munkatársnak a jogszabályi előírásoknak megfelelően naprakészen kell tartania. A PPKE munkavállalója / alkalmazottja esetén a munkavállalói nyilatkozat / alkalmazotti nyilatkozat aláíratása és tárolása az Információbiztonsági Felelős (IBF) feladata, külső személyek esetén pedig az adott projekt vezetőjének vagy annak a szervezeti egység, illetve intézmény vezetőjének a feladata, aki a szerződéskötést a PPKE oldaláról kezdeményezi.

2.4. Az információbiztonság független átvizsgálása

A rendszeres információ biztonsági felülvizsgálatok célja a kialakított védelmi rendszer működési hatékonyságának mérése az egyenszilárdságot veszélyeztető hiányosságok és sebezhetőségek feltárása, a szükséges helyesbítő védelmi intézkedések kidolgozása, előterjesztések elkészítése a Rektor részére. A Rektor feladata az információ biztonsági kockázatok független szakértővel történő felülvizsgálata, legalább kétévente. A felülvizsgálatoknak az alábbi területekre kell kiterjednie:

- Adminisztratív biztonság,
- Információs vagyonleltár,
- Információbiztonsági osztályok, osztályba sorolási elvek,
- Emberi erőforrás biztonsága, külső ügyfelek,
- Fizikai és környezeti biztonság, berendezések védelme,
- Kommunikáció és üzemeltetés irányítása, hozzáférés ellenőrzés,
- Információs rendszerek beszerzése, fejlesztése,
- Információbiztonsági incidensek kezelése,
- Működés folytonossága,
- Követelményeknek, jogszabályoknak történő megfelelés.

Külön figyelmet kell szentelni az előző felülvizsgálat során, vagy az adott időszakban észlelt hiányosságok vizsgálatára, a megvalósított védelmi intézkedések működőképességére.

A Rektor 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 a Gazdasági Főigazgató elé terjessze.

A Rektor 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 kiküszöbölését célzó javaslat elkészítése.

Az Adatgazda felelős az általa irányított üzleti területen / szervezeti egységen belül az IBSz-t érintő esemény kezelésére. Ha egy adott területen belülről kezdeményezett változások állnak be azon folyamatokban, melyeket az IBSz (is) szabályoz, erről a változásról írásban (mely történhet e-mail alkalmazásával) értesíteni kell az IBF-et, és a Gazdasági Főigazgatót. Így biztosítható, hogy az információbiztonságot érintő kérdésekben az IBF ellenőrizni tudja a változást, illetve kezdeményezheti az IBSz módosítását, amennyiben szükséges.

Az IBSZ legalább részleges, a megváltozott körülményeket érintő felülvizsgálatát az IBF-nek el kell végeznie az alábbi események bármelyikének bekövetkezésekor:

- a belső szabályozási dokumentumok információbiztonságot érintő módosítása,
- az információbiztonságot is érintő jogszabályváltozás, amennyiben annak hatálya a PPKE-re is kiterjed,
- az információkezelést és -feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében beállt lényeges változás,
- a PPKE tulajdonában vagy használatában lévő informatikai rendszerekben, illetve azok fizikai környezetében beálló lényeges változás.

3. Vagyontárgyak kezelése

3.1. Felelősség a vagyontárgyakért

3.1.1. Vagyonleltár

Valamennyi vagyontárgyat (információ – feldolgozó eszközt vagy ahhoz kapcsolódó vagyontárgyakat) egyértelműen azonosítani kell és valamennyi fontos vagyontárgyról leltárt kell felvenni, és azt meg kell őrizni. A vagyonleltár elkészítése / elkészíttetése és karbantartása az IBF feladata és felelőssége.

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

- hardver konfigurációs – elem,
- szoftver konfigurációs – elem (operációs rendszer, alkalmazás, fejlesztőeszköz, stb.),
- információs konfigurációs – elem (adatbázisok, adatállományok, stb.),
- hálózati konfigurációs – elem,
- szolgáltatási konfigurációs – elem, (világítás, elektromos energia, légkondicionálás, stb.),
- dokumentációs konfigurációs – elem (rendszerdokumentációk, felhasználói kézikönyvek, üzemeltetési utasítások, folytonossági tervek, stb.)

Az adatvagyonleltár elsődleges célja, hogy a PPKE vezetősége, ITO és a kapcsolódó szervezeti egységek naprakészen tájékozódhassanak a PPKE kezelésében és tulajdonában található vagyontárgyakról, folyamatosan meghatározott legyen a védelem tárgya.

3.1.2. A vagyonleltár felépítése

Az adatvagyonleltár az alábbi részekből épül fel:

- adatok leltára adatkörönként megjelölve (címke, metaadat)
- Informatikai alkalmazásleltár (SCCM)
- Szoftver leltár (SCCM)
- Harder leltár (SCCM)
- Dokumentum leltár

3.1.3. Informatika erőforrás leltárok

Az egyes informatikai erőforrásokról rendelkezésre álló nyilvántartások:

- Informatikai alkalmazásleltár, amely naprakész nyilvántartás a szolgáltatásait megvalósító alkalmazások és segédprogramok
    - nevéről,
    - verziójáról,
    - szoftver leltár, amely hardver elemként rögzíti a telepített alapszoftverek
    - nevét,
    - verzióját, a javítókészletek verziójával egyetemben,
    - a telepítéshez szükséges kulcsokat.
- Hardver leltár, amely hardver elemenként, értékhatárhoz kötötten rögzíteni az eszköz kiépítettségét a Társaság 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.

3.1.4. Vagyontárgyak tulajdonjoga

Az adatvagyonnal összefüggő vagyontárgyak (papír alapon és elektronikusan kezelt iratok) minden esetben a PPKE tulajdonában kell, hogy legyenek (iratok, felhasználási jog, hozzáférési jog, stb.). Így, valamennyi információ és az információfeldolgozással összefüggő vagyontárgy az PPKE tulajdona – a felhasználók csak használatra kapják meg azokat.
Szakterületeként szükséges adatgazdákat kijelölni, aki felelős a szakterület adatleltárak elkészítésért és karbantartásáért.

Az adatgazda kijelölését Informatikai Osztály vezető (ITO) jóváhagyásával a Gazdasági Főigazgató végzi. A szoftver eszközök tulajdonjogát illetően a szoftver lehet a PPKE tulajdonában és lehet bérlemény. Az informatikai osztály által használt szoftver és hardver elemek nyilvántartása az Informatikai osztály felelőssége. A szoftver- és hardver leltár naprakészségének ellenőriztetése az Informatikai osztály vezető feladata, az ellenőrzés végrehajtásáért az IBF felelős.
Kiszervezett tevékenységek eseténben a hardver és a szoftver a kiszervezett tevékenységet végző (adatfeldolgozó) tulajdonában is lehet. Használatukkal kapcsolatban a jelen IBSZ által meghatározott biztonsági kritériumoknak kell megfelelniük. Egyéb szerződéses partnerek esetében magának a szerződésnek kell meghatároznia, hogy a szerződés időtartama alatt melyik fél tulajdonában lévő szoftverek és hardvereket használja a partner.

3.1.5. Vagyontárgyak elfogadható használata

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

3.2. Információk osztályozása

3.2.1. Osztályozási elvek

A PPKE 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.

3.2.2. Biztonsági szintek meghatározása

A PPKE egyes számítógépei, informatikai eszközei, valamint a rajtuk futtatott alkalmazásai különböző jelentőséggel bírnak a PPKE biztonságos működésének szempontjából. A tevékenységek biztonsági kockázatának, figyelembevételével, a következő szinteket kell kialakítani.

- 1.szint:

  Ebbe a szintbe tartoznak az alapfunkciók működtetése és biztonsága szempontjából legfontosabb adatok, alkalmazások, rendszerszoftverek, eszközök, berendezése és a környezeti infrastruktúra ide tartozó elemei. Közös jellemzőjük, hogy még rövid időre (0 – 8 óra) történő működéskiesésük sem viselhető el a rendszer számára, illetve hiányuk és a rajtuk tárolt adatok bizalmasságának, sértetlenségének, hitelességének elvesztése olyan biztonsági problémát okoz, amelynek kockázata nem vállalható.

- 2. szint:

  Az ide tartozó informatikai eszközök, alkalmazások működésének viszonylag rövid ideig (8 – 48 óra) tartó kiesése elviselhető terheket ró a PPKE-re, mint a tevékenység ellátása, mind biztonsági szempontból.

- 3. szint:

  A harmadik szintbe tartozó informatikai eszközök, alkalmazások működésének még hosszabb ideig (1 hét) tartó megszűnése sem befolyásolja jelentős mértékben a PPKE működését.

A PPKE hardver-eszközeit az alábbi jellemzők alapján kell besorolni:

- 1. szint:
    - Azok a szerverek, alkalmazások és adatbázisok, amelyek a PPKE létfontosságú üzleti folyamatait és feladatait hivatottak szolgálni.
    - A hálózati eszközpark azon aktív elemei, amelyek nélkül a hálózatnak olyan szegmensei válnának kommunikáció képtelenné, amelyek a PPKE üzleti folyamatainak működés szempontjából létfontosságúak.
    - Azok a speciális informatikai eszközök, amelyek a PKKE, mint szervezet biztonságos működését és védelmét hivatottak szavatolni.
- 2. szint:
    - Azok a szerverek, amelyek működésének kiesése ideiglenesen elviselhető kockázatot jelent.
    - A hálózati eszközpark azon aktív elemei, amelyek nem sorolhatók az 1. szintbe.
    - A speciális feladattal ellátott számítógépek, szerverek (pl. audit, teszt).
    - Azok a személyi számítógépek, amelyek kiemelt fontosságú adatokat tartalmaznak, vagy kiemelt fontosságú hálózati kapcsolattal rendelkeznek (kiszolgálók, aktív hálózati eszközök konfigurálása, banki szoftvert tartalmazó PC).
- 3. szint:
    - Egyéb munkaállomások, amelyeken nem tárolnak kiemelt jelentőségű adatokat, illetve amelyek működésének kiesése a feladatellátás szempontjából nem meghatározó.
    - Azok a hordozható számítógépek, amelyek nem tartoznak a 2. kategóriába.

3.3. A PPKE adatvagyonának besorolása

A PPKE információrendszerében feldolgozott, továbbított, tárolt adatok kockázatarányos védelmének biztosítása érdekében az adatokat be kell sorolni információvédelmi osztályokba.

Az információ-osztályozási rendszert kell használni védettségi szintek meghatározására, valamint arra, hogy közvetítse a különleges kezelési intézkedésekre vonatkozó igényt.

Az osztályozási rendszernek figyelembe kell vennie:

- az információ osztályba sorolt vagyontárgyak sértetlenségének, rendelkezésre állásának és bizalmasságának az üzletmenetre gyakorolt hatását;
- a sértetlenség, rendelkezésre állás és bizalmasság elvesztéséből eredő vagyoni és nem vagyoni kár nagyságát;
- tárolás esetén az adathordozó típusát;
- a teljeskörűség elvét, vagyis az osztályozásnak ki kell terjednie a rendszer összes elem által kezelt információra;
- a besorolásnál fellépő (esetleges) logikai ütközéseket;

Minden besorolás osztályának tartalmaznia kell a kezelés – információfeldolgozás – eljárást is, mely kiterjed a:

- másolásra,
- tárolásra,
- továbbításra,
- megsemmisítésre.

Az információrendszerben elektronikusan tárolt adatok esetén az adatok azon halmazát, amelyekre a tárolás számítástechnikai körülményeiből adódóan jellemzően azonos védettség valósítható meg (közös adatbázis, azonos könyvtár), ugyanabba az információvédelmi osztályba kell sorolni, mégpedig oly módon, hogy a halmaz egészére ki kell terjeszteni a halmaz legérzékenyebb elemének besorolását.

Az adatgazdák – az IBF kezdeményezésére és koordinálásával – az adatok osztályozását évente legalább egyszer felülvizsgálják, és a besorolást megváltoztatják vagy jóváhagyják:

- ha az információkezelést és – feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében lényeges változás áll be,
- a PPKE tulajdonában vagy használatában lévő informatikai rendszerekben lényeges változás áll be.

Az adatokat az alábbiak szerint kell besorolni a meghatározott biztonsági osztályokba:

Információvédelmi biztonsági osztály	Az adott biztonsági osztályra jellemző adattípusok
Nyilvános	• A gazdálkodáshoz kapcsolódó mérlegadatok, amelyek közzétételére kötelezett az Egyetem • Internet közzétett, nyilvánosan szolgáltatott információk, tesztszolgáltatások
Belső	• Belső előterjesztések, jegyzőkönyvek, határozatok, utasítások, amelyek nem kerülnek külön besorolás révén a bizalmas biztonsági osztályba. • Definíció, vagy szabályzat szerinti belső adatok, információk, amelyek a belső üzleti célokra használhatók fel. • Nyilvános munkaanyagok, amelyek nem kerülnek külön besorolás révén a bizalmas biztonsági osztályba.
Bizalmas	• A PPKE normál üzleti tevékenységével kapcsolatos szerződés – és ügyféladatok. • Definíció, vagy szabályzat szerint üzleti titoknak nyilvánuló információ. • Az Informatikai infrastruktúrával kapcsolatos végleges, a pillanatnyi működést dokumentáló információk.

	• Olyan adatok, amelyek a nyilvánosságra kerülése hátrányosan befolyásolja a PPKE üzleti érdekeit.
Szigorúan Bizalmas	• Azonosító és hitelesítő adatok, információk (azon információk köre, amelyek kapcsolattartás során a jogi és anyagi kötelezettség elismeréséhez szükséges formai kellékeknek, azonosító és hitelesítő adatnak minősülnek). • Olyan adatok, amelyek nyilvánosságra kerülése különösen hátrányosan befolyásolja a PPKE üzleti érdekeit.

Azon adatok, amelyek egyértelműen máshova nem kerültek besorolásra a „Belső" kategóriába tartoznak.

A fenti besorolást kell alkalmazni az adatok mind elektronikus, mind nyomtatot formában történő megjelenése esetén.

3.3.1. Védelmi intézkedések a biztonsági célkitűzések alapján

A PPKE területén bevezetett védelmi biztonsági intézkedések csökkentik a PPKE működése során fellépő károk bekövetkezésének valószínűségét. A védelmi intézkedések kötelező jellegűek a PPKE munkavállalóira / hallgatóira nézve. A védelmi intézkedésektől eltérni csak egyedi esetben, a Rektor jóváhagyásával lehet. Az IBSZ-ben, illetve az információbiztonság területre vonatkozó jogszabályokban és egyéb utasításokban, intézkedésekben foglaltak betartásáért az Informatikai osztály vezető (ITO) felelős. Az ide vonatkozó erőforrások biztosítása a Rektor feladata.

3.4. Az adathordozók biztonságos kezelése

Az adathordozók biztonságos kezelésének kialakításával megakadályozható a PPKE magasabb szintű adatbiztonsági szintekbe besorolt adatainak illetéktelen kézbe való kerülése.

A PPKE tulajdonába lévő, a magasabb szintű adatbiztonsági szintekbe besorolt adatok tárolására használt adathordozókat, amennyiben az a kockázati értékelésen egy előzetesen meghatározott értéket elér, azt egyedi azonosítóval kell ellátni, nyilvántartást kell vezetni róla. Az adathordozóra tett címkén, az adattal dolgozó alkalmazottaknak fel kell tüntetnie az adott tartalomra vonatkozó bizalmassági kategóriákat. Kezelését ennek megfelelően kell megvalósítani.

3.4.1. Az adathordozók tárolására vonatkozó elvek

- Figyelembe kell venni a gyártó által meghatározott tárolási környezetre vonatkozó paramétereket, a tároló helynek tűzbiztos, elektromágneses hatásoktól védett helynek kell lennie,
- az adatbiztonsági kategóriákba besorolt adatokat tartalmazó adathordozók tárolásánál figyelembe kell venni a szabályzat adatok kezelésével kapcsolatos előírásaiban megfogalmazottakat.
- Két példányban való tárolás esetében a tároló helyet úgy kell kiválasztani, hogy szükség esetén az arra jogosult akadálytalanul és viszonylag gyorsan hozzáférhessen, de célszerűen, viszonylag távol. Ezzel megakadályozva mindkét példány egyidejű megsemmisülését természeti katasztrófa esetén.

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

4. Fizikai védelem és a környezet védelme

4.1. Területek védelme, biztosítása

A PPKE székhelyének, és egyéb telephelyeinek helyt adó irodákba és raktárba történő bejutás és benn tartózkodás rendjét a PPKE-n működő beléptető rendszer, valamint belépési igazolványok használatára vonatkozó szabályokról szóló utasítások határozzák meg.

4.2. Fizikai biztonsági határzóna

Azokon a területeken, ahol információkat vagy információkat-feldolgozó eszközök koncentráltan vannak jelen, biztonsági határzónát kell kijelölni, amelyet a belépés kontrollját megvalósító biztonsági megoldással kell védeni.

A fizikai biztonsági határzóna egyrészt a PPKE által elfoglalt irodai és raktár területének a határa, másrészt külön biztonsági határzónát képez a fokozottan védett kategóriába tartozó helyiségek határa. A kijelölt peremsáv határait lehetőség szerint fizikailag le kell zárni.

Az informatikai helyiségekbe való belépésre csak abban az esetben adható felhatalmazás, ha az adott személyenek arra:

- munkaköri kötelességének, feladatinak ellátásához,
- külső személy esetén a PPKE szembeni szerződéses kötelezettség teljesítéshez szüksége van (Ebben az esteben csak a helyiségbe belépésre felhatalmazott munkavállaló kíséretével léphet be ezekre a területekre).

Az informatikai helyiségekbe való belépés – az első bekezdésben foglaltak alkalmazása – mellett állandó jelleggel csak az IT terület munkavállalói, az Üzemeltetési Osztály kijelölt munkatársai, az Informatikai Osztály vezető valamint az IBF számára engedélyezhető. Az engedély kiadása, nyilvántartása, felülvizsgálata a Gazdasági Főigazgató – mint Adatgazda – feladata.

A szerverszobáról, mint kiemelten védendő területről jelen szabályzat külön fejezete rendelkezik.

Kiszervezett szolgáltatások esetén azon géptermekbe, ahol a PPKE szerverei vannak a kiszervezett szolgáltató vezetője engedélyezheti a belépést, de a kontrollnak működnie kell, amint az IBF ellenőriz.

4.3. A szerverszoba kialakításának követelményei

A szerverszoba elhelyezésének szempontjai:

- A belmagasságot is figyelembe véve biztosítsa az egyes szerverek, vagy egyéb aktív eszközök számára szükséges levegő térfogatot.
- A helyiség aljzatának megfelelő statikai terhelhetősége az elhelyezett eszközök tömegét, és fizikai méretét figyelembe véve.
- A helyiség ajtajának mérete biztosítsa az elhelyezésre kerülő eszközök akadálytalan ki- és beszállítását.
- A helyiségekhez vezető folyósok, lépcsők, liftek alkalmasak legyenek az elhelyezésre kerülő eszközök ki-, és beszállítására.
- A helyiség határoló falai és nyílászárói alkalmasak legyenek a fizikai betörések megakadályozására.
- A helyiség elhelyezését úgy kell megtervezni, hogy a felette elhelyezkedő helyiségekben ne legyen vizes blokk (mosdó, WC, konyha, stb.). Ellenkező esetben a födém vízzárásának kialakítása szükséges.
- Ha a szerverszoba szintjén vízkár veszélye forog fenn (árvíz, belvíz, csőtörés, stb.), akkor az alábbi védőmechanizmusok bevezetése szükséges:
    - Álpadlózat kialakítása, a berendezések mennyezetről történő elektromos betáplálása
    - Falak, nyílászárók vízbehatolás elleni védelme.
    - Védőtálcák, dobogók alkalmazása a berendezések elhelyezésére.

A szerverszoba behatolás védelme:

- A szobába történő be, és lehetőség szerint a kilépést is naplózó beléptető rendszer kialakítása.
- Automatikusan záródó bejárati ajtó, mely belülről kézzel nyitható (a menekülés biztosítása érdekében).
- Riasztó rendszer alkalmazása.
- Lehetőség szerint kamerás megfigyelés kiépítése.

A szerverszoba tűzvédelme:

- A tűz-, vagy füstriasztó rendszer alkalmazása.
- Aspirációs füstérzékelővel ellátott automatikus tűzoltó rendszer.
- Kézi tűzoltó-berendezések elhelyezése a bejárat közvetlen közelében.

A szerverszoba áramellátása:

A szerverszoba, illetve a szerverteremen kívüli zárt rack-szekrényben elhelyezett hálózati aktív eszközök áramellátásának biztosítása az alábbi szempontok szerint végrehajtani:

- A teljes épület villámvédelmének biztosítása.
- A szerverszobának a többi irodai elektromos hálózattól független betáplálásnak biztosítása.
- A szerverszobában illetve az azon kívül zárt rack-szekrényben üzemeltett eszközök túlfeszültség elleni biztosítása.
- Az elektromos kapcsoló és biztosíték szekrény biztonságos helyen való elhelyezése (lehetőleg benn a szerverszobában). Az elektromos főkapcsolók legyenek védve illetéktelen működtetés ellen.
- Az eszközök szünetmentes tápellátása (Központi UPS vagy helyi UPS-ek).
- A helyiség elektromos betáplálásának terhelés elosztása fázisonként.
- Az UPS-ek betáplálásának elosztása fázisonként.

- A szerverszobában illetve az azon kívül zárt rack-szekrényben elhelyezett eszközök részére minimálisan 20 perc tartási időre méretezett UPS-t kell alkalmazni.
- Az UPS-ek akkumulátorait legalább évente egyszer (pl. a tervszerű megelőző karbantartás alkalmával) tesztelni kell és szükség esetén gondoskodni kell azok haladéktalan cseréjéről).
- Érintésvédelem kialakítása, rendszeres felülvizsgálata.

A szerverszoba klimatizálása:

A szerverszobába üzemi hőmérsékletének szabályozásának érdekében az alábbi szempontok figyelembe vétele szükséges:

- A szerverszobában klíma-berendezéseket kell üzemeltetni, a megfelelő üzemi hőmérséklet szabályozására.
- A klímarendszer kialakítása független legyen az épület egyéb klíma rendszereitől.
- A klíma berendezések darabszámát, és teljesítményét úgy kell tervezni, hogy a szerverszobában nem csak a jelenleg elhelyezett eszközök, hanem a jövőbeli, maximális kihasználtság esetén is (az eszközök hődisszipációs mutatóit figyelembe véve), még egy klímaberendezés meghibásodása esetén is biztosítani tudják a megfelelő szabályozást.
- A klíma-berendezések automatikus újraindítását biztosítani kell az esetleges áramszünet megszűnése esetén.

Vezetett és sugárzott zavarvédelem:

A szerverszoba zavarálló képességének biztosítására az alábbiakat kell megfontolni: gépészeti eszközök (víz-, gáz-, fűtés vezetékek, stb.) eltávolítása javasolt. Ellenőrizni kell az épület villámvédelmi eszközeit, hogy villámcsapás esetén az általuk okozott elektrosztatikus zavar ne veszélyeztesse a szerverszobában üzemelő eszközöket.

A szerverszoba nyitásának, és zárásának szabályai:

A szerver termet folyamatosan zárva kell tartani még akkor is, amikor a helyiségben éppen munkavégzés folyik. Amennyiben a fenti követelmény valamilyen ok miatt nem követhető (pl.: meghibásodás, vagy beszállítás) a szerverszoba bejáratának felügyeletét meg kell oldani.

A szerverszobába történő belépés, kilépés rendje:

Kerülni kell a szerverszobába az indokolatlan belépést. Azokat az üzemeltetési feladatokat, amelyek távoli eléréssel elvégezhetők, távoli menedzsment alkalmazásával kell elvégezni. A szerverszobába csak az arra felhatalmazott személyek léphetnek be. A belépésre engedélyezettek köre jelen szabályzatban került meghatározásra. A szerverszobába történő belépéseket naplózni kell. A naplóállomány tartalmazza:

- a belépő nevét,
- a belépés célját,
- a belépés idejét,
- a kilépés idejét.

A szerverszobába történő munkavégzés rendje:

A szerverszobában csak a folyamatban lévő munkavégzéshez szükséges eszközöket, szerszámokat szabad tartani. A helyiségben tartózkodás ideje alatt az elrendelt munkavégzéstől eltérő tevékenységet folytatni (evés, ivás, stb.) tilos. A szerverszoba más irányú hasznosítása (pl. raktározás, stb.) tilos. Ha olyan tevékenységet kell a szerverszobában végezni, amely veszélyeztetheti az egyes eszközök rendelkezésre állását, akkor a feladat végrehajtását az Informatikai Vezetőnek engedélyeznie kell. A területen történő, külső személy bevonásával végzett, tervezett munkavégzésről a munka megkezdése előtt legalább 1 munkanappal, rendkívüli munkavégzésről (sürgős hibaelhárítás) a munka megkezdésével egy időben értesíteni kell az Információbiztonsági Felelőst.

Harmadik fél alkalmazottja a szerverszobában felügyelet nélkül nem végezhet munkát.

Az elvégzett tevékenységet (telepítés, konfigurálás, javítás, karbantartás, stb.) minden esetben dokumentálni kell.

A dokumentáció tartalmazza:

- A feladatot végző személy(ek) nevét
- A tevékenység leírását
- A tevékenység időtartamát

A dokumentáció lehet azonos a szerverszoba belépési naplóval.

4.4. Berendezések védelme

4.4.1. Berendezések elhelyezése és védelme

A berendezéseket úgy kell elhelyezni, illetve védeni, hogy kockázati besorolásuknak megfelelő mértékű legyen a környezeti fenyegetésekből és veszélyekből eredő kockázat, valamint a jogosulatlan hozzáférés lehetősége. A PPKE adatvagyonának biztonsági osztályokba sorolása alapján az 1. és a 2. szintbe sorolt hálózati aktív eszközök esetében az alábbi rendelkezéseket kell betartani:

- Az 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.
- Felhasználóknak tilos a munkaállomás hardver konfigurációját megváltoztatni, a hardver eszköz belsejébe bármilyen okból belenyúlni, burkolatukat megbontani. A csatlakozó külső perifériák csatlakozását megszüntetni.
- A felhasználók az informatikai eszközöket nem mozgathatják át más helyiségekbe, kivéve a hordozható informatikai eszközöket (pl. notebook-okat). Az informatikai eszközök mozgatását csak az IT osztály munkatársai végezhetik a kapcsolódó tárgyi eszköz mozgatási bizonylat kitöltésével. Az eszközök elhelyezésével és mozgatásával kapcsolatos előírások betartását az IBF ellenőrzi.

Szerverek fizikai hozzáférése:

- A PPKE szervereit az erre a célra kialakított szerverszobában kell elhelyezni.

Nyomtatók fizikai hozzáférése:

A PPKE nyomtatóit úgy kell elhelyezni, hogy az azokon kinyomtatott anyagok illetéktelen kezekbe ne kerülhessenek.

Ennek érdekében:

- A megosztott nyomtatókat úgy kell elhelyezni, hogy az állandó felügyelet, vagy a hozzáférés egyedisége és naplózása biztosított legyen. Elszeparált „nyomtatóhelység" használata tilos!
- A megosztott nyomtatókon „Fokozott" (Belső használatra vagy „Bizalmas"), illetve annál magasabb minősítésű információt csak abban az esetben szabad nyomtatni, ha biztosítható, hogy a nyomtatás során kizárható a nyomtatott anyaghoz történő illetéktelen hozzáférés. (pl. PIN kódos nyomtatás).

- Azokat a nyomtatókat, amelyeken „Kiemelt" (Titkos) anyagok nyomtatása történik, névhez kell kötni, és a munkaállomás közvetlen környezetében, ahhoz közvetlen módon csatlakoztatva (soros, párhuzamos vagy USB port) kell elhelyezni.

Harmadik fél, külső szervezet által biztosított eszközök:

- Idegen eszközt csak szerződéses formában, a Gazdasági Főigazgató, vagy az IBF jóváhagyásával lehet a PPKE területén elhelyezni.
- A harmadik féllel kötött szerződésben rögzíteni kell az információbiztonsági szempontokat az elhelyezésre, működtetésre és felügyeletre, illetve az elszállításra vonatkozóan.

4.4.2. Közműszolgáltatások

Azokat az informatikai berendezéseket, melyeket a PPKE által minősítetten Fokozottan és Kiemelten védett területén kerültek elhelyezésre szünetmentes áramforrás alkalmazásával védeni kell az esetleges áramkimaradásoktól. Ezeken a területeken a munkavégzésre használt számítógépek és egyéb berendezések védelmére használt szünetmentes áramforrások áthidalási idejét az adott területi vezetők határozzák meg. Az eszközök elhelyezési környezetét a közműszolgáltatásokkal összefüggő kockázatok figyelembevételével kell kialakítani, vagy megválasztani. Az esetlegesen felmerülő kockázatok felmérése és értékelése az IBF feladata.

4.4.3. Kábelbiztonság

Az adatátvitelt bonyolító, illetve az információszolgáltatásokat támogató elektromos energiaátviteli és távközlési kábelhálózatot védeni kell a károsodástól. Az elektromos hálózati kábeleket a falon belül, amennyiben ez nem lehetséges, úgy csatornában a környezettől elzártan kell vezetni. Törekedni kell arra, hogy az informatikai eszközök a lehető legrövidebb vezetékkel csatlakozzanak a falon vagy az álpadlóban kialakított csatlakozó aljzathoz.

A csatlakoztató kábelek típusát, állapotát (pl. kereszt kábel, szakadt, rossz) egyértelmű azonosítást lehetővé tevő módon kell jelöléssel ellátni, a használhatatlan kábeleket a hulladék gazdálkodás figyelembevételével kell kidobni;

A be- és átkötéseket, az azt végző rendszergazdának minden esetben dokumentálnia kell.

A központi rendezőt a szerverszobában kell elhelyezni. Tovább osztott (adott szinten, vagy iroda területen megvalósított) rendezés esetén zárható, vagy felügyelhető helyiségben, minden esetben zárt rack-szekrényben kell kialakítani.

Az adathálózati végpontokra idegen számítástechnikai eszköz csatlakoztatása külön engedély nélkül tilos.

Az épület villamossági felülvizsgálatát éves gyakorisággal kell elvégezni. Az infrastruktúra kialakításért és az előírások betartásáért az épület üzemeltetője felel.

4.4.4. Hardver eszközök fizikai biztonsága

A hardver eszközök fizikai biztonságának biztosítása érdekében minimálisan az alábbi védelmeket kell kialakítani:

- Tűzvédelem: A tűzvédelmi szabályzatban kell kitérni az egyes biztonsági zónák tűzvédelmi minősítéséről, és tűzvédelmi megoldásairól.
- Villámvédelem: A PPKE épületeit villámvédelemmel kell ellátni, melyek állapotát rendszeresen felül kell vizsgáltatni.
- Túlfeszültség-védelem: Túlfeszültség-védelmet kell telepíteni azoknak az eszközöknek a betáplálásához, amelyek kritikusak a meghibásodás szempontjából (szerverek, aktív eszközök, stb.)
- A fentieken túl biztosítani kell, hogy a hardver eszközök közelében ne folyjon olyan tevékenység, amely veszélyeztetheti az eszköz működőképességét. Tilos az alábbi tevékenységek folytatása:
    - A hardver eszközökön tilos tárolni olyan anyagokat, amelyek veszélyeztethetik a hardver eszközt (virág, élelmiszer, ital, mágneses tárgyak, stb.)

- Tilos a hardver eszközök közvetlen környezetében étkezni, és bármilyen italt fogyasztani.

4.4.5. Berendezések karbantartása

Gondoskodni kell az informatikai eszközpark minden elemének célszerű, folyamatos karbantartásáról (hardver és szoftver eszközök esetében egyaránt) a gazdasági racionalitás és a pénzügyi tervek keretein belül. Az 1. Biztonsági szintbe sorolt eszközök megelőző védelmi intézkedéseire vonatkozóan a Karbantartási szerződésekben foglaltak a mérvadóak.

A PPKE fő üzleti folyamatait támogató kiszolgálók (1. szint) védelmét redundáns kialakítással kell biztosítani. Az informatikai berendezések rendszeres karbantartásáért a Szerverüzemeltető/Hálózat mérnök felel.

4.4.6. Berendezések biztonsága a telephelyein kívül

Az informatikai eszköz(ök) az Egyetem által bérelt / vagy saját irodai területen kívüli használatát, a felhasználó személyére való tekintet nélkül a Gazdasági Főigazgató rendeli el. Az alábbi előírások betartása kötelező:

- A felhasználó kérelmezhet személyes használatra hordozható számítógépet. Ha kérvényét az Informatikai Vezető elfogadja, a kiadott hordozható számítógépet a PPKE irodaterületéről kiviheti (hazaviheti).
- Az asztali PC-k és egyéb informatikai eszközök PPKE történő elvitele minden felhasználó számára szigorúan tilos.
- Az eszköz vagy adathordozó soha nem maradhat felügyelet nélkül nyilvános helyen, a hordozható számítógépeket kézipoggyászként kell kezelni és utazás közben a táskában kell tartani, biztosítani kell az illetéktelen hozzáférés megakadályozását.
- A gyártó előírásait mindig be kell tartani az eszköz védelme érdekében.
- A kivitt eszközért a kiszállítót teljes anyagi és erkölcsi felelősség terheli.

- A ki- és beszállításokat minden esetben dokumentálni kell szállítólevél alkalmazásával, amelyen az adott informatikai eszköz egyedi azonosítóját fel kell tüntetni (típus, gyári szám, leltári szám), illetve nagy mennyiség esetén csatolt mellékletben kell felsorolni az egyedi azonosító adatait.
- A szállítólevelet a kiinduló és a fogadó helyen a szállítást engedélyező és a szállítmányt fogadó személynek kézjegyével ellen kell jegyeznie, ezáltal nyomon követhetővé válik az eszköz útja.
- Az engedély alapján kiadott hordozható számítógépnek a leltárban is meg kell jelennie, azt leltározási időszakban be kell mutatni.

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

4.4.7. Berendezések biztonságos selejtezése, illetve újra felhasználása

Valamennyi olyan berendezést, amely tárolóeszközt (merevlemez, SSD tároló) 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 Szerverüzemeltető/Hálózat mérnök feladata, aki egy munkalappal igazolja az IBF felé az adathordozó állapotát. A selejtezést évenként kell elvégezni. A selejtezéseknek a főkönyvi rendszerrel megfeleltetve kell történnie.

A használatból kivont információ-feldolgozó eszközöket egy hónapig raktározni kell az esetleges visszaállítás érdekében, feliratozva, illetéktelen hozzáféréstől védve – annak érdekében, hogy a fontos információk ne semmisüljenek meg és minősített információk ne szivárogjanak ki.

Adathordozók megsemmisítését vagy újra felhasználását kizárólag az Adatgazda kezdeményezheti. Az adathordozókra vonatkozó előírásokat jelen szabályzat Az adathordozók biztonságos kezelése pontja tartalmazza.

Az adathordozó, adattároló felülírását, újra hasznosítását (és az ehhez kapcsolódó műveleteket) csak az Informatikai terület munkatársa (Szerverüzemeltető/Hálózat mérnök) végezheti el.

Az eszközökben található adathordozókról az adatokat újra felhasználás, értékesítés előtt visszaállíthatatlan módszerrel törölni kell, akkor is, ha az nem tartalmaz minősített adatokat.

A bontásra, megsemmisítésre átadott gépek esetében is visszaállíthatatlan módszerrel törölni kell az adatokat. A megsemmisítést végzők és a Társaság közti szerződésben kell külön rögzíteni a titoktartási feltételeket, illetve a szerződőnek garanciát kell vállalni az adatok visszaállíthatatlan megsemmisítésére, teljes és feltétlen titoktartásra is.

Az elszállítást dokumentálni kell szállítólevél alkalmazásával, illetve selejtezéskor – mivel az elektronikus eszközök és berendezések veszélyes hulladéknak minősülnek – a környezetvédelmi törvénynek és előírásoknak megfelelően dokumentáltan, az erre jogosítvánnyal rendelkező céggel kell elszállíttatni.

A szállítólevél kiállításának feltétele a kiegyenlített számla, vagy a selejtezési jegyzőkönyv.

A leselejtezett informatikai eszközöket a PPKE a munkavállalók tulajdonába adhatja.

A Gazdasági Főigazgató és az Információbiztonsági Felelős köteles megbizonyosodni arról, hogy külső vállalkozó által használt törlési eljárás, valamint a vállalkozó belső ügyviteli folyamatai garantálják az adatok bizalmas kezelését és teljes megsemmisülését.

Visszaállíthatatlan törlés:

- A visszaállíthatatlan törlés a szoftveres úton történő törlés esetében, ugyanazon adathordozó minimálisan 5-szörös felülírását jelenti, adatot nem tartalmazó, véletlen mintákkal.
- Működésképtelen vagy törölhetetlen eszköz esetében, fizikai törlést kell alkalmazni, az erre alkalmas eszközzel (pl. optikai lemez – CD daráló, merevlemez – szétszerelés, lemezek eltörése).

4.4.8. Vagyontárgyak eltávolítása

Az adattároló médiák, az információ és más értékek fokozott fenyegetettségnek vannak kitéve szállítás közben, ezért alábbi kontrollok megfelelő alkalmazásával kell gondoskodni biztonságukról, ennek érdekében:

- a szállítást csak a PPKE ezzel a feladattal megbízott munkavállalója vagy erre a feladatra szerződött vállalkozó végezheti,
- a szállítandó eszközöket megfelelő csomagolással kell ellátni a fizikai károsodások megelőzése érdekében,
- az érzékeny, bizalmas információk szállítása esetén egyéb speciális kontrollokat is alkalmazni kell, mint:
    - zárható tároló doboz, vagy hordozótáska alkalmazása,
    - olyan csomagolás alkalmazása, mely felbontás után nem zárható vissza az eredeti formában, így az esetleges illetéktelen hozzáférés felderíthető.

Amennyiben a vagyontárgyat (például szervízelésre kijelölt nyomtató, számítógép) külső személy szállít el, meg kell bizonyosodni arról, hogy a szállítást végző személy valóban a szerződött külső partnerhez tartozik, illetve a vagyontárgyat hiánytalanul átvette (pl.: felkerül a teherautóra). Az átadás tényét átadás-átvételi nyilatkozattal, vagy szállítólevéllel dokumentálni szükséges.

5. A Kommunikáció és az üzemeltetés irányítása

5.1. ÜZEMELTETÉSI ELJÁRÁSOK ÉS FELŐSSÉGI KÖRÖK

5.1.1. Dokumentált üzemeltetési eljárások

Az üzemeltetési eljárásokat dokumentálni és karban kell tartani, és minden olyan felhasználó számára hozzáférhetővé kell tenni, akiknek arra szükségük van. (pl.: rendszergazdák, adatgazdák). Az üzemeltetési eljárások dokumentálását és karbantartását a PPKE külsős partnereivel végezteti (PL: Neptun, Nexon, SAP). Az eljárások ellenőrzését az IBF-nek eseti rendszerességgel (pl. verzióváltás) kell elvégeznie.

Az „Üzemeltetési eljárásoknak" tartalmaznia kell a következőket:

- előrelátható szolgáltatás kieséseket (pl.: szerver leállás),
- az informatikai erőforrások és üzemeltetők pontos, naprakész összerendelését, és az ezekhez tartozó felelősségi és jogköröket, a hozzárendelésben történő változásokat mind a nyilvántartásban, mind a felelősök munkaköri leírásában követni kell;
- definiálni kell azokat a katasztrófa helyzeteket, amelyekre a különleges védelmi intézkedéseket kell foganatosítani.

5.1.2. Változáskezelés

Az információ-feldolgozó eszközök és rendszerek változtatásaira vonatkozóan az alábbi előírásokat szükséges betartani:

- Az éles rendszerhez történő illesztés előtt a változó komponenseket minden esetben tesztelés alá kell vetni.
- A tesztelések eredményét dokumentálni kell.
- A változáskezelési folyamat koordinálását a szerver üzemeltetőnek kell ellátni.

5.1.3. 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.

5.1.4. Fejlesztői- és üzemeltetői hozzáférések különválasztása

A fejlesztői szerepkör és az üzemeltetői szerepkör egymással összeférhetetlen, így ezekkel csak másmás munkavállaló rendelkezhet.

A tesztkörnyezetet az éles üzemű környezettől el kell választani. A különválasztás virtuális környezetek létrehozásával is megvalósítható.

5.2. Harmadik felek szolgáltatásnyújtásának irányítása

5.2.1. Szolgáltatásnyújtás

A PPKE informatikai rendszerét támogató mindenkori cégre, valamint más, eseti tevékenységgel megbízott informatikai cégekre vonatkozó szolgáltatásnyújtással kapcsolatos szabályok:

- A külső támogatást biztosító cég általánosan a hardverrel és az operációs rendszerrel, az üzleti alkalmazásokkal, adatbázismotorokkal, valamint a hálózati kommunikáció lehetőségének biztosításával kapcsolatosan felmerülő kérdésekben jogosult a probléma megismerésére és megoldási javaslat benyújtására. Hatásköre kizárólag a szerződésben rögzítettekre terjed ki.
- A szerződésekben rögzített feltételek megfelelőségéért a PPKE felel.

5.2.2. Külső személyek szolgáltatásainak figyelemmel kisérése és átvilágítása

A külső személyek által nyújtott szolgáltatásokat, jelentéseket és feljegyzéseket rendszeresen figyelemmel kell kísérni, probléma (szerződéstől eltérő szolgáltatási minőség) esetén vizsgálatot kell indítani. Ha a vizsgálat eredménye komoly hiányosságot tárt fel, illetve a probléma továbbra is fennáll, azt jelentés formájában kell eljuttatni az Információbiztonsági Felelősnek.

5.2.3. Külső személyek szolgáltatásaival kapcsolatos változások kezelése

A szolgáltatások nyújtását – beleértve a meglévő információbiztonsági szabályzatok, eljárások és ellenőrző intézkedések fenntartását és fejlesztését – érintő változásokat az érintett működési rendszerek kritikusságára – beleértve a folyamatokat és a kockázatok újraértékelését – kezelni kell.

5.3. Rendszertervezés és elfogadás

5.3.1. Kapacitásmenedzselés

Az IT Osztályvezetőnek kell kidolgoznia a kapacitásmenedzsment folyamatát annak biztosítására, hogy az infrastruktúra rendszer megkívánt teljesítőképessége biztosítva legyen a jövőbeli kapacitásigényeknek megfelelően.

A hardver eszközök előírt rendelkezésre állási követelményeknek való megfelelősége érdekében a kiszolgáló hardver eszközök teljesítményét, és egyéb kapacitását (pl.: tároló kapacitás, memória kapacitás, processzor teljesítmény, nyomtató kapacitás, stb.) rendszeresen monitorozni kell.

A tapasztalatok alapján eszközönként meg kell határozni azokat a teljesítmény és kapacitás korlátokat, amelyek elérése esetén a hardver eszközök fejlesztése szükséges.

A kapacitástervezésnél figyelembe kell venni azokat az időkorlátokat is, amelyek az eszközök fejlesztéséhez szükséges beszerzésekhez szükséges.

Az üzleti terület köteles gondoskodni az üzleti igények várható jövőbeni alakulásának Informatika felé történő jelzéséről (pl. funkció bővülése, adat-, ügyfélszám növekedés).

Folyamatosan adatokat kell gyűjteni az üzemeltetett rendszerekről, a szűk keresztmetszetek időben történő felismerése, illetve a jelentkező bővítési igények megfelelő szintű kiszolgálása miatt. Az adatgyűjtést az adott hardver eszköz üzemeltetéséért felelős Szerverüzemeltető/Hálózat mérnök végzi, a megnevezett rendszeren, rendszereken.

Az adatgyűjtés 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

5.3.2. Rendszerek elfogadása, átvétele

A rendszerek elfogadására és átvételére a dokumentált fejlesztői és felhasználói teszteket követően kerülhet sor. Az erre vonatkozó részletes szabályokat a Változáskezelési Szabályzat tartalmazza.

5.4. Védelem a rosszindulatú és mobil kódok ellen

5.4.1. Rosszindulatú kód elleni intézkedés

Preventív védelem

A PPKE informatikai rendszerében csak az Informatikai Osztály által jóváhagyott külön belső szabályozási dokumentum szerinti konfigurációs leltárba felvett:

- hardverelemeket lehet használni,
- jogtiszta szoftvert lehet telepíteni és/vagy futtatni.

Az Informatikai környezet üzemeltetéséért felelős munkatársaknak és a Rendszergazdának kell gondoskodnia arról, hogy az informatikai eszközökre telepítve legyenek az ismert sebezhetőségeket, hibákat megszüntető aktuális javítócsomagok. A javítócsomagoknak a telepítés előtt a változáskezelési tevékenységekre vonatkozó mindenkori hatályos belső szabályok szerinti tesztelési és jóváhagyási eljáráson kell átesniük.

A vírusfertőzések kockázatainak csökkentése érdekében az Egyetemen meg kell oldani az alkalmazott vírusvédelmi szoftverek folyamatos biztonsági frissítését. A frissítéseket úgy kell ütemezni, hogy egy sérülékenység nyilvánosságra hozatala és a biztonsági frissítése között a lehető legkevesebb idő teljen el. A vírusvédelmi rendszer frissítése a Szerverüzemeltető feladata-(Futtatható) Szoftvert, alkalmazásokat a felhasználók az Internetről nem tölthetnek le, a hálózatról nem futtathatnak, külső adathordozón a PPKE területére nem hozhatnak be és nem

telepíthetnek. Eszköztelepítést (hardver, szoftver) csak az informatikai üzemeltetők végezhetnek az informatikai üzemeltetésre vonatkozó mindenkor hatályos belső szabályok alapján.

A PPKE informatikai hálózatába levélmellékletként érkezett állományokat ellenőrizni kell, hogy nem tartalmaznak-e rosszindulatú kódot. A vírusvédelmi rendszernek alkalmasnak kell lennie arra, hogy a rosszindulatú kódot hordozó csatolmányt eltávolítsa, karanténba helyezze

Felderítő intézkedések

Folyamatos felderítő intézkedésként a PPKE vírusvédelmi rendszert használ.

A PPKE által alkalmazott vírusvédelmi rendszerrel kapcsolatos rendelkezések:

- Minden munkaállomásra és – gyártó által biztosított szoftver rendelkezésre állása esetén – szerverre vírusellenőrző szoftvert kötelező telepíteni, amelyért a Szerverüzemeltető felel.
- A vírusellenőrző programnak minden újonnan érkezett állománnyal kapcsolatos fájlművelet esetében meg kell vizsgálnia az adathordozó tartalmát, és amennyiben vírust talált, nem engedhet másolást, futtatást a vírusok leirtásának megoldásáig.
- A programnak központilag menedzselhetőnek kell lennie.
- Biztosítani kell a vírusvédelmet ellátó programok, valamint a vírusok adatait tartalmazó állományok rendszeres, gyártó által kibocsátott verziók telepítésével történő mielőbbi (3 munkanapon belüli) frissítését.
- A vírusvédő alkalmazást a levelező rendszerek központi szervereihez is integrálni kell.
- A felhasználók részéről a vírusellenőrző szoftver beállításainak módosítása tilos - ha megoldható ezeket a beállításokat jelszóhoz kell kötni.
- Vírus felbukkanása esetén a szoftver kísérelje meg azt kiirtani, és értesítse a rendszergazdát, de legalább a felhasználót.
- Kárt okozó, rendszerek működését befolyásoló esemény vagy vírusfertőzés esetén a felhasználónak azonnal értesítést kell küldeni a Szerverüzemeltető számára. A beérkezett értesítés alapján a Szerverüzemeltető végzi el a vírus-mentesítést.

- A vírusvédő alkalmazás vírusdefiníciós fájljainak naprakészségét, az automatikus frissítés helyes működését a Szerverüzemeltető biztosítja, és az IBF ellenőrzi.

Az itt nem szabályozott, illetve technikai részleteket a PPKE Vírusvédelmi Szabályzata tartalmazza.

5.5. Biztonsági mentés

5.5.1. Információ biztonsági mentése

A PPKE legfőbb értékét a szervereken/adattárházakon tárolt adatok jelentik. Ezek védelmében meghatározó jelentőségű a biztonsági másolatok készítése. A mentés célja, egyrészt a ritkán használt adatok, illetve a kulcsfontosságú adatok (pl.: előfizetői, számlázási adatbázisok, forgalmi adatok) 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 visszaállíthatóak legyenek. Mentés során mind az egyes rendszerek adatait, mind az operációs rendszer, adatbázisrendszer és szoftverkörnyezet beállításait is tárolni kell. A mentésekkel kapcsolatos feladatok megfelelő végrehajtását az IBF ellenőrzi.

Az adatokat az 1. és 2. szintbe sorolt szervereken kell tárolni. Ezeken a kiszolgálókon található adatállományok mentésénél az alábbi rendelkezéseket kell betartani:

- A mentéseket naponta, központi mentőszoftverrel kell végrehajtani.
- A mentésből a rendszereket futtató és/vagy adatokat tároló szerver operációs rendszerének és beállításainak, az adatbázisrendszernek és beállításainak, a szoftverkörnyezet beállításainak és a tárolt adatoknak teljeskörűen visszaállíthatónak kell lennie a mentés időpontjában.
- Az 1. szintű szerverek esetében az adatokat legalább két példányban kell menteni, és egymástól földrajzilag elkülönítve, elzárt, a szerverteremtől elkülönülő térben, tűzbiztos helyen kell tárolni.

- A 2. szintű szerverek esetében az adatokat elég egy példányban menteni, és elzárt, a szerverteremtől elkülönülő térben, tűzbiztos helyen kell tárolni.
- A 3. szintű szerverek, továbbá a felhasználói munkaállomások, notebook számítógépek merevlemezei az adatállományok ideiglenes tárolására szolgálnak, nem kerülnek mentésre. A munkatársak felelőssége az általuk létrehozott fájlok szerverre való felmásolása.

A speciális funkciót betöltő szerverek, valamint a hálózati aktív eszközök esetén, amelyeken az adattartalmat a naplóállományok és a rendszer beállításai jelentik, az alábbi utasításokat kell figyelembe venni:

- A szerver mentését legalább hetente, illetve a hálózati aktív eszközökét a beállítás változtatásakor kell elvégezni, amelyért a Szerverüzemeltető/Hálózat mérnök felel.
- A mentés során vagy a meglévő (a szerver szempontjából belső) eszköztár segítségével kell dolgozni, vagy hivatalos, az adott hardver-, szoftverplatform felé támogatással rendelkező cégtől vásárolt mentő-szoftvert kell alkalmazni.

A mentésnek a napló-állományokat és ezeken kívül az összes olyan állományt is tartalmaznia kell, amelyek segítségével a szerver mentéskori állapota teljes mértékben visszaállítható. Ezek a konfigurációs állományok szerverenként különbözőek lehetnek. A mentett adatokhoz csak az arra jogosult rendszergazdák férhetnek hozzá. A mentések elkészítéséért és az esetleges visszaállításokért felelősöknek a munkavégzésükhöz szükséges megfelelő jogokkal kell rendelkezniük.

A 2. szintű munkaállomások esetében az alábbi rendelkezéseket kell betartani:

- A felhasználó a napi munkája során keletkezett dokumentumokat csak meghatározott hálózati könyvtárban (saját használatra kialakított „home" könyvtár), könyvtárakban (szervezeti egységek vagy meghatározott csoportok használatára kialakított „közös" könyvtárakban) tárolhatja, vagy olyan technikai megoldást kell alkalmazni, amely biztosítja, hogy a munkaállomáson lokálisan keletkezett dokumentumok másolati példánya a mentési körbe bevont szerveren rendelkezésre álljon.

- Az operációs rendszerről nem szükséges másolatot készíteni.
- Amennyiben a gép kivehető merevlemezzel rendelkezik, a felhasználó feladata, hogy munkaidő végén, a gép kikapcsolása után a kivehető merevlemezt egy zárható, biztonságos helyen eltárolja, és reggel a számítógép indítása előtt onnan a gépbe visszahelyezze. A fenti műveletre akkor van szükség, ha a helyiség, amelyikben a munkaállomás található, nem zárható.

A hálózatba kötött 3. szintű munkaállomásokon tárolt adatok megőrzésének és biztosításának érdekében az alábbi rendelkezéseket kell betartani:

- Semmilyen, az ügyvitel szempontjából fontos, minősített, pénzügy (bank-) vagy üzleti titkot, adatot tartalmazó, nem nyilvános fájlt sem szabad az adott munkaállomáson tárolni, valamint a fájlok, dokumentumok mentését mindig hálózati könyvtárba kell elvégezni.

A hordozható (laptop, notebook, palmtop stb.) számítógépeken tárolt adatok megőrzésének és biztosításának érdekében az alábbi rendelkezést kell betartani:

- Hálózat nélküli kapcsolat esetében a munkához szükséges adatok mentéséről a notebookot használó munkavállaló gondoskodik. A mentést titkosított formában, hordozható adathordozóra (pen drive) kell időszakosan elvégezni. A hordozható számítógépekről központi mentés nem készül.

A PPKE rendelkezik Mentési Szabályzattal, amelyben az Adatgazdáknak meg kell határoznia:

- a mentésre kerülő adatokat és feldolgozásukhoz szükséges alkalmazásokat,
- a mentés formátumát, és a mentési adathordozót,
- a mentésre használt eszköz(öket),
- a mentések gyakoriságát. típusát (teljes, inkrementális),
- mentések példányszámát,
- mentések időpontjait,
- mentések megőrzési idejét.

A mentési, archiválási, illetve visszatöltési rendszernek biztosítania kell az adatok adatosztályozási szintjének megfelelő rendelkezésre állási követelményeknek való megfelelést.

Az egyes mentési stratégiákat megvalósító mentési eljárásokra vonatkozó szabályokat a PPKE Mentési Szabályzata tartalmazza.

5.6. Hálózatbiztonság kezelése

5.6.1. 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 PPKE számára bizalmas hálózati kapcsolatnak számít a PPKE központjának belső hálózata, minden egyéb hálózat nem bizalmas hálózatnak számít, olyannak, amelyről azt kell feltételezni, hogy veszélyt jelent a PPKE biztonsága számára.

- A bizalmas és a nem bizalmas hálózatokat (pl.: Internet) csak határvédelmi megoldáson (tűzfal) keresztül lehet összekapcsolni.
- A tűzfalak konfigurációja során gondoskodni kell arról, hogy csak az engedélyezett kapcsolati lehetőségek legyenek elérhetők.
- A tűzfalakra vonatkozó intézkedéseket az informatikai rendszer üzemeltetéssel megbízott szolgáltató működteti és szabályozza:
    - a tűzfalak konfigurálásának, ellenőrzésének mikéntjét;
    - 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 használata engedélyezett,
- milyen erőforrásokhoz, célpontokhoz lehet hozzáférni,
- a felhasználókat kell-e (és, ha igen, milyen módon) azonosítani,
- milyen információkat kell naplózni.

A tűzfal üzemeltetésére vonatkozó eljárások a tűzfal konfigurációs beállításai kiemelt üzleti titkot képeznek. A belső hálózatot tűzfalaknak kell védenie, amelyekre a következő előírások vonatkoznak:

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

A tűzfalak fizikai elhelyezésére, mentésére a szerverekre vonatkozó szabályok érvényesek. A tűzfalmegoldás olyan hardver platformon és operációs rendszeren fusson, amelyről az üzemeltetéssel megbízott személyzet magas szintű szakmai tudással rendelkezik, és szakképzett módon tud kezelni. A tűzfalon keletkező napló (log) állományokat a tűzfal üzemeltetőinek rendszeresen ellenőrizniük kell. A betörésre utaló bejegyzéseket írásban jelenteni kell az IBF felé.

A tűzfal adminisztrátorok veszélyhelyzetben vagy ennek gyanúja esetén jogosultak a belső és külső rendszerek közötti kapcsolat megszakítására, majd ezt haladéktalanul jelenteni kell az IBF-nek, és az Informatikai osztályvezetőnek.

5.6.2. Hálózati szolgáltatások biztonsága

A hálózatbiztonsági követelményeknek eleget téve, a PPKE belső irodai hálózatát, és a fejlesztések, tesztelések kiszolgálására használt számítógépes hálózatot szét kell választani. A szegregáció megnehezíti a felhasználók által véletlenül vagy szándékoltan behozott kórokozók éles szerverek elleni támadását, valamint megakadályozza az idegen kézben lévő hálózati csomópontok általi teljes hálózati forgalom lehallgatását, befolyásolását, túlterhelését.

A PPKE informatikai rendszere és az Internet között határvédelmi technikai megoldások biztosítják a biztonság megfelelő szinten tartását. A biztonsági szint fenntartása érdekében az alább felsorolt előírások szükségesek. Az ún. demilitarizált zónákban csak azok az informatikai eszközök (szervereket, védelmi eszközöket, stb.) helyezhetők el, amelyek az Internet felé is nyújtanak szolgáltatásokat.

A PPKE egységes és homogén határvédelmi eszközök alkalmazására törekszik (tűzfal, vírusvédelmi gateway-ek, appliance, stb.). A határvédelmi eszköz felülvizsgálatát évente kell elvégezni és szükség esetén fejlesztéseket kell végrehajtani (cseréje, upgrade-je, újra licencelése, stb.).

Az életcikluson belül a határvédelmi eszközök biztonsági frissítéseit rendszeresen, folyamatosan el kell végezni. A firmware frissítéseket legalább évente szükséges ellenőrizni, illetve végrehajtani. A szignatúra frissítéseket, amennyiben automatikusan beállítható az eszközön, napi rendszerességgel kell ütemezni; amennyiben manuális beavatkozást igényel, hetente kell elvégezni.

Biztosítani kell, hogy a határvédelmi eszközökhöz csak kiemelt felhasználók (erre a célra kijelölt és kiképzett rendszergazdák) férjenek hozzá. A PPKE egységes határvédelmi eszközein minden tevékenységet naplózni kell, a beállításokat minden változtatást követően menteni szükséges.

Az egységes határvédelmi eszközöket rendszeresen monitorozni kell. A monitorozás eredményét minden esetben vissza kell csatolni, ha szükséges fejlesztést, vagy szabályozást kell végrehajtani, bevezetni. Az egységes és homogén határvédelem dokumentációját úgy kell tárolni, hogy az indokolatlan hozzáférés, illetve az illetéktelen kezekbe jutásuk elkerülhető legyen.

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

- I. és II. csoportba tartozó egyéb informatikai eszközök

A fenti eszközök típusát, hálózati nevét, IP címét, valamint fizikai helyét is fel kell tűntetni, vagy a nyilvántartásukra való hivatkozást kell elhelyezni. A III. csoportba tartozó munkaállomásokat és egyéb informatikai eszközöket nem szükséges az ábrába beilleszteni, de mindenképpen folyamatosan vezetni kell, merre találhatóak, és kik férhetnek hozzá.

A dokumentumot a Hálózat mérnöknek kell karbantartania. A határvédelemmel kapcsolatos feladatok ellátásáért a Hálózat mérnök felel.

A PPKE számítógép-hálózata és külső hálózatok közötti kapcsolat során csak az engedélyezett protokollok továbbíthatók, minden egyéb protokoll továbbítása tilos.

A PPKE számítógép-hálózatában alkalmazható külső kommunikációs protokollok köréről – a határvédelmi Hálózat mérnök javaslatára, az üzemeltetés és az IBF véleményének figyelembe vételével – a ITO dönt.

A nem használt, és a felülvizsgáltok során feleslegesnek ítélt, vagy nem engedélyezett hálózati szolgáltatásokat, protokollokat le kell tiltani!

Az engedélyezett protokollok körének kialakításakor külön kell kezelni:

- a felhasználók és az üzemeltetők, illetve
- az átviteli közeg szinten és az állomás szinten engedélyezett protokollokat.

Hordozható számítógépeket csak a Szerverüzemeltető/Hálózat mérnök által elvégzett ellenőrzés után lehet az Egyetem számítógép-hálózatára kapcsolni.

A PPKE számítógép-hálózatában a felhasználói hitelesítés adatait (felhasználó azonosító, jelszó) titkosítva kell továbbítani.

A PPKE számítógép-hálózata domain alapú rendszer, a jogosultságokat és követelményeket Group Policy-k használatával kell beállítani és kikényszeríteni. Tilos olyan munkaállomást csatlakoztatni a PPKE hálózatra, amely:

- nem bizalmas hálózati kapcsolattal is rendelkezik,

- nem egyetemi tulajdonú.

A Hálózat mérnök naprakész nyilvántartást vezet:

- az engedélyezett protokollokról,
- a hálózati határvédelem informatikai biztonsági architektúra elemeinek beállításairól,
- a titkosítás igénylő adatcsatornákról.

5.7. Adathordozók kezelése

A PPKE hivatalos adatforgalmazásban felhasználásra kerülő adathordozókon történő adatátvitel esetén a következő előírásokat kell betartani.

5.7.1. Az eltávolítható adathordozók kezelése

Csak a PPKE tulajdonában lévő, regisztrált eltávolítható adathordozót lehet használni.

Eltávolítható adathordozón jogszabály által minősített vagy „Bizalmas", illetve „Szigorúan bizalmas" védelmi osztályba besorolt adat, információ csak titkosítva tárolható.

A nagy mennyiségű adat rögzítésére és tárolására képes eszközök és számítógép-perifériák:

- CD (DVD) lemezek írására alkalmas eszközök,
- hordozható merevlemezegységek és más nagykapacitású mobil háttértárolók,
- a számítógéptől függetleníthető memóriák (pl. memória kártyák),
- vagy ilyen funkciójú egyéb eszközök (pl. pendrive) telepítése, használata csak különlegesen indokolt esetben, a felhasználó szervezeti egységének vezetője kezdeményezésére – egyedi engedéllyel az IBF jóváhagyásával lehetséges.

Az eszközhasználatot, a PPKE információ feldolgozó eszközeihez való csatlakoztatása után, minden előzetes értesítés nélkül a PPKE figyelheti, monitorozhatja.

Otthoni munkavégzés és bármilyen más célból bármilyen adatot CD/DVD-n, elektronikus levélben vagy egyéb más módon (pl.: Pendrive) az informatikai infrastruktúrájából kijuttatni csak az Adatgazda írásos engedélyével szabad. Az adatok kivitelét az Adatgazdának kell engedélyeznie, írásos formában.

Az adatkivitelt az IBF ellenőrzi, szúrópróba-szerűen.

A PPKE az adathordozók használatát információbiztonsági megfontolásból utasítással, hardver, illetve szoftver úton korlátozhatja.

A szállítás folyamán az adathordozót sérüléstől védő borítással kell ellátni.

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.

Az adatok szállításának biztonságáról mindig az adattulajdonos intézménynek kell gondoskodnia.

A mentésre, archiválásra és bármilyen szintű elektronikus információ-tárolásra 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 rendszergazdák tesztelik az adatok rendelkezésre állását)
- A felülvizsgálatot jegyzőkönyvezni kell, és amennyiben szükséges, a további rendelkezésre állást biztosítani kell. Az adathordozók kezelésével kapcsolatos előírások betartásáért az IBF felel.

5.7.2. Adathordozók selejtezése

A számítógépes feldolgozás során hibás, vagy feleslegessé vált, aktualitását vesztett mágneses és optikai adathordozókat selejtezés útján kell megsemmisíteni. A selejtezés esetében az alábbi intézkedéseket kell betartani:

- Amennyiben lehetőség van rá, a feleslegessé vált adathordozó (mágneslemez, mágnesszalag, CD, DVD, optikai diszk) megsemmisítését a keletkezés helyén, saját hatáskörben, bizottsági úton kell végrehajtani.
- Amennyiben a feleslegessé vált adathordozó (mágneslemez, mágnesszalag, CD, DVD, optikai diszk, merevlemez/winchester) megsemmisítése a keletkezése helyén nem lehetséges, az adathordozók selejtezéséről az Üzemeltetési Osztály külső cég bevonásával gondoskodik. A munkavállaló köteles a munkája során keletkezett selejtezendő adathordozókat a rendszergazdának eljuttatni.
- A megsemmisítésre kijelölt adathordozók fizikai megsemmisítéséről a PPKE Mentési Szabályzata vonatkozó rendelkezéseiben foglaltaknak megfelelően kell eljárni. Az adathordozókat úgy kell megsemmisíteni, hogy azok tartalmát semmilyen úton illetéktelen ne tudja újra olvasni, felhasználni.

5.7.3. Rendszerdokumentáció védelme

A rendszerdokumentációt a jogosulatlan hozzáféréstől védeni kell. A nyomtatott dokumentumokat elzárva kell tárolni. A feleslegessé váló dokumentumokat iratmegsemmisítővel meg kell semmisíteni, illetve az elektronikus formában tárolt dokumentációkat fizikai törléssel kell törölni, az eltávolítható adathordozón található dokumentációt jelen szabályzat Berendezések biztonságos selejtezése, illetve újra felhasználása pontjában foglaltak szerint kezelni.

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

- a rendszergazdák
- az adatgazdák
- a szakterületi vezetők
- a felhasználók.

A rendszerdokumentációk tárolási folyamatának kialakítása és ellenőrzése az ITO feladata. A rendszerdokumentációk hálózati megosztott mappába történő feltöltéséért és a sértetlenség megőrzéséért az adatgazda felel. A dokumentációk rendelkezésre állásáért a Szerverüzemeltető/Hálózat mérnök tartozik felelősséggel.

5.8. Információcsere

5.8.1. Fizikai adathordozók szállítása

A hordozható számítógépes eszközök (notebook, pendrive, DVD/CD) külső felhasználása során különös gondot kell fordítani az eszközök fizikai és adatvédelmére. A PPKE tulajdonát képező adathordozókat semmilyen esetben sem szabad személyes célra használni. A privát adathordozók munkahelyi használata külön engedélyhez kötött.

Az adatokról másolatok csak a munkafolyamatra vonatkozó előírásokkal összhangban készíthetők. A titokvédelmi szabályok szerint minősített adatokat csak nyilvántartott adathordozóra szabad felvinni. A nyilvántartott adathordozókat külön azonosítóval kell ellátni, ezeknek az azonosítóknak a feldolgozási, felhasználási folyamat végéig egyértelműen azonosíthatóknak kell lenniük és a titokvédelmi előírások szerint kell őket kezelni. Az adathordozók illetéktelen kézbe kerülése elleni védelem minden dolgozó felelőssége.

Abban az esetben, ha az adott területen dolgozók közül bárki észreveszi, hogy illetéktelen személy (idegen személy vagy munkatárs) a hatályos szabályok, utasítások, normatívák szerint számára nem megengedhető adatokat másol, kötelessége felszólítani az illetőt, hogy a tevékenységét hagyja abba, illetve köteles erről a vezetőjét értesíteni.

Az adathordozók érzékenyek a külső fizikai, mágneses behatásokra, ezért tilos azokat meghajtani, törni, mágneses eszközök közelébe vinni (és fordítva!). Óvni kell az adathordozókat bárminemű folyékony anyagtól (italok, virágok öntözésére szolgáló víz, vegyszerek) és fokozottan védeni 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 IBF-et és az ITO-t. Az előírások betartásának ellenőrzése az IBF felelőssége.

5.8.2. Elektronikus üzenetek küldése / fogadása (e-mail)

5.8.2.1. Az elektronikus levelezés biztonsága

Az elektronikus üzenetekben foglalt információkat védelméről gondoskodni kell.

- Védeni kell az üzeneteket a jogosulatlan hozzáféréstől, módosítástól.
- Biztosítani kell a korrekt címzést és célba juttatást.
- Biztosítani kell a szolgáltatás megbízhatóságát és hozzáférhetőségét.
- Elektronikus aláírások használatát biztosítani kell, ahol szükséges.
- Külső nyilvános szolgáltatásokat kontroll alatt kell tartani.
- Az Egyetemen csak azok a munkavállalók használhatják az elektronikus levelezést, akik rendelkeznek az ehhez szükséges jóváhagyással. A jóváhagyás csak az elektronikus levelezésre vonatkozó biztonsági szabályok megismerése után adható meg.

A levelezőrendszer felhasználóival kapcsolatos teendők ellátása az általános felhasználó kezelésen belül történik. A levelező rendszer naplózása biztosítja az elektronikus levélforgalom ellenőrizhetőségét, a naplófájlokat az esetleges problémák felderítés céljából folyamatosan elemezni kell. A PPKE informatikai rendszerét védő tűzfallal szembeni elvárások szabályozásánál rendelkezni kell az egyéb WEB-es, vagy POP3 stb. levelezési lehetőségek eléréséről. A szabályok betartását folyamatosan ellenőrizni kell.

A levelező kliensekkel elért és kezelt e-mailek a levelező szerveren történő tároláson túlmenően, lokálisan, a munkaállomásokon is tárolásra kerülnek. 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 az IBF felel.

5.8.2.2. Belső elektronikus levelezés szabályai

A PPKE 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 PPKE informatikai rendszeréből küldeni, amely a PPKE érdekeivel ellentétes.

Az elektronikus levél a papír alapú levelezéssel esik egy tekintet alá. A PPKE által hivatalosan támogatott levelező rendszeren kívül más, elektronikus levelezést hivatalos kommunikációra, valamint a PPKE munkaállomásait a munkakörhöz nem kapcsolódó feladatra használni tilos. A levelek kezelése és mentése a felhasználó felelőssége a kialakított saját könyvtárába, vagy saját munkaeszközére. A Rektor jogosult a Gazdasági Főigazgató és az IBF javaslatai alapján meghatározni azoknak az információknak a körét, amelyek elektronikus levelezés útján történő forgalmazása korlátozható.

5.8.2.3. Elektronikus levelezés harmadik személlyel

A PPKE személyes adat, üzleti titok nem továbbítható harmadik személy számára elektronikus levélben, kivéve, ha az adatgazda ehhez hozzájárult. Személyes adatok továbbítása esetében az IBF hozzájárulása is szükséges.

Az ITO a Gazdasági Főigazgató utasítására 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.

Az Informatikai osztály korlátozhatja a küldhető fájlok méretét.

Mivel mind az e-mail, mind az internet forgalom a PPKE által biztosított eszközökön történik, és ezen eszközök biztosítása a PPKE folyamatok ellátásával kapcsolatos tevékenység megkönnyítésére irányul. Az elektronikus levél egy tekintet alá esik a PPKE érkező bármely más hivatalos irattal. A Gazdasági Főigazgató utasítására az Informatikai Osztály jogosult a PPKE mail címeken (arról érkezett, vagy oda továbbított) bonyolított levelezést, illetve az interneten látogatott oldalakat, temporális internet fájlokat, letöltéseket a felhasználó gépén, vagy a szerveren ellenőrizni.

Az ellenőrzés kizárólag a munkavállaló munkaviszonyával összefüggésben ellenőrizhető, melyről előzetesen írásban tájékoztatni kell.

Az ellenőrzés során az Egyetem a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt, a munkaviszonnyal összefüggő adatokba tekinthet be, melyről jegyzőkönyvet szükséges készíteni.

Amennyiben a munkavállaló a felek megállapodása alapján a munkaviszony teljesítése érdekében saját számítástechnikai eszközt használ, a fenti rendelkezéseket szükséges alkalmazni.

5.8.3. Nyilvánosan hozzáférhető információ

A nyilvánosan közzétett információk, úgymint a PPKE weboldalán elhelyezett tartalom, jelentős értéket képvisel az ügyfelekkel és a leendő ügyfelekkel való kapcsolat tartás 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 kiszervezési szerződésben. A szerződésben foglaltak betartását időközönkénti audit vizsgálatokkal szükséges ellenőrizni. A rendelkezések betartásáért az IBF felel.

5.9. FIGYELEMMEL KÖVETÉS (MONITORING)

5.9.1. Audit naplózása

A számon kérhetőség és az auditálhatóság biztosítása érdekében olyan naplózási rendszert kell kialakítani, amely biztosítja a PPKE informatikai rendszereiben bekövetkezett fontosabb események utólagos kivizsgálását, különös tekintettel azokra, amelyek a biztonságot érintik. A naplózással kapcsolatos részletes szabályokat a Naplózási Szabályzat tartalmazza. A naplózási funkció működtetéséért az Informatikai Osztály felel. Az előírásoknak való megfelelőséget az IBF feladata ellenőrizni.

5.9.2. Rendszerhasználat figyelése

A felelős Szerverüzemeltető/Hálózat mérnök időközi feladata kiértékelni a naplóállományokat és riportot készíteni róluk. Havi rendszerességgel a Szerverüzemeltető/Hálózat mérnök kiértékeli a jelentéseket egy speciális szempont szerint. A kiértékelésről Jegyzőkönyv készül, amely tartalmazza az egyes intézkedéseket. A felsőbb vezetők felé az eszkalációs utat minden esetben biztosítani szükséges.

5.9.3. Naplóinformációk védelme

A kiszolgálók naplóállományait minden esetben menteni szükséges. Továbbá a naplóállományok védelmének egyezőnek kell lennie a kiszolgálók védelmével.

5.9.4. Órajelek szinkronizálása

A szervezeten belül, illetve adott biztonsági tartományban működő valamennyi érintett információ feldolgozó rendszer órajelét a PPKE központi tartományvezérlőjéhez kell szinkronizálni. A Szerverüzemeltető/Hálózat mérnök felel, hogy a tevékenység zavartalanul működjön. Az IBF feladata ellenőrizni a tevékenység előírás szerinti működését.

6. Hozzáférés – ellenőrzés

6.1. Felhasználói hozzáférés irányítása

6.1.1. Felhasználók regisztrálása

A hozzáférések és jogosultságok menedzselése a PPKE szempontjából kiemelkedően fontos biztonsági feladat.

Az új felhasználókkal kapcsolatos minden, a hozzáférési rendszerrel kapcsolatos kérést, módosítási igényt elektronikusan az ITSM rendszerben kell bejelenteni. Érvénytelen a kérés, ha az űrlap nincs megfelelően kitöltve és a felhasználónak nincs jogosultsága a hozzáférés kérésére! A beérkezett igényléseket az IBF-nek a Jogosultságkezelési Szabályzatban megfogalmazott előírások szerint ellenőriznie kell.

6.1.2. Felhasználói jelszavak kezelése, és ellenőrzése

A jelszavakkal és hozzáférésekkel kapcsolatos szabályozásokat egy egységesen dokumentált Jogosultságkezelési Szabályzatban kell rögzíteni.

6.2. Felhasználói felelősségek

6.2.1. 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 sem ismerheti, még a rendszergazdák sem.

Amennyiben rendszergazdai teendők merülnek fel egy felhasználó gépén, a felhasználónak kötelessége ott tartózkodni, hogy szükség esetén a nevével be tudjon lépni az Informatikai

osztály munkatársa. Ha az Informatikai osztály munkatársa megismerte a felhasználó jelszavát köteles új 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 rendszert úgy kell beállítania, hogy a felhasználó az első bejelentkezésekor azonnal meg kell, hogy változtassa a jelszavát.

A jelszót soron kívül meg kell változtatni, ha az illetéktelen (más) személy tudomására jutott, illetve juthatott, vagy a felhasználó azt 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.

6.2.2. Őrizetlenül hagyott felhasználói berendezések, tiszta képernyő politika

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

6.3. Hálózati szintű hozzáférés ellenőrzés

6.3.1. Hálózati szolgáltatások használatára vonatkozó szabályzat

A határvédelem megfelelő üzemeltetése és működésének biztosítása érdekében a PPKE mind külső mind pedig belső hálózatának rendelkezésre állása és biztonságos működése is elengedhetetlen. A PPKE határvédelmi rendszerének (Tűzfalak, IDS, IPS Vírusvédelem stb.) üzemeltetésével kapcsolatos szabályozását több szabályozásban rögzítette. Ilyenek a

vírusvédelmi szabályzat, a változáskezelési szabályzat és a naplózásra vonatkozó szabályzatok. A határvédelmi rendszer működtetésért a Hálózati mérnök tartozik felelősséggel.

A Hálózat mérnök köteles:

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

6.3.2. Felhasználó hitelesítése külső csatlakozások esetén

A külső hozzáférés minden esetben azonosítás útján kell, hogy történjen. A kommunikációs csatornát titkosítani kell. A tevékenységért a Hálózat mérnök felel. A követelményeknek való megfelelést az IBF ellenőrzi.

6.3.3. Hálózathoz való csatlakozás ellenőrzése

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

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

Hálózati forgalom analizálása, ellenőrzése érdekében a következők megtétele szükséges:

- A rendelkezésre álló eszközök segítségével a PPKE 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 PPKE 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 illetékes Hálózat mérnök felé.

6.4. Operációs rendszer szintű hozzáférés-ellenőrzés

6.4.1. Biztonságos bejelentkezési eljárások

Az operációs rendszerekhez való hozzáférést biztonságos bejelentkezési eljárásokkal kell ellenőrzés alatt tartani. Ezen ellenőrzéseket az IBF-nek kell gyakorolnia. A felhasználói bejelentkezés felhasználónévvel és egyedi jelszóval kell, hogy történjen. 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.

6.4.2. Felhasználó azonosítása és hitelesítése

Minden egyes felhasználónak saját személyes és kizárólagos használatára szóló egyedi azonosítóval (felhasználó ID) kell rendelkeznie, és alkalmas hitelesítési technikát kell választani a felhasználó állítólagos azonosságának igazolására.

6.4.3. Jelszókezelő rendszer

A jelszóhasználatra vonatkozó rendelkezéseket az operációs rendszer beállításaival kell támogatni. Ennek beállítását az adott rendszer Alkalmazás gazdája kell, hogy elvégezze az alábbi minimális kritériumoknak megfeleltethetően:

- A hálózati jelszó legalább 12 karakterből álljon, és kis- és nagybetűk, számok közül legalább kettő típusút tartalmazzon, valamint kizárólag az angol ABC betűit és számokat tartalmazhat.
- Az alkalmazásokhoz tartozó jelszavak legalább 12 karakterből kell, hogy álljanak.
- A jelszó nem lehet azonos a felhasználónévvel, annak becézett formájával, vagy egyéb könnyen visszafejthető kifejezéssel.

- A felhasználók (kivéve a rendszer üzemeltetésével foglalkozó felhasználók) a rendszerekre bejelentkezve csak a munkájukhoz szükséges alkalmazásokat indíthatják el, egyéb utasítást nem adhatnak ki.
- A hálózatba kötött számítógépek esetében a felhasználóknak a hálózati, illetve ennek hiánya esetén helyi bejelentkezési jelszavaikat 730 naponta meg kell változtatniuk.
- Ahol ezt az operációs rendszer támogatja, 5 sikertelen bejelentkezés után az operációs rendszernek le kell tiltani a felhasználó fiókját.
- A 3. szintbe sorolt, helyi hálózatra nem kapcsolódó számítógépek esetében a jelszavakat az eszköz használójának 730 naponta meg kell változtatnia.
- A jelszó megváltoztatásakor az új jelszó nem lehet azonos a „leváltott", megelőzően adott 12 jelszóval.
- Ahol ezt az operációs rendszer támogatja, meg kell oldani a jelszavak hasonlóságának problémáját is, azaz az új jelszónak minimum 2 karakterében különböznie kell az előző, illetve az eddig megadott jelszavaktól.

Az előírások betartását az IBF feladata ellenőrizni.

6.5. Alkalmazás és információ szintű hozzáférés-ellenőrzés

6.5.1. Információ hozzáférési korlátozás

A hozzáférések korlátozására vonatkozó előírások a Jogosultságkezelési Szabályzatban kerültek kialakításra. A jogosultsági csoportokhoz hozzárendelhető szerepkörök kialakítását a szakterületi vezetőknek a felelőssége elvégezni. A tevékenységet a belső ellenőr feladata ellenőrizni.

6.6. Mobil számítógépek használata és távmunka

6.6.1. Mobil számítógép használata

A PPKE által használatba adott hordozható számítógépekkel kapcsolatosan az alábbi a rendelkezést kell betartani: Az eszközökbe épített vezeték nélküli hálózati kapcsolatot a PPKE területén kikapcsolt állapotban, vagy az operációs rendszer számára nem használható állapotban kell tartani abban az esetben, ha a számítógépet a vezetékes hálózatba kötve használják. Ez alól kivételt jelent, ha a PPKE tulajdonában lévő eszközt más módon nem lehet a PPKE hálózatba kötni, és erre mindenképpen szükség van.

Amennyiben a vezeték nélküli csatlakoztatás nem kerülhető el, a kapcsolatot titkosított módon kell létrehozni. A szükséges beállításokat csak a rendszergazdák végezhetik el. A hordozható munkaállomásokat fájlrendszer szinten titkosítani szükséges. Az előírásoknak való megfelelőséget a Rendszergazdának kell biztosítania és ellenőriznie.

6.6.2. Távmunka

Amennyiben a PPKE-n engedélyezve lesz a távmunka lehetősége, ebben az esetben a felhasználóknak külön VPN-es hozzáférésekkel kell hozzáférni a vállalati erőforrásokhoz. Melyen egyedi felhasználónevet és jelszavat kapnak, és előre meghatározott ideig érvényesek. A VPN használatához külön VPN Kliens szükséges, melyet a Informatikai osztály telepít a számítógépekre.

7. Információs rendszerek beszerzése, fejlesztése és fenntartása

Az üzleti folyamatokat támogató alkalmazások fejlesztését belső és külső fejlesztések útján valósítja meg. A PPKE 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 Alkalmazás gazdája, továbbá az üzleti területről delegált Adatgazdája.
- A fejlesztőknek nem lehet jogosultsága az éles alkalmazásokra.
- Ha egy rendszert futtató szerver alap szoftvereiben, hardverkomponenseiben speciális javításokat, módosításokat kell végrehajtani, ezt csak az Adatgazda engedélyével, írásbeli dokumentáltság mellett végzi el a Szerverüzemeltető/Hálózat mérnök.
- Amikor a javítások, módosítások, változások végrehajtásra kerülnek, akkor azokat dokumentálni, éles rendszer esetén jegyzőkönyvezni is kell, amelynek felelősei a Rendszergazdák. A verzióváltások rendjét a Változás-szabályozási eljárások című fejezet 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 Változáskezelési Szabályzat tartalmazza.

7.1. Információs rendszerek biztonsági követelményei

7.1.1. Biztonsági követelmények elemzése és meghatározása

Alapvető biztonsági követelmény, hogy a PPKE informatikai rendszereiben minden esetben készüljön visszaállítási pont. Ezáltal visszaállíthatóvá kell tenni a legutolsó helyes állapotot. Az

információs rendszerekben történő bármilyen változás esetén az üzleti területek munkavégzését minden esetben biztosítani szükséges. Amennyiben szükséges, úgy az üzleti területek bevonásával kell, hogy történjen a rendszerekben történő változások bevezetése. A követelmények betartásáért azt IBF felel.

7.1.2. Helyes információfeldolgozás az alkalmazásokban

Az információfeldolgozási 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 tevékenységet a Belső ellenőr feladata ellenőrizni.

7.2. Titkosítási intézkedések

7.2.1. Titkosítási eljárások használatára vonatkozó szabályzat

Az információk védelme érdekében ki kell alakítani és alkalmazni kell a titkosítási eljárások használatára vonatkozó szabályzatot. A titkosítási intézkedéseket szükséges kiterjeszteni az üzleti rendszerekre és folyamatokra, továbbá a vezetői levelezésre. A titkosítási intézkedések betartásának ellenőrzése a Gazdasági Főigazgató feladata.

7.2.2. Kulcsirányítás

A PPKE külső digitális kulcshitelesítési szolgáltatót kell igénybe vennie, amennyiben a partnerek közötti információ átadás azt, az információ minősítése miatt megköveteli. (pl. tanúsítvány alapú levelezés titkosítás, hitelesség igazolása) A kulcsirányítási folyamat felelőse az ITO.

7.3. Rendszerfájlok biztonsága

7.3.1. Üzemelő szoftverek ellenőrzése

Az engedélyezett szoftverek nyilvántartását a Szoftverleltárban naprakészen kell vezetni. Az eljárásban meg kell fogalmazni a feladat és felelősségi köröket, továbbá az ellenőrzési jogkört. Az ellenőrzések előírás szerinti végrehajtásáért az ITO felel.

7.3.2. 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 ITO felel.

7.3.3. Programok forráskódjához való hozzáférés ellenőrzés

A programok forráskódjához való hozzáférést dokumentálni szükséges, továbbá az azokhoz történő hozzáférés csak az ITO írásos engedélyével lehetséges. Az adathordozókat biztos helyen páncélszekrényben kell tárolni. Az adathordozón egyértelműen fel kell tüntetni az aktuális verzió információkat. Az IBF feladata ellenőrizni az előírások betartását.

7.4. BIZTONSÁG A FEJLESZTÉSI ÉS TÁMOGATÓ FOLYAMATOKBAN

7.4.1. Változás-szabályozási eljárások

A fejlesztés során felmerülő változási igényeket, és az adott megoldásokat minden esetben kötelező írott formában dokumentálni. A változás kezelés hiteles dokumentumait csatolni kell a

fejlesztés teljes dokumentációjához. A fejlesztésekkel kapcsolatos adminisztrációs feladatok a következők:

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

A fejlesztésekkel kapcsolatos előírások betartását az IBF ellenőrzi.

7.4.2. Alkalmazások műszaki átvizsgálása az üzemelő rendszerek megváltoztatását követően

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

A rendszertesztelésekkel kapcsolatos előírások a következők:

- a teszt és az éles környezet elkülönítése
- a fejlesztő éles adatokhoz való hozzáférésének megakadályozása

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

8. INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE

8.1. INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK ÉS GYENGESÉGEK JELENTÉSE

A PPKE minden alkalmazottjának és hallgatóinak, illetve partnerének kötelessége az általa tapasztalt biztonsági eseményt vagy általa feltárt biztonsági sebezhetőséget haladéktalanul jelenteni az IBF-nek. A bejelentés formai követelményeit, kezelésének módját a ITO és DPO határozza meg. A biztonsági események kezelésekor az IBF-nek, mint szakértőnek be kell tartani a jelen IBSz-ben rögzítetteket. Ugyancsak ezen utasítás előírásai szerint kötelessége a bejelentés dokumentálása, valamint a kiértékelés elvégzése és átadása az DPO-nak.

A biztonsági esemény kiértékelését az IBF-nek 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;
- biztonságsértéssel kapcsolatos;
- meg kell határoznia a biztonsági esemény okát;
- meg kell határoznia a javító intézkedést, az előzetesen gyűjtött adatok felhasználásával;
- értesítenie kell az DPO-t és ITO a foganatosított intézkedésekről.
- ha az intézkedés csak a hasonló biztonsági esemény kizárását célozza, akkor jeleznie kell az DPO, ITO és a Rektor 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 információ biztonsági sérüléseket azonosítani, dokumentálni és

- a felülvizsgálatokkal összhangban, a védelmi intézkedésekkel együtt előterjesztést készíteni a vezetői értekezlet elé.

8.2. MŰKÖDÉS FOLYTONOSSÁGÁNAK IRÁNYÍTÁSA

A működés folytonosság menedzselésére vonatkozó előírásokat az „Üzletmenet folytonossági- és katasztrófa elhárítási tervek készítésének keretrendszere" szabályozás tartalmazza.

8.3. Záró rendelkezések

- A Pázmány Péter Katolikus Egyetem Információbiztonsági Szabályzatát (IBSz) az Egyetemi Tanács a 46/2023. (VI.15.) számú határozatával jóváhagyta.
- A jelen szabályzat a kihirdetését követő napon lép hatályba.
- A jelen szabályzat hatályba lépésével egyidejűleg a PPKE Informatikai- és Információbiztonsági Szabályzat[1] hatályát veszti.

Budapest, 2023. június 29.

Dr. Kuminetz Géza György
rektor
Pázmány Péter Katolikus Egyetem

PÁZMÁNY PÉTER KATOLIKUS EGYETEM * REKTOR * BUDAPEST

[1] 8/2019 (IV.12.) sz. ET határozat, hatályos 2019. 04. 16-tól kezdődően.

9. Mellékletek

9.1. Fogalomtár

Az **adatbiztonság** olyan technológiák és szervezési módszerek összessége, amelyek lehetővé teszik az összegyűjtött adatvagyon integritását, használhatóságát és bizalmas jellegét.

Az **adatfeldolgozó** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel. Az adatfeldolgozónak való minősítésnek két alapvető feltétele van: az adatkezelőtől elkülönült szervezet, és az adatkezelő nevében kezeli a személyes adatokat.

Az **adatkezelő** olyan szerv, amely meghatározza az adatkezelés egyes kulcsfontosságú elemeit. Az adatkezelést jogszabály határozhatja meg, illetve az ügy tényállási elemeinek vagy körülményeinek elemzéséből eredhet. Bizonyos adatkezelési tevékenységek úgy tekinthetők, mint amelyek természetes módon kapcsolódnak a szervezet szerepéhez (munkáltató a munkavállalókhoz, a kiadó az előfizetőkhöz vagy az egyesület a tagjaihoz). Sok esetben a szerződési feltételek segíthetnek azonosítani az adatkezelőt, bár azok nem minden körülmények között meghatározóak.

A helyi hálózat (LAN – Local Area Network) olyan számítógépes hálózat, amely egy korlátozott területen, tipikusan egy épületen vagy irodán belül kerül kialakításra.

A LAN kialakításához szükséges a gépekben hálózati csatlakoztató kártyát elhelyezni, szükség van egy központ hálózati kapcsolóra is, illetve a gépeket és a kapcsolókat összekötő kábelekre, vagy éppen egy vezeték nélküli (WiFi) hálózatra.

Az adatátvitel kapcsoló (Switch) egy aktív számítógépes hálózati eszköz, mely a rácsatlakozott eszközök között adatáramlást valósít meg.

Az útválasztó (Router) működik központi kapcsoló eszközként, de lehetővé teszi hálózatok összekapcsolását, akár másik hálózattal vagy az Internettel.

A MAC-cím (Media Access Control) egy hexadecimális számsorozat, amellyel még a gyárban látják el a hálózati kártyákat. A hálózat többi eszköze a MAC-címet használja a hálózat előre meghatározott portjainak azonosítására. Ezek mellett a irányítótáblák és egyéb adatszerkezetek létrehozására és frissítésére is alkalmas.

Ethernet: A hálózati kommunikációs szabályok összefoglaló szabványa, szabályozza a hálózati kártyák (NIC) és a központi kapcsolók (Switch) közötti adat átvitel módját. Minden hálózati kártyának és kapcsolónak azonos, ideértve kompatibilis Ethernet "nyelvet" kell beszélni a sikeres kommunikációhoz.

IP cím (IPv4 = Internet Protocol version 4): Minden számítógép és egyéb eszközök is rendelkeznek hálózati azonosítóval. Az IP cím lehetővé teszi minden számítógép számára, rendezett és hatékony módon tudjon adatokat küldeni és fogadni. Az IP cím azonosítja a számítógépet a hálózaton és magát a hálózatot is, ahol a számítógép megtalálható.

Privát IP (Private IP): Az ilyen címekkel rendelkező számítógépek nem kommunikálhatnak más hálózatok gépeivel. Ezek a számítógépek rendszerint egy tűzfal (Firewall) vagy Proxy mögött helyezkednek el.

Publikus IP (Public IP): Az ilyen publikus címeket használjuk az Internetes kommunikációra. Minden publikus IP címmel rendelkező számítógéppel kommunikálhatnak.

IPSec (Internet Protocol Security): Az IPSec (Internet Protocol Security) a biztonsági protokoll a TCP/IP-n belül, amely hitelesítést és titkosítást tesz lehetővé. Az IPSec protokollt virtuális magánhálózatok (VPN – Virtual Private Network) részeként használjuk, illetve szerves részét képezi az IPv6-os protokollnak.

ARP – címfeloldási protokoll (Address Resolution Protocol): A hoszt vagy a router IP címének leképezése MAC (Media Access Control) címmé.

Kábeles LAN (Wired LAN): A számítógépek és egyéb eszközök (Router, Switch, Firewall, stb.) réz sodort érpárral (kábel) kapcsolódnak össze.

Vezeték nélküli LAN (Wireless LAN – WLAN): A vezeték nélküli helyi hálózatnak (WLAN) számos előnye van, amelyekből a legnyilvánvalóbb és legkényelmesebb a szabad helyváltoztatás lehetősége. Vezeték nélküli eszközök lehetővé teszik, a számítógépek és egyéb eszközök központi csatlakozását.

Virtuális LAN (VLAN): A virutális LAN (VLAN) a hosztok egy csoportja, mely a fizikai helyüktől függetelnül úgy kommunikálnak a velük azonos VLAN-ban lévő számítógépekkel, mintha egy kapcsolóra lennének csatlakoztatva. A VLAN ugyanazokkal a jellemzőkkel bír, mint egy fizikai helyi hálózat (LAN), de lehetővé teszi az eszközök együtt kezelését még akkor is, ha nem ugyanarra a hálózati kapcsolóra csatlakoznak.

Hálózati topológia (Network Topology): A hálózati topológia (Network Topology) meghtározza a hosztok összekötésének módját a hálózatban.

DNS (Domain Name System): A DNS (Domain Name System) vagyis a tartománynévrendszer, amely világszinten működő szolgáltatás a számítógép nevek IP címekre való feloldásához. A DNS egy jól megtervezett hierachikus, nagymértékben elosztott elnevezési rendszer. A DNS szerverek (kiszolgálók) egymástól lekérdezve derítik fel a névfeloldáshoz szükséges adatokat.

Network Address Translation (NAT): A NAT az a folyamat, amely során a privát címek Interneten irányítható, nyilvános címekké alakulnak, a hálózati címfordítást (NAT). A belső, privát címek helyi, amíg a külső nyilvános címeket globális címeknek nevezzük. A hálózati forgalom során ekkor elkülönül a hálózaton belüli, és az azon kívüli kommunikáció.

Internet: Az Internet egy globális világméretű, kapcsolódó hálózatok rendszere. Az Internethez kapcsolódó számítógépeknek a TCP/IP protokoll készletet kell használniuk.

Világháló (WWW – World Wide Web): A Világháló (WWW), az Interneten működő egymással úgynevezett hiperlinkekkel kapcsolódó dokumentumok rendszere, melyet egy böngésző segítségével lehet elérni.

Intranet: A számítógép hálózat, mely a TCP/IP protokoll készletet használja, azon a külvilág felé nem érthető el, egy szervezet belső kialakítású rendszere. A felhasználói hitelesítés szerves része

az Intranet-nek. (Felhasználói fiók, jogosultság kezelés). Ideális esetben elzárjuk a külvilág elől a hozzáférhetőségét, ha a konfigurációnk és a felépítésünk ennek megfelelő.

Extranet: A felépítése hasonló az Intranet-hez azonban, az elérés ki van terjesztve a szervezeten kívüli felhasználók számára is, akár egy teljesen másik szervezet is kapcsolódhat.

Virtuális magánhálózat - (Virtual Private Network): A virtuális magánhálózat (Virtual Private Network - VPN) lehetővé teszi két számítógép között a biztonságos kapcsolat felépítését úgy, hogy a számítógépek nem ugyanazon a privát hálózaton helyezkednek el.

Egy „csatorna – (Tunnel) jön létre, mely áthalad a kapcsolódó LAN (Local Area Network) és WAN (Wide Area Network) hálózatokon keresztül. A csatornába csak a két végpont számára olvashatóak az adatok.

IPSec – (Internet Protocol Security): Elsősorban az útválasztók (Router) és a tűzfalak (Firewall) közé (és nem VPN-ekhez) tervezték, a forgalom biztosítása miatt. Az L2TP-vel együtt használva nagy biztonságú, többprotokollos magánhálózatokat is meg lehet vele valósítani.

AAA – (Authentication, Authorization, Accounting): Az AAA (Authentication, Authorization, Accounting) protokoll, azaz a hitelesítés, hozzáférés és naplózás egy a számítógépes biztonság körében használt kifejezés. Egy biztonsági architektúrára utal, mellyel irányítani lehet a felhasználók hozzáférését az egyes szolgáltatásokhoz, illetve, hogy mekkora erőforráshoz férhetnek hozzá.

Tűzfalak (Firewall) és DMZ: Tűzfalakat (Firewall) használjuk az ártalmas szándékú behatolások és támadások kivédésére. A hálózatok elsődleges védelmét biztonsági eszközök, mint tűzfalak (Firewall) védik. A demilitarizált zóna – DMZ segítenek kontrollált módon információt megosztani a külvilággal, miközben a hálózat többi része titokban marad.

Az **LDAP (Lightweight Directory Access Protocol)** egy *egyszerűsített címtárhozzáférési protokoll*, amely címtárak, címjegyzékek elérésére és karbantartására szolgáló, platformfüggetlen protokollcsalád. Olyan fa struktúrán alapuló adatbáziskezelést valósít meg, ahol tipikusan gyorsan kell keresni és sok kis információt kell benne elraktározni. Az LDAP sokféle feladatra használható, például a felhasználók

és csoportok felügyeletének központosítására, a rendszerkonfigurációs adatok kezelésének megkönnyítésére, vagy akár egyszerű címjegyzékek kezelésére.

9.2. Értelmező rendelkezések

GDPR 4.cikk: „**személyes adat**": azonosított vagy azonosítható természetes személyre („érintett") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;

„**adatkezelés**": a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

„**harmadik fél**": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

„**adatvédelmi incidens**": a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

„**személyes adatok határokon átnyúló adatkezelése**":

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy

b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

9.3. Kapcsolódó dokumentumok és szabályzatok

Kapcsolódó szabályzatok, dokumentumok:

- PPKE Szervezeti és Működési Szabályzata (PPKE SZMSZ);
- PPKE Informatikai Szabályzat (PPKE IT-SZ);
- PPKE Információbiztonsági Szabályzata (PPKE IBSZ);
- PPKE Informatikai Felhasználói Szabályzata (PPKE ITF-SZ);
- PPKE Adatvédelmi és Adatbiztonsági Szabályzata (PPKE AVBSZ);
- PPKE Információátadási Szabályzata (PPKE IASZ);
- PPKE Incidenskezelési Szabályzata (PPKE ITINC);
- PPKE Változáskezelési Szabályzata (PPKE ITVA);
- PPKE IT munkaköri leírásai;
- PPKE Információbiztonsági Politika
- PPKE Jelszókezelési szabályzat
- A Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzata (20/2004. (VI.21). IHM rendelet).
- PPKE szolgáltatás katalógus (pl. Neptun, SAP, Nexon, ECM).
- Üzemeltetési / felhasználói dokumentációk.
- Valamint az IT üzemeltetés – szabályozási utasításait (pl. IT folyamat szabályozások, jogosultság kezelés, DRP, mentési rend, BCP)
- Szolgáltatási szint vállalások (SLA – Service Level Agreement)
- PPKE IT stratégia
- Szervezeti Diagram

10. Mellékletek

- Szervezeti Diagram
- Változáskezelési Szabályzat
- Vírusvédelmi Szabályzat
- Jelszókezelési szabályzat
- Információbiztonsági Politika
- Információátadási Szabályzata
- Felhasználói Szabályzata
- Szolgáltatási szint vállalások (SLA – Service Level Agreement)
- PPKE IT szolgáltatásai (Szolgáltatás katalógus)
- Mentési Szabályzat
- Naplózási Szabályzat
- Jogosultságkezelési Szabályzat
- Hálózati szolgáltatásokra vonatkozó Szabályzat
- Titkosítási eljárások használatára vonatkozó Szabályzat
- Incidenskezelési Szabályzat
- IT Üzemeltetés – Szabályozási utasításai
- IT Folyamatszabályozás
- DPR – Disaster Recovery Plan (katasztrófa elhárítási terv)
- BCP – Business Continuity Plan (Üzletmenet folytonosság)
- PPKE_IT_Szolgáltatásai
- Titoktartási szabályzat
- PPKE IT stratégia