Debreceni Egyetem
Információbiztonsági Szabályzat

Dokumentum történet

Verzió	Kiadás dátuma	Kiadás célja / módosítás lényege
1.0	2026.03.20.	KIberbiztonsági törvény és kapcsolódó rendeleteinek betartásához szükséges teljes szabályozás első kiadása.

TARTALOMJEGYZÉK

1. A Szabályzat célja, hatálya, általános rendelkezések

Kapcsolódó dokumentumok:

a) Jelen Információbiztonsági Szabályzat függelékben felsorolt eljárásrendjei
b) Információbiztonsági Politika
   - A biztonság erősítése és fenntartása érdekében az Információbiztonsági Szabályzat 1. számú mellékleteként a Debreceni Egyetem (a továbbiakban: ***Egyetem***) kiadja Információbiztonsági Politikáját (a továbbiakban: ***IBP***), aminek betartása és ismerete minden érintett számára kötelező, és amelynek karbantartása, folyamatos felülvizsgálata, szükség esetén módosítása az ***Egyetem*** elektronikus információs rendszer biztonságáért felelősének (a továbbiakban: ***IBF***) a feladata. A jelen szabályzat elválaszthatatlan részét képező IBP-t évente felül kell vizsgálni.
   - Amennyiben az ***Egyetem*** informatikai rendszereiben, vagy a vonatkozó jogszabályokban jelentős változások következnek be, akkor az ***IBP***-t felül kell vizsgálni és módosítani kell. A módosítások, felülvizsgálatok kezdeményezése és a módosítások elvégzése az Informatikai Biztonsági Központ Igazgatójának a feladata. A módosított ***IBP***-t, mint az Információ Biztonsági Szabályzat mellékletét, előterjesztést követően a Szenátus fogadja el.
   - Az ***IBP***-t az ***Egyetem*** minden munkatársával éves rendszeres Információbiztonsági oktatás keretében ismertetni kell. Az ***IBP***-t az ***Egyetem*** honlapján kell folyamatosan elérhetővé tenni.

1.1 A szabályozás célja

Az Információbiztonsági Szabályzat (a továbbiakban: ***IBSZ***) célja az ***Egyetem*** szervezeti egységei számára az információbiztonsággal kapcsolatos követelmények és szabályozások dokumentálása, a szerepkörök, feladatok, folyamatok, felelősségi körök definiálása, az elvárt és betartandó magatartásformák és gyakorlatok meghatározása az egyetemi elvárásoknak megfelelően, a vonatkozó jogszabályok és szakmai ajánlások figyelembevételével. Célja továbbá, hogy támogassa a biztonság erősítését, a káros behatások számának csökkentését, védelmi prevenció kidolgozását és a katasztrófakezelés költséghatékony optimalizálását.

Jelen ***IBSZ*** magába foglalja az ***Egyetem*** informatikai biztonságra vonatkozó szabályozását is. Az ***IBSZ***-ben meghatározott védelmi elveknek megfelelő működés biztosításának a rendszerek fennállásának teljes ciklusa alatt érvényesülniük kell (megtervezés, üzembe helyezés, működés, megszüntetés-kivonás).

Az ***Egyetem*** nagy mennyiségű, heterogén adatot (személyes, gazdasági, gazdálkodási, kutatási, oktatási, egészségügyi) kezel, birtokol. Ezen adatvagyon védelme a bizalmasság, sértetlenség és rendelkezésre állás kritériumok biztosításához kiemelt stratégiai fontosságú, összetett és csak felelősségteljes hozzáállással megvalósítható feladat.

Az ***IBSZ*** célja olyan szabálykörnyezet létrehozása, amely átfogó, tudatos és követhető elvárásokat fogalmaz meg az informatikai, adat és információ védelem ***Egyetem*** szintű, ***Egyetem*** érdeke szerinti megvalósítására.

Az ***IBSZ*** kiterjed a távoli munkavégzés szélesebb körben történő alkalmazásával a saját tulajdonú munkaeszközöknek az ***Egyetem***, mint munkáltató érdekében történő használatára is. A munkavállaló köteles az ilyen módon használt eszközök és hálózati környezet vonatkozásában az elvárható gondosság elvének megfelelően eljárni, és az információbiztonsági kockázatok csökkentésére irányuló előírásokat betartani.

Az információbiztonsági szabályozás kidolgozása során a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvényben (továbbiakban: ***Kiberbiztonsági tv.***) és Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII.23.) Korm.rendeletben (a továbbiakban: ***Vhr.***), továbbá a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében

alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. VI. 24. MK rendeletben (továbbiakban: ***MK rendelet***) megfogalmazott irányelvek betartása volt az irányadó.

A Kiberbiztonsági tv. 5. § (1) bekezdése értelmében: Az e törvény hatálya alá tartozó elektronikus információs rendszerek (továbbiakban: ***EIR***) teljes életciklusában meg kell valósítani és biztosítani kell:

a) az ***EIR***-ben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint
b) az ***EIR*** és elemeinek sértetlensége és
c) rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

1.2 Területi hatály

Az ***IBSZ*** területi hatálya kiterjed az ***IBSZ*** tárgyi hatálya alá tartozó informatikai erőforrások üzemelési és használati helyszíneire;

a) az ***Egyetem*** valamennyi saját helyszínére és bérelt helyiségeire,
b) a kiszervezett adatfeldolgozási- és üzemeltetési tevékenységeinek helyszíneire az ott tárolt adatok és hosztolt rendszerek tekintetében,
c) az irodán kívül használt eszközök, illetve a saját tulajdonú hivatali munkavégzésre használt eszközök esetében, azok használatának helyére, amelyet részletesen a „HOZZÁFÉRÉS FELÜGYELETI ELJÁRÁSREND” szabályoz.

1.3 Szervezeti hatály

Jelen ***IBSZ*** szervezeti hatálya kiterjed:

a) az ***Egyetem*** összes szervezeti egységére

1.4 Személyi hatály

Jelen ***IBSZ*** személyi hatálya kiterjed:

a) az ***Egyetem*** valamennyi munkavállalójára és hallgatójára,
b) az ***Egyetem*** informatikai rendszereinek valamennyi felhasználójára,
c) az ***Egyetemmel*** szerződéses vagy egyéb jogviszonyban álló természetes és jogi személyekre, abban az esetben és olyan mértékben, amennyiben tevékenységük során az ***Egyetem*** informatikai rendszereihez, információihoz vagy adatvagyonához hozzáférnek, azokat kezelik, feldolgozzák vagy azok működésére hatással vannak.

1.5 Időbeli hatály

Jelen ***IBSZ*** a hatálybalépés napjától, annak, hatályon kívül helyezéséig hatályos.

1.6 Tárgyi hatály

Jelen ***IBSZ*** tárgyi hatálya kiterjed:

a) az ***Egyetem*** valamennyi informatikai rendszerére és szakrendszerére,
b) a teljes informatikai infrastruktúra eszközrendszerére,
c) az informatikai rendszerben feldolgozás alatt álló és ott tárolt, illetve a feldolgozás eredményeként létrejött, minden adatra és adathordozóra, függetlenül annak feldolgozási, vagy előállítási módjától és megjelenési formájától,
d) az informatikai rendszerek és folyamatok összes dokumentációjára (tervezési, fejlesztési, üzemeltetési, felhasználási),
e) nem egyetemi tulajdonban lévő, de az ***Egyetem*** belső hálózatára – egyetemi elektronikus információs rendszer funkciójának biztosítása céljából - csatlakoztatott informatikai eszközökre,
f) Iratkezelési szabályzat- és információbiztonság alá tartozó dokumentációkra, iratokra és azok kezelésére és postázási folyamatára.

2. Az *IBSZ*-szel kapcsolatos feladatok

Az ***IBSZ***-szel kapcsolatos feladatokat és felelősségeket az alábbi táblázat szemlélteti:

Feladat	Gyakoriság	Felelős	Konzulens(ek)	Tájékoztatandó(k)
Az *IBSZ* elkészítése, felülvizsgálata és módosítása	**Évente, szükség esetén**	**IBF**	**IT üzemeltető szervezetek vezetői, Adatvédelmi tisztviselő, Egészségügyi adatvédelmi tisztviselő, Biztonsági főigazgató, Compliance önálló osztályt vezető igazgató, Jogi Igazgató**	**Kancellár**
***IBSZ* elfogadása**	**Új verzió kiadásakor**	**Szenátus**		**IBF**
***IBSZ* kihirdetése**	**Új verzió kiadásakor**	***IBF***		**Szervezeti egységvezetők és munkavállalók**
Az *IBSZ* betartásának ellenőrzése	**Folyamatosan**	**IBF**	**Az Egyetem információbiztonsági feladatainak ellátásában közreműködő szervezetek**	**Kancellár, Adatvédelmi tisztviselő, Egészségügyi adatvédelmi tisztviselő**

2.1 Az *IBSZ* elkészítése

Az ***IBSZ*** elkészítése, a szakmai egyeztetések lefolytatása, a Kancellári jóváhagyásra és a Szenátusi elfogadásra való előterjesztés kezdeményezése az ***IBF*** feladata és felelőssége. Az ***IBSZ*** elkészítésnek folyamatába konzulensként be kell vonni. a Biztonsági Főigazgatót, az IT üzemeltetést végző szervezetek vezetőit, így különösen az Informatikai Szolgáltató Központ Igazgatóját, valamint az ***Egyetem*** adatvédelmi tisztviselőjét, az egészségügyi adatvédelmi tisztviselőjét, a Compliance önálló osztályt vezető igazgatóját és a Jogi Igazgatót

A dokumentum végleges verzióját Szenátusi elfogadásra, az ***IBF*** terjeszti fel a Kancellár felé, engedélyezésre és jóváhagyásra.

2.2 Időszaki felülvizsgálat

Az ***IBSZ*** rendszeres időközönként, de legalább évente egyszer felül kell vizsgálni. Az ***IBSZ***-t soron kívül felül kell vizsgálni minden olyan változás esetén, amelyek az ***IBSZ***-ben foglaltak alkalmazhatóságát, megfelelőségét vagy hatékonyságát érintik; ha a kapcsolódó szabályzatok, különösen ide értve a kockázatmenedzsment keretrendszert, módosításra kerülnek; illetve, ha olyan információbiztonsági incidens történik, amit jelen szabályzási és eljárásrendi környezet az eset egyedisége, ismeretlensége miatt nem érint, nem érinthet. A felülvizsgálat alapja az időközi ellenőrzések, rendkívüli események jegyzőkönyvei, naplói, valamint a kockázatelemzés és -kezelés megállapításai.

Az ***IBSZ*** felülvizsgálata, folyamatos karbantartása az ***IBF*** feladata.

2.3 Eljárásrendek felülvizsgálata

Jelen ***IBSZ***-ben megjelölt és függelékként hivatkozott eljárásrendek részletesen meghatározzák az egyes tevékenységek, folyamatok szabályozott módszereit, lépéseit, amik biztosítják a védelmi és ellenőrzési műveletek reprodukálhatóságát, a tevékenységek hatékony és célorientált végrehajtását, minden érintett megfelelő szintű bevonását.

Az eljárásrendek a vonatkozó törvények és végrehajtási rendeletek keretein belül, a napi gyakorlat, a biztonsági események, incidensek során szerzett tapasztalatok kiértékelése alapján, a hatékonyabb védekezés érdekében módosíthatók.

A módosításokat szakmai érintettség okán az eljárásrendek egy részében az Informatikai Szolgáltató Központ (a továbbiakban: ***ISZK***) Igazgatója, valamint, az Informatikai Biztonsági Központ (a továbbiakban: ***IBK***) Igazgatója kezdeményezheti, az ***IBF*** felé, aki az eljárásrend tematikája szerinti indokolt mértékben bevonja az érintett szervezeti egységek vezetőit, a módosítás megvalósíthatósági egyeztetésébe.

Egyeztetést követően, a véglegesített módosítással egységes eljárásrendet az IBF hagyja jóvá.

Az eljárásrend „***Dokumentum kontroll***" fejezetében a változáskezelést verziókövetéssel kell dokumentálni.

2.4 Rendkívüli felülvizsgálat

Az ***IBSZ***-t az időszakos felülvizsgálaton túl felül kell vizsgálni és szükség esetén módosítani kell:

- az ***IBSZ***-ben hivatkozott szervezetek vagy munkakörök változása esetén;
- súlyos biztonsági kockázatú információbiztonsági események bekövetkezése esetén;
- az információs vagy informatikai biztonság szabályozását érintő jogszabályváltozások esetén;
- az információs vagy informatikai rendszer nagymértékű változása esetén, amikor az információs vagy informatikai rendszer működését, működést kiszolgáló architektúráját, adatkezelését vagy információbiztonsági kockázati szintjét érdemben befolyásolja a változás;
- ha olyan biztonsági incidens következik be, aminek kezelésére, precedens értékére vonatkozó eljárás, utasítás, kezelés, prevenció nincs lefektetve.

2.5 Az *IBSZ* elfogadása és kihirdetése

Az ***IBSZ*** elfogadása az ***Egyetem*** Szenátusának a joga, kihirdetése az ***IBF*** felelőssége.

Az ***IBSZ*** hatályba lépését követő 2 munkanapon belül minden érintettet e-mailben értesíteni kell, és egyben biztosítani kell az ***IBSZ*** folyamatos elérhetőségét. A kommunikációk lebonyolítása az ***IBF*** feladata.

Az ***IBSZ***-t az ***Egyetem*** honlapján „Az Egyetemről – Közérdekű – Szabályzatok", a Kancellária honlapján a „Szabályzatok", menüpont alatt kell elérhetővé tenni, míg az ***IBSZ*** hivatkozott eljárásrendjeit, belső bizalmas információ tartalmuk miatt, védetten, egyetemi EduID belépés kényszerítéssel, a *https://biztonsag.unideb.hu* honlapon az „IBK/IT BIZTONSÁGI SZABÁLYOZÁS DOKUMENTÁCIÓ" menüpont alatt.

2.6 Az *IBSZ* betartásának ellenőrzése

Az ***IBSZ*** betartásának elősegítése és ellenőrzése az ***IBF*** felelőssége, melyben közreműködnek az információbiztonsági feladatok ellátásában érintett személyek, szervezeti egységek, munkacsoportok, informatikai rendszerek üzemeltetésével foglalkozó szervezeti egységek, valamint az ***EIR*** üzemeltetéséért, fejlesztéséért és az ***EIR***-hez kapcsolódó ellátási lánc kapcsolattartásért felelős szervezeti egységek vezetői.

Az ***IBSZ*** betartásának ellenőrzésével összefüggésben az ***IBF***-nek az ***Egyetem*** Kancellárja felé, míg GDPR érintettség esetén az Adatvédelmi és Egészségügyi adatvédelmi tisztviselő felé is tájékoztatási kötelezettsége is van.

2.7 Az *IBSZ* közlése

Az ***IBSZ*** végrehajtásával kapcsolatos releváns ismereteket az ***Egyetemmel*** hallgatói viszonyban, munkaviszonyban, vagy munkavégzésre irányuló más jogviszonyban álló személlyel a rá vonatkozó mértékben ismertetni kell elsődlegesen tudatossági és elővigyázatossági képzés formájában, ügyelve arra, hogy az ***IBSZ*** védelme biztosított legyen. A megismertetett részek szükség szerint korlátozhatók a munkavégzés/tevékenység szempontjából releváns részekre korlátozottak.

2.8 Kivételkezeléssel kapcsolatos feladatok

Amennyiben az ***Egyetem*** informatikai rendszereinek üzemeltetésében olyan indokolt, az ***IBSZ***-ben nem deklarált - biztonsági integritást nem sértő - megoldást kell a szolgáltatási eredményesség érdekében végrehajtani, azt „kivételes kezelést igénylő esetként” kell tekinteni, és a szabályozásban kezelendő céllá kell minősíteni.

2.9 Az *IBSZ* felépítése

Az ***IBSZ*** felépítése, logikai vezetése követi a 7/2024. (VI.24.) MK rendeletet, a biztonsági osztályba sorolás követelmén**yeiről**, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről követelményeinek felépítését, fő fejezetcímek, alfejezetek, valamint a kapcsolódó követelmények rendeleti fejezetcímeinek vonatkozásában.

3. Az *IBSZ*-ben alkalmazott definíciók

Rövidítés	Leírás
BIA	Business Impact Analysis – Üzleti hatáselemzés, mely egyes rendszerek vagy funkciók kiesésének, biztonsági eseményeknek az üzleti folyamatokra és szolgáltatások működésére, valamint a szervezeti költségvetésre gyakorolt hatását méri fel
EIR	Elektronikus információs rendszer a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat; b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy c) az a) és b) alpontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok; Forrás: **Kiberbiztonsági tv.** Egy elektronikus információs rendszernek kell tekinteni az azonos célból kezelt adatok kezelésében, feldolgozásában résztvevő erőforrások (technikai eszközök, személyek, eljárási szabályok) együttesét. Ennek alapján: Több elektronikus információs rendszernek lehetnek közös rendszerelemei. Egy elektronikus információs rendszernek lehetnek külső közreműködő tulajdonában álló rendszerelemei. Forrás: https://nki.gov.hu/hatosag/tartalom/gyik/
IBIR	Az információbiztonsági irányítási rendszer, az ***Egyetem*** átfogó vállalatirányítási rendszerének az a része, amely a működési kockázatokra építve az információk védelmét, kezelését, felülvizsgálatát és folyamatos fejlesztését biztosítja. Nemcsak informatikai eszközökről, hanem szabályzatokról, folyamatokról és a kockázatok szisztematikus kezeléséről szól, magában foglalja a Biztonsági Eseménykezelő Központot és támogatja az Integrált Eseménykezelő Csoportot.
IBSZ	Információ Biztonsági Szabályzat – Jelen dokumentum

Rövidítés	Leírás
SZTFH	Szabályozott Tevékenységek Felügyeleti Hatósága
NKI	Nemzeti Kiberbiztonsági Intézet
IBF	Elektronikus Információs Rendszerek Biztonságáért Felelős személy (megegyezik az ***EIRBF***-fel)
EIRBF	Elektronikus Információs Rendszerek Biztonságáért Felelős személy, megegyezik az ***IBF***-fel.
Kiberreziliencia	A kiberreziliencia (kiber-ellenállóképesség) egy szervezet képessége arra, hogy a kiberfenyegetéseket megelőzze, azokra reagáljon, és támadás vagy üzemzavar esetén gyorsan helyreálljon, miközben folyamatosan biztosítja az alapvető üzleti funkciókat. Túlmutat a hagyományos kiberbiztonságon: nemcsak a behatolás megakadályozására, hanem a működőképesség fenntartására fókuszál.
Kiberhigiénia	A kiberhigiénia (cyber hygiene) olyan alapvető, rendszeresen végzett biztonsági gyakorlatok és óvintézkedések összessége, amelyeket a digitális eszközök (számítógépek, okostelefonok, hálózatok) használói alkalmaznak az adataik védelme és a kiberbiztonsági kockázatok csökkentése érdekében.

4. Informatikai biztonsági szerepkörök és felelősségek

Az Egyetemnek, mint az ***EIR***-ek felett rendelkezési joggal rendelkezőnek, az ***EIR***-ek teljes életciklusában meg kell valósítani és biztosítani kell;

a) az adatok, információk kezelésére használt eszközök, ideértve a környezeti infrastruktúrát, a hardvert, a hálózatot és az adathordozókat,
b) az adatok, információk kezelésére használt eljárások, ideértve a szabályozást, a szoftvert és a kapcsolódó folyamatokat, valamint,
c) az *a)* és *b)* pontban foglaltakat kezelő személyek együttesének,

védelmét.

Az informatikai és információbiztonsági feladatokat ellátó szervezeti egységeket egyetemi szinten el kell különíteni. Az ***Egyetem*** információbiztonsági feladatainak ellátása során a következő szerepkörök érintettek:

a) Kancellár
b) Biztonsági főigazgató
c) ***IBF***
d) ***IBK*** Igazgató
e) ***ISZK*** Igazgató
f) Adatgazda szerepkör
g) Alkalmazásgazda szerepkör
h) Rendszergazda szerepkör
i) Szervezeti egység vezetője
j) Felhasználó

4.1 Kancellár

Hatásköre

Az Egyetem információbiztonsági rendszerének működtetése a Kancellár felelőssége. Tevékenységét a Kancellár-helyettesek, a Biztonsági főigazgató, az Elektronikus Információs Rendszerek Biztonságáért

Felelős személy, az Információ biztonságért felelős szervezet igazgatója, valamint az Informatikai szolgáltatást nyújtó szervezet igazgatója bevonásával gyakorolja, a rájuk vonatkozó feladatkiosztással és felelősség meghatározásával a Kancellária Ügyrend szerint.

Felelőssége

a) A Nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény 13/A. §, és az ***Egyetem*** Szervezeti és Működési Szabályzatának 24. § (3) bekezdésének a) pontja alapján a Kancellár felel az ***Egyetem*** informatikai tevékenységéért;
b) amelynek keretében felelőssége az informatikai biztonsággal kapcsolatos felsővezetői döntések meghozatala, a szükséges pénzügyi keretek biztosítása;
c) biztosítja, hogy rendelkezésre álljanak az ***EIR*** védelmének szükséges feltételei, jogosultságok, információk, humán-és anyagi erőforrások;

Törvény által előírt kötelezettségei

a) az ***Egyetem EIR***-jeinek biztonsági osztályba sorolásának jóváhagyása;
b) ***IBF***-et nevez ki vagy bíz meg;
c) biztosítja az ***IBF*** részére, hogy valamennyi, az ***EIR***-ek védelmét érintő döntés előkészítésében részt vegyen;
d) döntéshozatal az ***IBF*** hatáskörét meghaladó ügyekben;

4.2 Biztonsági főigazgató

Hatásköre

Az irányítása alá tartozó szervezeti egységek és funkciók működtetése, irányítása és felügyelete, ellenőrzése.

Felelőssége

a) Felelős az ***Egyetem*** információbiztonsági rendszere védelmének a védelmi koncepcióba integrálásáért és a rendszerbiztonsági intézkedések végrehajtásának támogatásáért, koordinációjáért;
b) A Kancellár rendszeres tájékoztatása a hatáskörébe tartozó feladatok végrehajtásáról és a felmerült problémákról;
c) A külső és belső ellenőrzésekhez szükséges feltételek biztosítása, intézkedés kezdeményezése az ellenőrzések által feltárt hiányosságok megszüntetése érdekében;
d) ***IBSZ*** előterjesztés előtti jóváhagyása;

Feladatai

a) Az ***Egyetem*** biztonsági és védelmi feladatainak koordinálása;
b) Ellenőrzi és felügyeli a kritikus információbiztonsági projektekben a szakmai munkát;
c) Koordinálja a fizikai biztonság, személyi biztonság és rendszerbiztonság összehangolását.

4.3 Elektronikus információs rendszer biztonságáért felelős (*IBF*)

Az ***Egyetem*** Kancellárja a ***Kiberbiztonsági tv.*** előírásainak betartása érdekében, elektronikus információs rendszer biztonságáért felelős (IBF) személyt nevez ki, vagy bíz meg. Az ***IBF*** feladatai személyes felelősség mellett láthatóak el.

Az ***IBF*** szerepe az egyetemi ***EIR***-ek védelméhez kapcsolódó szabályozás kialakítása, a rendszervédelmi feladatok ellátása, a kockázatmenedzsment keretrendszer működtetése, a kiberbiztonsági incidensek bejelentése és a kiberbiztonsági incidenskezelő központtal való kapcsolattartás törvényi feladatainak betartása.

Hatásköre

Jogosult bármely ***EIR*** tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, auditálásában, vizsgálatában, kockázatelemzésében és kockázatkezelésében, karbantartásában vagy javításában közreműködőtől a biztonsági követelményekről tájékoztatást kérni. Ennek keretében az általa előzetesen meghatározott követelményeknek való megfelelőség alátámasztásához jogosult bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az ***EIR***-ek biztonsága tárgyában keletkezett valamennyi IT biztonságot érintő dokumentumot. Jogosult ezen bekért információk és dokumentumok

véleményezésére, továbbá véleményezési joga van valamennyi elektronikus információbiztonságot érintő szabályzat tekintetében, továbbá minden olyan beszerzés esetében, amelynek közvetlen vagy közvetett hatása lehet az elektronikus információbiztonságra. A fizikai védelmi szabályoknak megfelelően jogosult belépni információbiztonsági ellenőrzés céljából az ***Egyetem*** olyan helyiségébe, ahol információbiztonságot érintő munkavégzés folyik;

a) Jogosult minden - információbiztonságot érintő - kérdésben észrevételeit és javaslatait megtenni. Jogosult a szolgáltatási szerződések információbiztonsági követelményeinek szakmai meghatározására, véleményezésére és felülvizsgálatára;
b) Feladatai ellátása során a Kancellárnak és a Biztonsági főigazgatónak közvetlenül adhat tájékoztatást, jelentést;

Felelőssége

A ***Kiberbiztonsági tv.*** és kapcsolódó rendeleteiben előírt jogszabályi megfelelés biztosítása és kapcsolódó feladatok végzése.

Feladatai

a) Gondoskodik az ***Egyetem EIR***-jeinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról;
b) Gondoskodik a kockázatkezelési keretrendszer szerinti tevékenységek tervezéséről, szervezéséről, koordinálásáról, elvégzéséről és ellenőrzéséről;
c) Előkészíti az ***Egyetem EIR***-jeire vonatkozó ***IBSZ***-t és gondoskodik annak folyamatos aktualizálásáról, valamint a jóváhagyott ***IBSZ***-t megküldi a nemzeti kiberbiztonsági hatóság részére;
d) Előkészíti az ***Egyetem EIR***-jeinek biztonsági osztályba sorolását;
e) Előkészíti és kezdeményezi a kiberbiztonsági hatóságnál az ***Egyetem EIR***-jeivel kapcsolatos engedélyezési eljárásokat;
f) Véleményezi az ***EIR***-ek biztonsága szempontjából az ***Egyetem*** elektronikus információbiztonságot érintő szabályzatait és szerződéseit;
g) Kapcsolatot tart a kiberbiztonsági hatósággal és a kiberbiztonsági incidenskezelő központtal;
h) Az ***Egyetem*** bármely ***EIR***-jét érintő incidensről tájékoztatja a kiberbiztonsági incidenskezelő központot;
i) Folyamatos és tervezett ellenőrzéseket végez annak vizsgálatára, hogy az ***Egyetem*** elektronikus információbiztonságra vonatkozó belső normáiban lévő előírások hogyan valósulnak meg, ennek megállapításait írásban rögzíti a Kancellár számára;
j) Gondoskodik a vezetők és az alkalmazottak IT biztonsági tudatosságának növelésére, informatikai jellegű támadás vagy egyéb informatikai vészhelyzet esetén követendő magatartására vonatkozó oktatásról;
k) Felülvizsgálja, hogy az ***Egyetem*** elektronikus információbiztonságot érintő belső szabályzatai összhangban vannak-e a hatályos jogszabályokkal és az ***Egyetem*** belső szabályozóival;
l) Az ellenőrzések és az esetleges incidensek tapasztalatai felhasználásával – a fejlesztendő területekre vonatkozó javaslatokat tartalmazó – biztonsági helyzetértékelést készít a Kancellár számára;
m) Legalább évente megvizsgálja az ***EIR***-re vonatkozó biztonsági osztályhoz kapcsolódó védelmi intézkedések értékelése során megállapított hiányosság megszüntetésére készített intézkedési tervet. Ennek előre haladásáról beszámolót készít a Kancellár számára, amiben kiemeli az esetleges lemaradásokat és a rövidtávon szükséges intézkedéseket;
n) A kiberbiztonsági auditokra történő felkészülés irányítása és a megfeleléshez szükséges felülvizsgálatok végzése, folyamatok gondozása;
o) Részt vesz az informatikáért felelős miniszter rendeletében meghatározott szakmai képzésen és továbbképzésen;
p) Elemzéseket végez és javaslatokat tesz a megfelelő védelmi intézkedésekre és a biztonságos működéssel összefüggő szabályok megváltoztatására;

4.4 Informatikai Biztonsági Központ Igazgató

Hatásköre

Az informatikai biztonsági feladatok koordinálásáért, végrehajtásáért és a védelmi intézkedések felügyeletéért felelős vezető.

Felelőssége

a) Az ***Egyetem*** (elektronikus) információbiztonságának fenntartása, felügyelete és folyamatos fejlesztése, az Informatikai Biztonsági Irányítási Rendszer (a továbbiakban: ***IBIR***) működtetése, eseti és rendszeres karbantartása;
b) Az előírt adatszolgáltatási és jelentési kötelezettség teljesítése más szervezetek, szakmai csoportok irányába, illetve a folyamatos szakmai kapcsolat fenntartása az érdekeltekkel, szakmai csoportokkal;
c) Ennek keretében felel az ***Egyetemnél*** előforduló, az ***EIR***-ek védelméhez kapcsolódó feladatok ellátásáért, a kialakított biztonsági kontrollok hatékony működéséért, az információbiztonságával kapcsolatos tevékenységek koordinálásáért a vonatkozó jogszabályok, szabványok, ajánlások előírásainak megfelelően.
d) Kiberreziliencia megvalósítása és fenntartása céljából szükséges szakmai feladatok, döntések előkészítése;
e) Az információbiztonság fejlesztésével kapcsolatos célok meghatározása és az intézkedések megtervezésében való részvétel;

Feladatai

a) Elemzéseket végez és javaslatokat tesz a megfelelő védelmi intézkedésekre és a biztonságos működéssel összefüggő szabályok megváltoztatására;
b) Felügyeli a biztonsági előírások betartását;
c) Az ***Egyetem*** információbiztonsági kockázatkezelő rendszerének szabályozása alapján az informatikai és információbiztonsági területre vonatkozó kockázatkezelési tevékenység szervezetszintű megvalósításának irányítása és szükség szerinti ellenőrzése;
d) A kockázatok mérséklésére vagy a működés hatékonyságának növelésére vonatkozó ajánlások készítése;
e) Informatikai biztonsági oktatási stratégia elkészítése, a stratégia alapján az informatikai biztonsággal kapcsolatos oktatási anyagok kidolgozása és az oktatások elvégeztetése, kapcsolódó nyilvántartások vezetése;
f) Kiber gyakorlatok keretében támadás szimulációs kampányok végzése a dolgozók körében, kampány eredmények kiértékelése és a javító intézkedések megtétele;
g) Javaslattétel az információbiztonsági felhasználói tudatosság fejlesztésével kapcsolatos intézkedésekre;
h) Felügyeli és ellenőrzési terv keretében, valamint ad-hoc ellenőrzésekkel biztosítja az informatikai biztonsági előírások betartását, valamint az informatikai rendszerek biztonsági folyamatainak ellenőrzése;
i) Az információbiztonsággal összefüggő biztonsági szabályzatok előírásainak durva megsértéséről, azonnali jelentési kötelezettsége áll fenn a Kancellár, a Biztonsági főigazgató, az ***IBF***, valamint az érintett területek vezetői felé;
j) Az informatikai rendkívüli események és IT biztonsági incidensek kivizsgálása, kezelése;
k) IT biztonsági hibajegykezelő (ticketing) rendszer kialakítása, bejelentések kezelése, statisztikák-riportok összeállítása;
l) Az ***EIR***-ek nyilvántartásának (szoftvernyilvántartás) és adatvagyon leltárjának összeállítása, rendszeres karbantartása;
m) Információbiztonsági projektek vezetése, informatikai projektekben a biztonsághoz kapcsolódó szakmai munka támogatása, ellenőrzése;

n) A jogosultságok nyilvántartásának és a felhasználói adminisztrációkban szereplő jogosultságok érvényesülésének ellenőrzése;
o) Kíberhigiénia kialakítása, fenntartása;

4.5 Informatikai Szolgáltató Központ Igazgató

Hatásköre

Az ***Egyetem EIR***-jeinek és az azokat kiszolgáló infrastruktúra biztonságos üzemeltetéséért felelős vezető.

Felelőssége

Az informatikai üzemeltetés-, beszerzések koordinálása, felügyelete az informatikai biztonsági elvárások betartásának figyelembevételével.

Feladatai

a) az ***EIR*** funkcionális és biztonsági követelményeknek megfelelő működtetése;
b) az informatikai rendszer üzletmenet folytonossági elvárásoknak megfelelő rendelkezésre állásának biztosítása;
c) működésfolytonossági tesztek elvégzése;
d) az informatikai folyamatok és tevékenységek tervezése és folyamatos fejlesztése;
e) rendkívüli helyzetek elhárítása;
f) az informatikai rendszer biztonsági komponenseinek üzemeltetéséhez szükséges erőforrások biztosítása;
g) az informatikai rendszerüzemeltetés és rendszerhasználat rendszeres felülvizsgálatának biztosítása;
h) az informatikai szervezeti egység vezetők bevonásával gondoskodik a mentési stratégia kialakításáról, a mentési rend elkészítéséről. Ellenőrzi a mentési eljárások betartását, gondoskodik a mentések tárgyi és személyi feltételeiről;
i) rendszeresen – az ***Egyetem*** Informatikai Katasztrófa-elhárítási Tervében leírtak szerint – gondoskodik a katasztrófahelyzet kezeléssel kapcsolatos tesztek elvégzéséről;
j) a programfejlesztési igények, az elkészült termékek informatikai ellenőrzése az ***Egyetem*** belső szabályzatai és jelen ***IBSZ*** előírásai szerint.
k) a fokozottan védett területekre (erőforrástermek) történő belépés és az ott történő munkavégzés engedélyezése, az engedélyek rendszeres felülvizsgálata;
l) Engedélyezési eljárás lefolytatása a rendszerhez való távoli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően;

Az *IBF*-fel megosztott feladatai:

a) az ***Egyetem*** információbiztonsági követelményeinek alkalmazása, és betartatása;
b) gondoskodni arról, hogy az információbiztonsági feladatok és követelmények beépüljenek a hatáskörébe tartozó szolgáltatások üzemeltetési folyamataiba;
c) a fokozottan védett területek (erőforrástermek) belépési nyilvántartásának ellenőrzése a Biztonsági főigazgató és a Humán és Fizikai Védelmi Osztályvezető tájékoztatásával;
d) beszállítói lánc szolgáltatási szerződések információbiztonsági elvárásainak felülvizsgálata;
e) szakmailag közreműködik a működésfolytonosságot biztosító szabályozás elkészítésében, és a működésfolytonosság megszakadása esetén értesítendő személyek elérhetőségeit tartalmazó címlista aktualizálásában.

4.6 Adatgazda szerepkör

Hatásköre

Az adatgazda annak az önálló szervezeti egységnek a vezetője, ahol az adat keletkezik, illetve amelyhez jogszabály vagy szervezetszabályozó eszköz az adat kezelését vagy nyilvántartás vezetését elrendeli. Egy ***EIR***-hez több adatgazda is kijelölhető, akik között megoszlanak a szerepkörrel járó, alábbiakban felsorolt feladatok és felelősségek. Az ***Egyetemen*** üzemeltetett, adatokat kezelő informatikai rendszerek mindegyikét be kell sorolni legalább egy-egy adatgazda felügyelete alá.

Felelőssége

Az adatgazda felel:

a) az adatokkal és az adatok felhasználásával kapcsolatos stratégiai szintű döntések meghozataláért;
b) általa felügyelt vagy irányított tevékenységekhez kapcsolódóan keletkezett, informatikai rendszerben tárolt és kezelt adatok, információk megbízhatóságát, hitelességét biztosító folyamatok megfelelősségét biztosító és illetékességi körében releváns szabályok betartásáért;
c) az illetékessége alá tartozó ***EIR***-ek biztonsági osztályba sorolásáért az ***IBF***-fel együttműködve.

Feladatai

a) az ***Egyetem*** egyes működési folyamatai esetében, az általuk használt adatok vonatkozásában az adatgazdák az ***IBF***-fel közösen állapítják meg az adatkezelés biztonsági követelményeit;
b) Meghatározza az adatokhoz / tevékenységekhez hozzáférőket, a szükséges-elégséges hozzáférési elv alapján, azaz mindenki csak annyi jogot kapjon, amennyi a munkája elvégzéséhez feltétlenül szükséges;
c) Az alkalmazásgazdák közreműködésével összegyűjti azokat a szakmai igényeket, amelyek alapján az informatikai fejlesztések, beruházások prognosztizálhatók.

4.7 Alkalmazásgazda szerepkör

Hatásköre

Az alkalmazásgazda az a szakmai kompetenciával rendelkező, felhasználói területi kulcsfelhasználó munkatárs, aki az adott alkalmazás teljes funkcionalitását, felhasználói üzleti logikáját ismeri, valamint a rendszer funkcióit rendszeresen alkalmazza. Támogatja az érintett rendszert használó szakterületi munkatársakat a rendszer napi használatában, valamint segítséget nyújt a változtatási igények megfogalmazásában. Egy ***EIR***-hez több alkalmazásgazda is kijelölhető, akik között megoszlanak a szerepkörrel járó, alábbiakban felsorolt feladatok és felelősségek.

Feladatai

a) az adatgazda utasítása szerint köteles közreműködni az ***EIR***-ek biztonsági osztályba sorolásában;
b) a szakterületi felhasználók tevékenységének a támogatása az adott alkalmazás használatában;
c) közreműködik a felhasználók által megfogalmazott módosítási, fejlesztési igények pontos definíciójának (követelményspecifikációjának) kialakításában, továbbá – amennyiben egy módosítási, fejlesztési igény több szakterületet érint – gondoskodik az igények, vélemények konszolidálásáról;
d) az adatgazda utasításai alapján közreműködik: az adatok azok tárolására rendszeresített alkalmazásban való rendelkezésre állását biztosító folyamatok napi működtetésében;
e) a hatáskörébe tartozó informatikai rendszerek forráskód tárai tartalmának aktualizálásában, érvényességének folyamatos fenntartásában;
f) az ***Egyetemen*** rendelkezésre álló adatok, információk felhasználását (hasznosítását), valamint az adatok külső vagy belső publikálását, átadását biztosító folyamatok napi működtetésében.

Felelőssége

a) a hozzárendelt alkalmazás teljes funkcionalitásának, üzleti logikájának az ismerete, amely a rendszer funkcióinak a rendszeres használatán alapul,
b) az alkalmazás használatával kapcsolatos nem informatikai jellegű problémákról az adatgazda tájékoztatása és a megoldási lehetőségek megfogalmazása.

4.8 Rendszergazda szerepkör

Hatásköre

A rendszergazda az az üzemeltetésért felelős személy, aki adott rendszer üzemeltetési szakmai kompetenciájával rendelkezik, aki a rendszer beállításait, működés felügyeletét, jogosultság

beállításait rendszeresen végzi. Egy ***EIR***-hez több rendszergazda is kijelölhető, akik között megoszlanak a szerepkörrel járó, alábbiakban felsorolt feladatok és felelősség.

Feladatai

a) az általa üzemeltetett rendszer nyilvántartásait (mint ***EIR*** rendszerelem leltár, rendszerbeállítási paraméterek, jogosultság) naprakészen tartja;
b) a hatáskörébe tartozó üzemeltetési feladatokat végrehajtja;
c) biztosítja a rendszerfelügyeletet;
d) üzemelteti a rá bízott ***EIR***-eket;
e) időszakos periódusokban ellenőrzi a munkahelyek eljárásrendben rögzített biztonsági előírásainak betartását.

Felelőssége

Az általa üzemeltetett ***EIR***-ek jelen ***IBSZ***-ben, valamint a kapcsolódó eljárásrendjeiben foglaltak szerinti biztonságos üzemeltetése.

4.9 Szervezeti egység vezetők

Hatáskörük

A szervezeti egységük által használt ***EIR***-ekhez és azokban lévő adatokhoz a hozzáférési jogosultságok meghatározása, beállításuk kezdeményezése (igénylés, módosítás, visszavonás), továbbá a szervezeti egységük dolgozói felé utasítási jogkörrel rendelkeznek.

Felelősségük

A közvetlen munkatársai körében a munkavégzésük során használt ***EIR***-ekben kezelt adatok információbiztonsági követelményeinek megismertetése és betartatása, és az elektronikus információbiztonsági kontrollok működtetése. Felelős a hatás- és jogosultsági körének megfelelően az előírásait megszegőkkel szemben a felelősségre vonás kezdeményezéséért, a szervezeti egységet érintő szerződésekben az ***IBSZ*** előírásainak a vállalkozókkal, szolgáltatókkal, szakértőkkel szembeni érvényesítéséért. Köteles a tudomására jutott, az ***Egyetem*** információbiztonságát veszélyeztető, működését sértő eseményekről, körülményekről – azok jellegétől függően – az ***IBF***-nek információt nyújtani. Felelőssége továbbá a területéhez tartozó személyes adatoknak a személyes adatok kezelésére vonatkozó jogszabályok szerinti, illetve a szervezeti egysége egyéb adataiknak a vonatkozó jogszabályoknak és elvárásoknak megfelelő kezelése, valamint az ezekhez kapcsolódó hozzáférési jogosultságok meghatározása, beállításuk kezdeményezése, valamint felülvizsgálata.

4.10 Felhasználók

Hatáskör

Adott ***EIR***-eket munkavégzése során igénybe vevő munkavállaló.

Jogosultak a munkavégzésükhöz szükséges és elégséges mértékű hozzáférést kapni az információs rendszerekhez, eszközökhöz, szolgáltatásokhoz.

Feladat

a) Kötelessége az információk védelmét, azok keletkezésének, feldolgozásának, szétosztásának, tárolásának teljes folyamata, életciklusa során biztosítani;
b) Valamennyi felhasználó köteles azonnal értesíteni a felettesét vagy az ***IBK***-t (https://biztonsag.unideb.hu/kapcsolat menüpont alatt felsorolt elérhetőségek), információbiztonságot érintő esemény észlelése/bekövetkezése esetén.

Felelősség

Valamennyi felhasználó felelős;

a) az ***IBSZ*** megismeréséért és az abban foglalt szabályok betartásáért;
b) a birtokában lévő, vagy tudomására jutott információk bizalmasságának megfelelő kezeléséért;
c) az ***EIR***-ben végzett műveletekért;
d) az ***Egyetem EIR***-jeinek szakszerű kezeléséért;

e) a használatában lévő informatikai eszközök előírásszerű használatáért, megőrzéséért;
f) az előírások és biztonsági követelmények betartásáért azon adatok és információs rendszerek tekintetében, amelyeket használnak, vagy amelyekkel bármilyen módon kapcsolatba kerülnek;
g) biztonságtudatos viselkedés az ***Egyetem*** kiberbiztonságának erősítése érdekében.

4.11 Kapcsolattartás a hatóságokkal

A jogszabályokban meghatározott hatóságokat az ***IBF*** tájékoztatja az ***EIR***-ek biztonsági eseményeiről és incidenseiről, valamint teljesíti az ***Egyetem*** jogszabályi előírásként megfogalmazott elektronikus információbiztonsággal összefüggő adatszolgáltatási kötelezettségeit, valamint az incidensbejelentési és ezzel összefüggő jelentési feladatait is, továbbá a kapcsolatot tart fenn a Nemzeti Kiberbiztonsági Intézettel (továbbiakban: ***NKI***) és a Szabályozott Tevékenységek Felügyeleti Hatóságával (továbbiakban: ***SZTFH***).

A fenti tevékenységeiről az ***IBF*** a Kancellár és a Biztonsági főigazgató felé tartozik tájékoztatással, továbbá megosztja a tudomására jutott naprakész informatikai biztonsági – fenyegetésekre és sebezhetőségekre vonatkozó – információkat, eljárásokat és technikákat az érintett szervezeti egységekkel.

Az ***IBF***-nek folyamatosan figyelemmel kell kísérnie a jogszabályban kijelölt szervezetek által kiadott riasztásokat, és gondoskodnia kell az egyes ***EIR***-ekre vonatkozó megfelelő ellenintézkedésekről és válaszlépésekről.

4.12 Összeférhetetlen funkciók

Az ***Egyetem*** folyamatosan törekszik mindazon szervezeti feladatok és funkciók különválasztására, melyek együttes ellátása a biztonsági kockázatokat indokolatlanul növeli. Ezen összeférhetetlen funkciók általánosságban:

a) az információbiztonsági és az informatikai üzemeltetési feladatok együttes ellátása;
b) az ***IBF*** szerepkört a pártatlanság és függetlenség fenntartása miatt nem szabad összevonni IT üzemeltetéssel vagy fejlesztéssel kapcsolatos szerepkörrel (**Kiberbiztonsági tv.** 7/11§/4);
c) rendszer vagy adatbázis üzemeltetési (adminisztrátori) és rendszer vagy adatbázis felhasználói szerepkör együttes birtoklása.

Alapvetően összeférhetetlennek kell tekinteni minden (jogosultság) igénylési és jóváhagyási feladatot, ezért, az engedélyezési folyamatokban az igénylő, engedélyező és megvalósító szerepköröket külön kell választani.

5. Biztonsági osztályba sorolás

Az ***Egyetem*** az ***MK rendelet,*** a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló rendeletben található szempontok alapján biztonsági osztályba sorolja az ***EIR***-jeit. A biztonsági osztályba sorolás eredményét a Kancellár, vagy az általa meghatalmazott képviselő hagyja jóvá. Az ***EIR*** nyilvántartásban és az egyes rendszerek rendszerbiztonsági tervében dokumentálásra kerülnek a jóváhagyott biztonsági osztályba sorolás eredményei.

Az ***Egyetem EIR***-jeinek biztonsági osztályba sorolása kockázatelemzésen és hatáselemzésen alapul (Business Impact Analysis, továbbiakban: ***BIA***), aminek eredményeképpen a biztonsági besorolási osztály szakmai szempontok alapján felülbírálható, A módosítási javaslatot részletes indoklással az ***IBF*** terjeszti fel a Kancellárnak jóváhagyásra.

Az ***IBF*** a kockázatelemzést és a ***BIA***-t legalább évente egyszer felülvizsgája, nagyobb szervezeti változások esetén frissíti, az IT üzemeltető szervezetek vezetőinek közreműködésével. A felmérés módszertana a ***BIA*** módszertan dokumentumban érhető el.

Az ***Egyetemnél*** az informatikai biztonság szinten tartása, valamint az ***EIR***-ek biztonsági osztályba sorolása elvégzésének megalapozása érdekében az informatikai biztonsági kockázatelemzésre

vonatkozó további részletes követelményeket és eljárásokat, továbbá szabályokat a „KOCKÁZATELEMZÉSI ÉS KOCKÁZATKEZELÉSI ELJÁRÁSREND” tartalmazza.

A biztonsági osztályba sorolást az ***EIR*** – illetve az abban kezelt adatok – jelentős megváltozása esetén, de legalább évente felül kell vizsgálni.

6. Informatikai biztonsági ellenőrzés

Az informatikai biztonsági ellenőrzések alapvető célja, hogy a kockázatok csökkentése és a rendkívüli események elkerülése érdekében objektív információkat szolgáltasson a felelős vezetők számára az informatikai biztonság helyzetéről.

Az informatikai biztonsági ellenőrzés célja, hogy rendszeresen vizsgálja:

- az informatikai rendszerek biztonsági megfelelését az ***Egyetem*** által elfogadott biztonsági követelményeknek;
- az egyetemi és rendszerszintű biztonsági szabályozásokban foglaltak érvényesülését;
- az alkalmazott módszerek a jogszabályi előírásoknak való megfelelését;
- az informatikai rendszerek és az általuk nyújtott szolgáltatások biztonságát;
- a biztonsági alapelveket sértő események bekövetkezési valószínűségét, illetve bekövetkezését és kivizsgálását.

Az ellenőrzések során feltárt hiányosságok képezik azon védelmi intézkedések alapját, melyek biztosítják, hogy minimális legyen a védelmi képességek kívánt és valós szintje közötti különbség. A megállapításokat mindig írásos jelentésbe kell foglalni, a védelmi intézkedések megsértésével kapcsolatban adott esetben szankciókat is lehet alkalmazni (lásd Személyi biztonsági eljárásrend). Az ellenőrzések során tapasztalt hiányosságok megszüntetésére intézkedési tervet kell kidolgozni.

Potenciális vagy a valódi biztonsági eseményekkel és biztonsággal kapcsolatos információk, vagy riasztások alapján tesztelési eljárást vagy biztonsági ellenőrzést kell végezni.

Az informatikai rendszereket rendszeres időközönként ellenőrizni kell, vizsgálva azt, hogy az informatikai rendszerek műszaki paraméterei teljesítik-e a feléjük támasztott biztonsági elvárásokat. A rendszer biztonsági ellenőrzésének követelményeit, valamint az ellenőrzést is magában foglaló tevékenységeket (ideértve az automatizált sebezhetőség-vizsgálatokat) gondosan meg kell tervezni, és az érintettekkel egyeztetni szükséges annak érdekében, hogy minimalizálni lehessen az egyetemi folyamatok megszakadásának a kockázatát.

Az informatikai rendszer biztonsági ellenőrzésére az Informatikai Szolgáltató Központ Igazgatójának tájékoztatása mellett, a vele egyeztetett időszakban kerülhet sor. Egyetemi rendszerek biztonsági ellenőrzése előtt az adott rendszer szakmai adatgazdájával történő egyeztetés is szükséges.

A biztonsági teljesítmény mérésének részleteit a „Felügyeleti stratégia” és a „Biztonságértékelési terv” című dokumentumok tartalmazzák.

7. Információbiztonsági véleményezés

Minden olyan esetet, amely az ***IBF*** által előzetesen meghatározott irányelvektől eltérő módon befolyásolhatja az ***Egyetem*** adat- és információ vagyonát, vagy ezek kezelését érintő változást előzetesen, lehetőség szerint már a tervezés fázisában, véleményeztetni kell az ***IBF***-fel. A véleményeztetés kizárólag a szükséges mértékben, különösen az információbiztonságot érintő műszaki, egyetemi és adatkezelési szempontokra terjed ki.

8. Programmenedzsment

8.1 Feladatok - Programmenedzsment

Feladat	Gyakoriság	**Felelős**	Konzulens(ek)	Tájékoztatandó(k)
IBF kinevezése, megbízása	**Szükség esetén**	**Kancellár**		**Biztonsági főigazgató; IT üzemeltető szervezetek vezetői; Jogi Igazgató**
Információbiztonsági célok végrehajtásához és fejlesztéséhez szükséges erőforrások tervezése	**Szükség esetén**	**IBF**	**IBK Igazgató; ISZK Igazgató; Biztonsági főigazgató**	**Kancellár**
Információbiztonsági célok eléréséhez szükséges erőforrások beépítése az éves költségvetés tervezésébe és beruházási igényekbe	**Szükség esetén**	**Kancellár**		
Az információbiztonsági célok eléréséhez szükséges beruházással kapcsolatos döntések meghozatala	**Szükség esetén**	**Kancellár**		
Dokumentációk hatályos törvényeknek, végrehajtási rendeleteknek, irányelveknek, szabályozásoknak, szabványoknak és ajánlásoknak való megfeleltetése	**Szükség esetén**	**IBF**	**ISZK; IBK;**	
Intézkedési terv kidolgozása, frissítése	**A hiányosság megállapítását követően haladéktalanul**	**IBF**	**Biztonsági főigazgató; ISZK; IBK**	**Kancellár**
Intézkedési terv elfogadása	**Szükség esetén 10 munkanapon belül**	**Kancellár**	**IBF**	**Biztonsági főigazgató; IBK**
Intézkedési terv megvalósulásának ellenőrzése	**Negyedévente**	**IBF**	**ISZK; IBK**	**Biztonsági főigazgató**
Riportot készít az intézkedési terv megvalósításáról	**Negyedévente**	**IBF**	**ISZK; IBK**	**Kancellár; Biztonsági főigazgató**

Feladat	Gyakoriság	**Felelős**	Konzulens(ek)	Tájékoztatandó(k)
EIR nyilvántartás készítése és frissítése	**Negyedévente**	**IBK**	**ISZK**	**IBF**
Kritikus infrastruktúra és kulcsfontosságú erőforrások rendszer és architektúra biztonsági terveinek módosítását információbiztonsági szempontból véleményezi.	**Szükség esetén**	**IBF**	**ISZK; IBK**	**Biztonsági főigazgató**
Előkészíti a hatósági jelentéseket egyéb külső szervezetek felé irányuló szakmai információáramlást	**Szükség esetén**	**IBF**	**ISZK; IBK**	**Biztonsági főigazgató**
Engedélyezi a külső szervezetek felé irányuló szakmai információáramlást	**Szükség esetén**	**Kancellár**	**Biztonsági főigazgató; IBK**	**IBF**
Biztonságértékelés készítése, biztonságértékelési terv alapján	**Évente egyszer**	**IBF**	**ISZK; IBK**	**Biztonsági főigazgató**
Kockázatkezelési stratégia elkészítése, frissítése	**Évente egyszer, szükség esetén haladéktalanul**	**IBF**	**ISZK; IBK; Biztonsági főigazgató**	**Kancellár**
Üzleti hatáselemzés (Business Impact Analysis – BIA) frissítése	**Évente egyszer**	**IBF**	**ISZK; IBK**	**Kancellár**
Biztonsági osztályba sorolás, EIR nyilvántartás frissítése	**Évente egyszer**	**IBF**	**ISZK; IBK Alkalmazás adatgazda**	**Kancellár**
Kockázat menedzsment keretrendszer kialakítása, működtetése	**Folyamatosan**	**IBF**	**ISZK; IBK; Biztonsági Főigazgató**	**Kancellár**
Biztonsági tesztelések tervezése	**Folyamatosan**	**ISZK**	**IBF, IBK; Biztonsági Főigazgató**	
Biztonsági tesztelések végzése - jegyzőkönyvezés	**Folyamatosan**	**ISZK**	**IBF, IBK; Biztonsági Főigazgató**	
Szakmai csoportokkal való kapcsolattartás	**Folyamatosan**	**IBF**	**ISZK**	**Biztonsági főigazgató**

8.2 Információbiztonságot érintő erőforrások

Az ***Egyetem*** beépíti az információbiztonsági célok végrehajtásához és fejlesztéséhez szükséges erőforrásokat az éves költségvetés tervezésébe és beruházási kérelmeibe, és biztosítja az információbiztonsági célok végrehajtásához és fejlesztéséhez az ***Egyetem*** vezetése által jóváhagyott forrásokat.

8.3 Intézkedési terv és mérföldkövei

Az ***Egyetem*** kockázatkezelési folyamatának részeként biztosítja, hogy az információbiztonság és az ellátási lánc kockázatkezelése, valamint a kapcsolódó egyetemi ***EIR***-ek intézkedési tervei:

- ki legyenek dolgozva és karban legyenek tartva;
- dokumentálják a helyreállító információbiztonsági és ellátási lánc kockázatkezelési intézkedéseket, a kockázatelemzési eljárásrendjében megfogalmazottak szerint, annak érdekében, hogy megfelelően reagáljanak az egyetemi műveletek és eszközök, személyek, más szervezetek kockázataira;
- a meghatározott jelentési követelmények bemutatásra kerüljenek.

Amennyiben az ***Egyetem*** az adott ***EIR***-jére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, akkor a vizsgálatot követően haladéktalanul intézkedési tervet kell készítenie a számára előírt biztonsági osztály elérésére vagy hiányosságok megszüntetésére.

Az ***Egyetem*** biztosítja, hogy az intézkedési tervek és mérföldkövek összhangban álljanak az egyetemi kockázatmenedzsment stratégiával és a kockázatkezelési intézkedések egyetemi szintű prioritásaival.

8.4 *EIR*-ek nyilvántartása és rendszerelem leltár

Az ***IBK*** létrehozza és felülvizsgálja az ***EIR***-ek nyilvántartását: az ***Egyetem EIR***-jeiben bekövetkező változások esetén (pl. új rendszer bevezetése, meglévő rendszer kivezetése); de legalább negyedévente.

El kell készíteni az információs vagyonelemek felmérését a kritikus adatvagyon-elemekről (ideértve az információkat, iratokat, adatkezelő alkalmazásokat, rendszereket, eszközöket), és a nyilvántartást napra készen kell tartani.

El kell készíteni továbbá a szoftver adatvagyon leltárt, ami az üzleti hatáselemzések elvégzésével (***BIA***) és az arra épülő információk felhasználásával az információbiztonsági sérülékenységek, biztonsági rések feltárását, azok kezelését, kockázatkezelés kidolgozását teszik lehetővé.

A szoftver adatvagyon felmérés, nyilvántartás és a bevallott adatok feldolgozása az ***IBK*** feladata.

Szoftver adatvagyon bevallásra minden munkaszervezeti egység kötelezett, aki saját fejlesztésű, egyetemi fejlesztésű, vagy vásárolt szoftver termék támogatásával végzi tevékenységét.

8.5 Biztonsági teljesítmény mérése

A biztonsági teljesítmény mérésének részleteit a „**Felügyeleti stratégia**” és a „**Biztonságértékelési terv**” című dokumentumok tartalmazzák. A terv alapján tett megállapításokat dokumentált formában az ***IBF*** készíti el rendszeresen, de legalább évente. Az elkészült jelentéseket a Biztonsági főigazgató valamint az ***ISZK*** Igazgató részére adja át.

A biztonsági teljesítmény mérése dokumentált mérési módszertannal történik, amely kiterjed a biztonsági események utáni feltáró vizsgálatok eredményeiről és az elvégzett sérülékenység vizsgálatok által feltárt kritikus megállapítások értékelésére. A biztonsági teljesítményt a biztonsági események elemzésével és az elvégzett sérülékenység vizsgálatok kritikus megállapításaival kell értékelni.

8.6 *Egyetemi* architektúra

Az ***Egyetem*** kifejleszti és fenntartja az egyetemi szervezeti rendszert, amely tekintettel van mindazon információbiztonsági kockázatokra, amelyek hatással lehetnek az ***Egyetem*** működésére, az eszközökre, az egyénekre és más szervezetekre.

8.7 Az *Egyetem* működése szempontjából kritikus infrastruktúra biztonsági terve

Az ***Egyetem***, az ***Egyetem*** működése szempontjából kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági tervének kidolgozása, dokumentálása és frissítése során kezeli az információbiztonsági kérdéseket. A kapcsolódó információkat, a Rendszerbiztonsági terv dokumentumok tartalmazzák.

8.8 Kockázatmenedzsment stratégia

Az ***Egyetem*** elkötelezett az ***EIR***-ek működéséből és használatából eredő biztonsági kockázatok kezelésében, amelynek érdekében, egy átfogó és egységes információbiztonsági kockázatmenedzsment stratégiát kell kidolgozni. Az ***Egyetem*** számára kiemelt fontosságú, hogy az információbiztonság a működési folyamatok szerves része legyen.

Az ***Egyetem*** a kockázatkezelési stratégiát az egész struktúrájában egységesen alkalmazza, beleértve a különböző szervezeti egységeket és folyamatokat. A stratégia hatékonyságának biztosítása érdekében azt rendszeresen, az ***Egyetem*** által meghatározott gyakorisággal, valamint jelentős egyetemi változások esetén az ***IBF*** felülvizsgálja és frissíti. A stratégia végrehajtása során az ***Egyetem*** célja, hogy a jogszabályi előírásoknak és a nemzetközi legjobb gyakorlatoknak megfelelően minimalizálja a kockázatokat, és egy megbízható, biztonságos információs környezetet teremtsen.

8.9 Engedélyezési folyamatok meghatározása

Az ***Egyetem*** egyes engedélyezési folyamatait az ***IBIR*** dokumentációiban (szabályzatok, eljárásrendek, stratégiák, rendszer dokumentációk stb.) dokumentálja, míg kifejezetten a kockázatmenedzsment folyamatok felelőseit a „KOCKÁZATELEMZÉSI ÉS KOCKÁZATKEZELÉSI ELJÁRÁSREND” dokumentum határozza meg.

8.10 Szervezeti működés és üzleti folyamatok meghatározása

Az ***Egyetem*** a ***BIA*** során határozza meg az ***Egyetem*** legjobb gyakorlatnak megfelelő működési folyamatait és a kapcsolódó ***EIR***-eket, valamint a folyamatok és így az egyes rendszerek kritikusságát. Ezen elemzés, illetve a kockázatelemzés az alapja a biztonsági osztályba sorolásnak, mely végül meghatározza az információbiztonság követelményrendszerét.

Az Üzleti hatáselemzés frissítéséért a rendszerek változása esetén - vagy teljesen, vagy részben – az ***IBK*** Igazgatója felel az illetékes üzleti alkalmazás adatgazda bevonása mellett.

8.11 Biztonsági személyzet képzése

8.11.1 A folyamatos működésre felkészítő képzés

Az ***Egyetem*** az ***EIR*** folyamatos működésére felkészítő képzést tart a felhasználóknak, szerepkörüknek és felelősségüknek megfelelően:

- szerepkörbe vagy felelősségbe kerülésüket követő 30 munkanapon belül;
- a folyamatos működésre felkészítő képzésben szimulált eseményeket kell alkalmazni, hogy elősegítse a személyzet hatékony reagálását a kritikus helyzetekben;
- a képzéseket évente el kell végezni az ***EIR*** mindenkori állapotának megfelelően.

8.11.2 Képzés a biztonsági események kezelésére

Az ***Egyetem*** biztonsági eseménykezelési képzést biztosít az ***EIR*** felhasználóinak a számukra kijelölt szerepköröknek és felelősségnek megfelelően:

- szerepkörbe vagy felelősségbe kerülésüket követő 30 munkanapon belül;
- a képzéseket évente el kell végezni az ***EIR*** mindenkori állapotának megfelelően, vagy amikor az ***EIR*** változásai megkívánja.

8.11.3 Az informatikai biztonsági oktatás és képzés

A jelen szabályzat személyi hatálya alá tartozó személyeket – feladatának és jogkörének figyelembevételével – megfelelő képzésben kell részesíteni az ***Egyetem*** biztonsági szabályairól és

eljárásairól. Ezeket az ismereteket rendszeresen naprakész ismeretek közlésével fel kell újítani. A képzés magában foglalja a:

- a biztonsági követelményeket;
- a jogi felelősséget;
- az ***Egyetem*** óvintézkedéseit;
- az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát;
- a fenyegetések felderítését szolgáló szervezeten belüli és szervezetek közötti információmegosztási képességet;
- általános biztonságtudatossági ismereteket, illetve a kiberbiztonsági tudatosságon alapuló helyes viselkedési szabályokat.

Az általános képzést azelőtt kell lefolytatni, mielőtt a belépők megkapnák a hozzáférési jogot (hivatalos levelezési postafiók kivételével) az informatikai rendszerekhez vagy az adatokhoz. A képzés elvégzéséhez szükséges információk az új belépők levelezési címére kerülnek kiküldésre határidő megjelölésével együtt.

A biztonságtudatossági képzés az érintett személyeket felkészíti a belső fenyegetések felismerésére, a pszichológiai manipuláció és adatgyűjtés lehetséges és valós jeleinek felismerésére, valamint felkészíti azok jelentésére.

Az informatikai biztonsággal foglalkozó személyek részére, szerepkör alapú információbiztonsági képzést szükséges tartani. A biztonsági képzés mélységének az ***Egyetemen*** belüli általános fontosságához kell igazodnia, és az adott szerep biztonsági követelményeinek megfelelően kell változnia. Amennyiben szükséges, sokkal széleskörűbb oktatást is biztosítani kell. Informatikai biztonsági képzési programot kell kialakítani az összes biztonsághoz kapcsolódó igény lefedésére. A képzési eljárásrendet rendszeresen felül kell vizsgálni, és körülmények, rendszer változásával frissíteni.

A különleges biztonsági képzésre küldendő alkalmazottak kiválasztásakor a következőket kell figyelembe venni:

- az informatikai rendszerek tervezésében és fejlesztésében kulcsszerepet játszó alkalmazott, informatikai rendszerek üzemeltetésében kulcsszerepet játszó alkalmazott;
- szervezeti, projekt és rendszerszintű Informatikai Vezető;
- a biztonság adminisztrációjáért felelős személy, például a hozzáférés ellenőrzés vagy a címtár kezelés területén.

Minden esetben ellenőrizni kell, hogy a tevékenységekhez szükséges-e különleges biztonsági képzés. A lefolytatott képzéseken készült jelenléti íveket vagy digitális naplót, valamint a kapcsolódó tematikát 5 évig meg kell őrizni.

A képzések szervezéséről és megtartásáról részleteket a „*TUDATOSSÁG ÉS KÉPZÉS ELJÁRÁSREND*" dokumentum tartalmaz.

A biztonsági képzésre vonatkozó dokumentációk

Az információbiztonsági képzésen történő részvételt alá kell íratni, vagy digitális tanúsítvány formában el kell fogadtatni a résztvevőkkel. Az aláírt dokumentumokat / online képzési naplókat, 5 évig meg kell őrizni.

8.12 Tesztelés, képzés és felügyelet

Az egész ***Egyetemre*** kiterjedő biztonsági tesztelési, képzési és felügyeleti folyamat segít biztosítani, hogy a vezetők mindig tisztán lássák a tesztelési, képzési és felügyeleti tevékenységek aktuális állapotát, és lehetőségük nyíljon arra, hogy ezeket a tevékenységeket összehangoltan kezeljék.

A folyamatos felügyeleti folyamatok növekvő fontosságával, az információbiztonsági védelmi intézkedések megvalósításával a kockázatelemzések alapján, valamint az egész ***Egyetemre*** kiterjedő

biztonsági követelmények széles körű használatával az ***Egyetem*** összehangolja és konszolidálja a különböző biztonsági követelmények megvalósulását támogató folyamatos értékelések részeként rutinszerűen végzett tesztelési és felügyeleti tevékenységeket.

A tesztelési, képzési és felügyeleti terveket és tevékenységeket az aktuális fenyegetés- és sérülékenységi vizsgálatok eredményei alapján határozzák meg.

Mindegyik fejlesztendő, illetve beszerzendő alkalmazás, szolgáltatás esetében meg kell határozni a következőket:

- a biztonsági tesztelés folyamata;
- a biztonsági tesztelés szintjei;
- a használt tesztelési típusok;
- a használt teszttervezési technikák.

A tesztelést mindig az adott rendszer dokumentációjának megfelelően kell végrehajtani.

8.13 Szakmai csoportokkal és közösségekkel való kapcsolattartás

Az ***Egyetem*** felveszi és kialakítja a kapcsolatot a kiválasztott szakmai csoportokkal és közösségekkel (például MKIK, ISACA) annak érdekében, hogy

- elősegítse az ***Egyetemhez*** köthető személyek folyamatos biztonsági oktatását és képzését;
- naprakész információkkal rendelkezzen az ajánlott biztonsági gyakorlatok, technikák és technológiák terén;
- megossza az aktuális biztonsággal kapcsolatos információkat, beleértve a fenyegetéseket, sérülékenységeket és biztonsági eseményeket.

8.14 Fenyegetettség tudatosító program

Kapcsolódó dokumentum: „*TUDATOSSÁG ÉS KÉPZÉS ELJÁRÁSREND*”

Az ***Egyetem*** a fenyegetésekkel kapcsolatos információk megosztására fenyegetettség tudatosító programot vezet be, amely magában foglalja a fenyegetések felismerését szolgáló szervezeten belüli és szervezetek közötti információmegosztási képességet.

9. Kockázatmenedzsment keretrendszer

Az ***IBF*** által kialakított Kockázatmenedzsment keretrendszer fő komponense a „*KOCKÁZATELEMZÉSI ÉS KOCKÁZATKEZELÉSI ELJÁRÁSREND*”, mely definiálja a kockázatmenedzsment feladatokat és felelősségeket.

9.1 Kockázatkezelésért felelős szerepkörök

Az ***Egyetem*** a Kockázatelemzési és kockázatkezelési eljárásrendben meghatározza az információbiztonsági kockázatok kezelésével kapcsolatos feladatokat és kijelöli a felelős személyeket. Az ***Egyetem*** információbiztonsági kockázatkezelésért felelős vezetője az IBF, aki biztosítja a kockázatok egyetemi szintű áttekintését és elemzését, valamint a kockázatmenedzsment ***Egyetemen*** belüli egységes működését.

9.2 Ellátási lánc kockázatmenedzsment stratégiája

Az ***IBF*** által kialakított Kockázatmenedzsment keretrendszeren belül kezeli az ellátási láncra vonatkozó kockázatokat.

Az ellátási lánccal kapcsolatos kockázatkezelés szabályait a „KOCKÁZATELEMZÉS ÉS KOCKÁZATKEZELÉSI ELJÁRÁSREND” tartalmazza, mely definiálja a kockázatmenedzsment feladatokat és felelősségeket. Az ellátási lánc kockázatkezelési stratégiája megegyezik az általános kockázatmenedzsment stratégiával.

Az eljárásrend tartalmazza az ***Egyetem*** kockázatkezelési stratégiájának céljait, amely az ***Egyetemre*** ható biztonsági és adatvédelmi kockázatok azonosítására, értékelésére, kezelésére és nyomon követésére irányul. Részletesen bemutatja a kockázatkezelés konkrét céljait és feladatait, mint az éves

kockázatértékelés, az incidenskezelési képesség fejlesztése, a biztonságtudatosság növelése, az adatvédelmi intézkedések erősítése, valamint a biztonsági tesztelések végrehajtása.

9.3 Folyamatos felügyeleti stratégia

A folyamatos felügyelet stratégiai célja, hogy az ***Egyetem*** biztosítsa információs rendszereinek és adatainak magas szintű biztonságát a ***Kiberbiztonsági tv.*** előírásainak megfelelően. A stratégia pontos tartalmát a „**Felügyeleti stratégia**" című dokumentum tartalmazza.

10.Hozzáférés-felügyelet

Kapcsolódó dokumentum: „*HOZZÁFÉRÉS FELÜGYELET ELJÁRÁSREND*" c. dokumentum

Az ***Egyetem*** hozzáférés felügyeleti szabályait szervezeti és folyamat, valamint rendszerszinten egy különálló dokumentumban határozta meg, mely tartalmazza a „*HOZZÁFÉRÉS FELÜGYELET ELJÁRÁSREND*" célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal, ajánlásokkal, valamint az ***Egyetem*** belső szabályzataival, és meghatározza a Hozzáférés felügyelet eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend rendelkezik a felhasználói fiókok kezelésének részletes szabályozásáról, beleértve az új fiókok létrehozását, a jogosultságkezelési feladatokat, a fiókok karbantartását, az ideiglenes hozzáférések kontrollját, valamint a használaton kívüli fiókok, illetve egyéb szükséges fiókok letiltását. Kezelni szükséges az automatizált eszközök alkalmazását a fiókkezelési folyamatokban, különös hangsúlyt helyezve az ideiglenes és vészhelyzeti hozzáférések gyors és biztonságos kezelésére. Az eljárásrend előírja az érintett folyamatok rendszeres ellenőrzését és az esetleges visszaélések megelőzésére irányuló intézkedések bevezetését is, az egyetemi integritás és az erőforrások biztonságának érdekében.

Az eljárásrend a felhasználói fiókok védelmével kapcsolatban a felhasználók kijelentkeztetését, a munkaszakaszok védelmét, a fiókkal végzett műveletek naplózását, a sikertelen bejelentkezési kísérletek maximalizálását is szabályozza. A megoldások, különböző szolgáltatást támogató ***EIR***-ek tekintetében eltérőek lehetnek, de a szabályozásnak teljes körűen eleget kell tenniük.

Az eljárásrendben kezelt egyéb témák;

- Hozzáférés szabályok érvényesítése, információmegosztás, felelősségek szétválasztása, illetve a legkisebb jogosultság elvének szabályozása;
- A rendszerhasználat jelzésének definiálása;
- Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek szabályozása;
- Távoli hozzáférés szabályozása;
- Vezeték nélküli hozzáférés szabályozása;
- Mobil eszközök hozzáférés-ellenőrzésének szabályozása;
- Külső ***EIR***-ek használatának szabályozása;
- Információmegosztás szabályai;
- Nyilvánosan elérhető tartalmak kezelésének szabályai.

11.Tudatosság és képzés

Kapcsolódó dokumentum: „*TUDATOSSÁG ÉS KÉPZÉS ELJÁRÁSREND*" c. dokumentum

Az ***Egyetem*** képzési szabályait szervezeti- és folyamat-, valamint rendszerszinten egy különálló dokumentumban határozta meg, mely tartalmazza a tudatossági és képzési eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli

együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza a Tudatossági és képzési eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend rendelkezik a biztonságtudatosság és képzések egyetemi szintű szabályozásáról, beleértve a képzési programok kidolgozását, dokumentálását, megvalósítását és rendszeres felülvizsgálatát. Meghatározásra kerülnek a célkitűzések, a hatókör, valamint a szükséges készségek és kompetenciák, amelyek biztosítják a munkavállalók biztonságtudatos viselkedését és a kockázatok kezelésére való felkészültségüket. Az eljárásrend előírja a képzések eredményességének rendszeres ellenőrzését, és az esetleges hiányosságok megszüntetésére irányuló intézkedések meghozatalát, az ***Egyetem*** biztonsági kultúrájának fejlesztése érdekében.

Információbiztonsági tudatosság növelése érdekében, és ahhoz, hogy az ***Egyetem*** munkavállalói naprakész tudással rendelkezzenek a fenyegetésekről, sebezhetőségekről, humán kockázatokról, biztonsági eseményekről és felkészülhessenek a lehetséges belső fenyegetések felismerésére, folyamatos oktatásban, képzésben kell részesüljenek.

A felhasználók biztonságtudatossági oktatását a kapcsolódó eljárásrendnek megfelelően, tudás, ismeret ellenőrzéssel kell végrehajtani.

12.Naplózás és elszámoltathatóság

Kapcsolódó dokumentum: „*NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG ELJÁRÁSREND*” c. dokumentum

Az ***Egyetem*** naplózási és elszámoltathatósági szabályait szervezeti- és folyamat-, valamint rendszerszinten különálló eljárásrendben határozta meg, mely tartalmazza a naplózásról és elszámoltathatóságról szóló eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal, ajánlásokkal, valamint az ***Egyetem*** belső szabályzataival, és meghatározza a naplózási és elszámoltathatósági eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

A következő témák kerülnek definiálásra: naplózási szabályok, naplóállományok létrehozásának, tárolásának, hozzáférésének és védelmének szabályozása. Az eljárásrend kiemeli a naplózási folyamatok rendszeres ellenőrzését, valamint az észlelt anomáliák és események dokumentálását és vizsgálatát. Fontos követelmény továbbá, hogy a naplózott adatok alapján a felelősségi körök egyértelműen megállapíthatók legyenek, elősegítve ezzel az elszámoltathatóságot és a biztonsági események hatékony kezelését.

A Naplózás és elszámoltathatóság eljárásrend szabályozza az alábbiakat:

a) Naplózandó rendszerelemek meghatározásának módja,
b) Naplózandó események köre,
c) Naplók felülvizsgálatának módja (ad-hoc vagy rendszeres, automatikus), jelentéskészítés,
d) Naplók biztonságos tárolása, védelme, megőrzése,
e) Napló tárkapacitások meghatározása.

13.Értékelés, engedélyezés és monitorozás

Kapcsolódó dokumentum: „*BIZTONSÁGÉRTÉKELÉSI TERV”, „HOZZÁFÉRÉS FELÜGYELET ELJÁRÁSREND*”, „*ÉRTÉKELÉS, ENGEDÉLYEZÉS ÉS MONITOROZÁS ELJÁRÁSREND*” c. dokumentumok

Az Értékelés, engedélyezés és monitorozás eljárásrend előírja a biztonságértékelések rendszerét, dokumentálását és rendszeres felülvizsgálatát, valamint az intézkedési terv – a szükséges elvégzendő

feladatok azonosítását - kialakításának szabályait. A meghatározott követelmények közé tartozik az egyetemi erőforrások engedélyezési folyamatainak szabályozása, amely biztosítja, hogy csak a megfelelően értékelt és jóváhagyott rendszerek és folyamatok kerülhessenek bevezetésre, valamint a külső és belső rendszerkapcsolatok, illetve információmegosztások elvárt szabályozási kereteit. Az eljárásrend továbbá kiterjed a folyamatos rendszerfelügyelet szabályaira is.

14.Konfigurációkezelés

Kapcsolódó dokumentum: „*KONFIGURÁCIÓKEZELÉSI ELJÁRÁSREND*" c. dokumentum

Az ***Egyetem*** konfigurációkezelési szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló eljárásrendben határozta meg, mely tartalmazza a konfigurációkezelési eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza a Konfigurációkezelési eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend előírja a konfigurációkezelési eljárások szabályait, dokumentálásukat és rendszeres felülvizsgálatukat. Meghatározza a konfigurációs elemek azonosításának, nyomon követésének és változáskezelésének részletes szabályait, biztosítva a változások kontrollálhatóságát és a konfigurációs állapotok pontos dokumentációját. Előírja továbbá a konfigurációs adatok rendszeres ellenőrzését, valamint az észlelt eltérések és hibák kezelésére irányuló intézkedések végrehajtását.

Az eljárásrend kiterjed az Alapkonfiguráció dokumentációk kialakítására és fenntartására, a konfigurációkezelési folyamatok szabályaira (biztonsági hatásvizsgálatok, legkisebb jogosultság elve).

A szabályozás a rendszerelem leltár kialakítására és fenntartására, valamint a rendszerelemekhez kapcsolódó konfigurációkezelési tervek kidolgozására is kiterjed, definiálja a szoftvertelepítési és szoftverhasználati korlátozásokat.

15.Készenléti tervezés (Üzletmenet-folytonosság)

Kapcsolódó dokumentum: „*KÉSZENLÉTI TERVEZÉS ELJÁRÁSREND*" c. dokumentum

Az ***Egyetem*** üzletmenet-folytonosság szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló eljárásrendben határozta meg, mely tartalmazza a készenléti tervezési eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza az Üzletmenet-folytonossági eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend előírja az üzletmenet-folytonossági és katasztrófaelhárítási tervek kidolgozását, dokumentálását és rendszeres felülvizsgálatát. Meghatározza a célkitűzéseket, a hatókört, valamint az érintett folyamatokat és felelősségi köröket. A követelmények közé tartozik a kockázati forgatókönyvek elemzése, a katasztrófahelyzetek kezelésére szolgáló intézkedések részletezése, valamint a helyreállítási gyakorlatok rendszeres végrehajtása, valamint a folyamatos működésre felkészítő képzéssel kapcsolatos elvárások.

16.Azonosítás és hitelesítés

Kapcsolódó dokumentum: „*AZONOSÍTÁSI ÉS HITELESÍTÉSI ELJÁRÁSREND*" c. dokumentum

Az ***Egyetem*** azonosítási és hitelesítési szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló eljárásrendben határozta meg, mely tartalmazza az azonosítás és hitelesítési eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen***

belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza az Azonosítási és hitelesítési eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend előírja az ***Egyetemen*** használandó azonosítási és hitelesítési szabályokat, valamint a kapcsolódó elemek dokumentálását és végrehajtását, különös tekintettel a felhasználók, rendszerek és folyamatok biztonságos azonosítására és hozzáférés-kezelésére. Meghatározásra kerülnek a felhasználói azonosítók és hitelesítési adatok létrehozásának, nyilvántartásának, módosításának, visszavonásának, valamint a többtényezős hitelesítés alkalmazásának szabályai. Az eljárásrend tartalmazza a felhasználói fiókok és privilegizált fiókok kezelési rendjét, a hozzáférés ellenőrzését, valamint a jogosultságok kiosztásának és naplózásának elveit, biztosítva a tevékenységek visszakövethetőségét. Emellett szabályozza a hitelesítési eszközök kezelésének, védelmének és visszavonásának szabályait, valamint a személyazonosság igazolásának és újra hitelesítésnek a feltételeit, biztosítva az ***EIR***-ek integritását és biztonságát.

17.Biztonsági eseménykezelés

Kapcsolódó dokumentum: „*BIZTONSÁGI ESEMÉNYEK KEZELÉSE ELJÁRÁSREND*” c. dokumentum

Az ***Egyetem*** biztonsági eseménykezelési szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló eljárásrendben határozta meg, mely tartalmazza a biztonsági eseménykezelési eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza a Biztonsági eseménykezelési eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend átfogóan meghatározza a biztonsági események kezelésének teljes életciklusát, a felismeréstől az utókövetésig. Meghatározza a biztonsági események azonosításának és osztályozásának elveit, az események súlyossági szintjeit, valamint a bejelentési kötelezettségeket az érintett egyetemi egységek és felelős személyek felé. Egyértelműen definiálja a szerepköröket és felelősségeket, biztosítva, hogy minden érintett tisztában legyen feladataival az események kezelése során.

A szabályozás továbbá részletezi a kivizsgálás folyamatát, amely magába foglalja az események okainak elemzését, a kapcsolódó rendszerek és folyamatok ellenőrzését, valamint a kockázatok és hatások felmérését. Továbbá strukturált keretet ad a biztonsági események során elvárt kommunikációs folyamatoknak, biztosítva az érintettek időben történő értesítését, valamint a helyreállítási tevékenységek megszervezését és végrehajtását, hogy minimalizálja a biztonsági események hatását a működésre és az információbiztonságra.

18.Karbantartás

Kapcsolódó dokumentum: „*KARBANTARTÁSI ELJÁRÁSREND*” c. dokumentum

Az ***Egyetem*** karbantartási szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló dokumentumban határozta meg, mely tartalmazza a karbantartási eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza a Karbantartási eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend előírja a karbantartási tevékenységek tervezésére, végrehajtására és dokumentálására vonatkozó eljárásokat, valamint a rendszeres karbantartási időszakok és eljárások meghatározását.

Rendelkezik továbbá a karbantartási folyamatok során alkalmazott eszközök, technikák és felelősségi körök pontos rögzítéséről. A szabályozás biztosítja, hogy a rendszerek működőképessége és biztonsági szintje fenntartható legyen.

19.Adathordozók védelme

Kapcsolódó dokumentum: „*ADATHORDOZÓK VÉDELME ELJÁRÁSREND*" c. dokumentum

Az ***Egyetem*** az adathordozók védelmének szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló eljárásrendben határozta meg, mely tartalmazza az adathordozók védelméről szóló eljárásrendjének célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza az Adathordozók védelmére vonatkozó eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend definiálja az adathordozók használatára, tárolására, szállítására és megsemmisítésére vonatkozó eljárásokat. Meghatározza az adathordozók azonosítására és nyilvántartására vonatkozó követelményeket, valamint a biztonsági intézkedéseket, amelyek biztosítják az adatok sértetlenségét és bizalmasságát. A szabályozás tartalmazza a jogosulatlan hozzáférés megelőzésére, a sérült vagy elavult adathordozók biztonságos megsemmisítésére, illetve újra felhasználásuk esetén az adatok teljes törlésére vonatkozó előírásokat.

20.Fizikai és környezeti védelem

Kapcsolódó dokumentum: „*FIZIKAI ÉS KÖRNYEZETI VÉDELMI ELJÁRÁSREND*" c. dokumentum

Az ***Egyetem*** fizikai védelmi szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló eljárásrendben határozta meg, mely tartalmazza a fizikai és környezeti védelem eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza a Fizikai védelmi eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend szabályozza az ***Egyetem*** fizikai védelmi intézkedéseinek kialakítását, dokumentálását és végrehajtását, amelyek célja az informatikai eszközök és adatok illetéktelen hozzáférés elleni védelme. Rendelkezik a belépési jogosultságok kezeléséről, a védett területek kijelöléséről, valamint a hozzáférési naplózás alkalmazásáról. Meghatározza továbbá a környezeti kockázatok kezeléséhez szükséges intézkedéseket, beleértve a tűzvédelem, az áramellátás, valamint az éghajlati és mechanikai hatások elleni védelmet.

21.Tervezés

Kapcsolódó dokumentum: „*BIZTONSÁGTERVEZÉSI ELJÁRÁSREND*" c. dokumentum

Az ***Egyetem*** szabályozza az ***EIR***-ek biztonsági követelményeit, meghatározva a rendszerek elemeit, működési környezetét, alapfeladatait, biztonságkritikus részeit, az ***EIR***-hez kapcsolódó felelősségi köröket, valamint az adatok bizalmasságát, sértetlenségét és rendelkezésre állását biztosító intézkedéseket. A Biztonságtervezési eljárásrend kiterjed a rendszerbiztonsági terv készítésére, felülvizsgálatára és frissítésére, az információbiztonsági architektúra leírására, a biztonsági követelmények kiválasztására és testre szabására, valamint az egyes eljárásrendekhez kapcsolódó védelmi intézkedések meghatározására. Ezen túlmenően tartalmazza a felhasználók viselkedési szabályait, az internet- és közösségi média használat korlátozásait, az elektronikus levelezés rendeltetésszerű használatát, valamint a jogosultságok kezelését és azok rendszeres felülvizsgálatát.

Az eljárásrendben definiált előírások biztosítják a biztonsági intézkedések végrehajtásának koordinációját az érintett egyetemi egységek között, fenntartva a rendszerek biztonságát és az ***Egyetem*** zavartalan működését.

22.Személyi biztonság

Kapcsolódó dokumentum: „*SZEMÉLYI BIZTONSÁG ELJÁRÁSREND*" c. dokumentum

Az ***Egyetem*** a személyi biztonság szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló eljárásrendben határozta meg, mely tartalmazza a személyi biztonsági eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza a Személyi biztonsági eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

A szabályozás előírja a munkavállalók biztonságtudatos viselkedésének támogatását, valamint a személyi biztonsági kockázatok azonosítására és kezelésére vonatkozó eljárások kidolgozását, dokumentálását és végrehajtását. Meghatározza az ***Egyetem*** munkavállalói és külső partnerei számára előírt belépési, hozzáférési, oktatási és képzési követelményeket. A szabályozás tartalmazza a személyes adatok védelmét szolgáló intézkedéseket, továbbá a felelősségi körök és a rendszeres ellenőrzési tevékenységek rögzítését.

Az eljárásrend definiálja a munkakörök biztonsági szempontú besorolásának szabályait és folyamatát, a személyek háttérellenőrzésével kapcsolatos elvárásokat, illetve a munkaviszony megszűnés, átirányítás és áthelyezés során követendő egyes szabályokat.

A külső személyekkel kapcsolatos elvárások is e szabályozásban kerülnek definiálásra.

23.Kockázatkezelés

Kapcsolódó dokumentum: „*KOCKÁZATELEMZÉSI ÉS KOCKÁZATKEZELÉSI ELJ*ÁRÁSREND" c. dokumentum

Az ***Egyetem*** kockázatkezelési szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló dokumentumban határozta meg, mely tartalmazza a Kockázatelemzési és kockázatkezelési eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza a Kockázatelemzési és kockázatkezelési eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend szabályozza a kockázatelemzési és kockázatkezelési eljárásmódok kidolgozását, dokumentálását és végrehajtását, valamint az ***Egyetem*** információbiztonsági kockázatainak azonosítását, értékelését és kezelését. Meghatározza a kockázatkezelési stratégiák kialakításának és alkalmazásának követelményeit, beleértve a kockázatok nyomon követését, rendszeres felülvizsgálatát és az intézkedések hatékonyságának ellenőrzését.

24.Rendszer- és szolgáltatásbeszerzés

Kapcsolódó dokumentum: „*RENDSZER ÉS SZOLGÁLTATÁSBESZERZÉSI ELJÁRÁSREND*" c. dokumentum

Az ***Egyetem*** beszerzési szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló dokumentumban határozta meg, mely tartalmazza a rendszer- és szolgáltatásbeszerzési eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és

ajánlásokkal, és meghatározza a beszerzési eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend szabályozza az informatikai beszerzési folyamatokat, különös tekintettel a biztonsági követelmények figyelembevételét a rendszerek és szolgáltatások kiválasztása során. Meghatározza a beszerzési igények elemzésére, a szolgáltatók értékelésére, valamint a szerződésekben rögzítendő biztonsági elvárásokra vonatkozó előírásokat, ideértve a funkcionális és garanciális biztonsági követelmények teljesítéséhez szükséges védelmi intézkedések dokumentálását és ellenőrzését. Az eljárásrend definiálja a biztonságtervezési alapelveket, illetve a fejlesztéssel, a fejlesztői teszteléssel, változáskövetéssel kapcsolatos egyetemi elvárásokat.

25.Rendszer- és kommunikációvédelem

Kapcsolódó dokumentum: „*RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELMI ELJÁRÁSREND*” c. dokumentum

Az ***Egyetem*** rendszer- és kommunikációvédelmi szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló eljárásrendben határozta meg, mely tartalmazza a rendszer- és kommunikációvédelmi eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza a Rendszer- és kommunikációvédelmi eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend definiálja a kapcsolódó folyamatok dokumentálásának és végrehajtásának elvárásait, amelyek biztosítják az egyetemi információs rendszerek és kommunikációs csatornák biztonságát. Meghatározza a hálózati forgalom figyelésére, az adatok titkosítására, valamint a jogosulatlan hozzáférések megelőzésére vonatkozó követelményeket. A szabályozás előírja továbbá a kommunikációs infrastruktúrák védelmét szolgáló technikai és egyetemi intézkedések alkalmazását, valamint a kapcsolódó folyamatok rendszeres ellenőrzését.

Az eljárásrend olyan témákat kezel, mint:

- Rendszer és felhasználói funkciók szétválasztása és elkülönítése,
- Tárolt adatok védelme / információk az osztott használatú rendszererőforrásokban,
- Szolgáltatásmegtagadással járó támadások elleni védelem,
- A határok védelme / a hálózati kapcsolat megszakítása,
- Az adatátvitel bizalmassága és sértetlensége / folyamatok elkülönítése,
- Kriptográfiai védelem,
- Együttműködésen alapuló informatikai eszközök, (Pl. kamerák, mikrofonok)
- Tanúsítványok használata,
- Biztonságos név/cím feloldási szolgáltatás,
- Mobilkód használat, (Pl. Olyan szoftver (pl. < JavaScript, < Java appletek), ami távoli rendszerekről töltődik le és települ a felhasználó gépére, például weboldalak tartalmának futtatásához)
- Munkaszakasz hitelessége. (Pl. egyedi munkamenet azonosítók kezelése)

26.Rendszer- és információsértetlenség

Kapcsolódó dokumentum: „*RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉGI ELJÁRÁSREND*” c. dokumentum

Az ***Egyetem*** rendszer- és információsértetlenség szabályait szervezeti- és folyamat, valamint rendszerszinten egy különálló eljárásrendben határozta meg, mely tartalmazza a rendszer- és információsértetlenségi eljárásrend célkitűzését, a hatókörét, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az ***Egyetemen*** belüli együttműködés kereteit és a megfelelőségi

kritériumokat. A szabályozás összhangban van az ***Egyetemre*** vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal, és meghatározza a Rendszer- és információsértetlenségi eljárásrend kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felelőst.

Az eljárásrend technikai részleteiben meghatározza az informatikai rendszerek integritásának és bizalmasságának megőrzéséhez szükséges eljárásokat és intézkedéseket. Ezek közé tartozik az adatok sértetlenségének ellenőrzésére szolgáló technológiák, a rendszerek naplózásának és monitorozásának bevezetése, valamint a naplóállományok biztonságos tárolása és rendszeres elemzése.

Az eljárásrend ezeken kívül olyan témákat fed le, mint hibajavítás, kártékony kód védelem, kártékony levélszemét elleni védelem, szoftver sértetlenség védelme és bemeneti információk védelme.

27.Ellátási lánc kockázatkezelése

Kapcsolódó dokumentum: „*ELLÁTÁSI LÁNC KOCKÁZATKEZELÉSI ELJÁRÁSREND*” c. dokumentum

Az ***Egyetem*** ellátási láncra vonatkozó kockázatkezelési szabályait szervezeti- és folyamat, valamint rendszerszinten a Kockázatelemzés és kockázatkezelési eljárásrend részeként határozta meg.

Az eljárásrend előírja az ellátási láncban részt vevő partnerek és szolgáltatók kockázatainak azonosítását, elemzését és kezelését. Meghatározza az ellátási lánc szereplőinek biztonsági követelményeit, beleértve a szerződésekben rögzített biztonsági elvárásokat, a beszállítói auditokat, valamint a partnerek teljesítményének rendszeres értékelését.

28.Mesterséges intelligencia alkalmazásának információbiztonsági szabályai

28.1 A Mesterséges Intelligencia használatának alapelvei

Az ***Egyetem***, a mesterséges intelligenciával (a továbbiakban: ***MI***) kapcsolatos tevékenységet, a „***Mesterséges intelligencia intézményi elveiről és etikus használatáról a Debreceni Egyetemen***” szabályzatában szabályozza.

A felügyeletet a ***MI*** Bizottság (MIB) gyakorolja.

Jelen fejezet, az ***MI*** használatára vonatkozó biztonsági kérdések tekintetében fogalmaz meg elvárásokat.

Az ***Egyetem*** minden ***MI***-vel kapcsolatos tevékenységét az alábbi, nemzetközi normákon és legjobb gyakorlatokon alapuló alapelvek vezérlik. Minden munkavállalónak ezen elvek szellemében kell eljárnia.

Információbiztonság és adatvédelem: az ***Egyetem***, ügyfelei és partnerei adatainak védelme a legmagasabb prioritás. Szigorúan tilos személyes adatokat, üzleti titkot, bizalmas ügyfél-információkat vagy védett forráskódot nem biztonságos, nyilvános ***MI***-modellekbe bevinni. Az adatkezelésnek mindenkor meg kell felelnie a beépített és alapértelmezett adatvédelem (privacy by design and by default) elveinek.

Felelősségvállalás és elszámoltathatóság: bár az ***MI*** képes komplex feladatok elvégzésére, a végső felelősség az általa generált tartalomért, annak pontosságáért, minőségéért és következményeiért mindig az azt felhasználó munkavállalót terheli.

28.2 Engedélyezett felhasználási módok

A jóváhagyott ***MI*** eszközök az alábbi, nem kimerítő jellegű feladatokra használhatók, az ***IBSZ*** többi pontjában foglalt korlátozások figyelembevételével:

- Kreatív és koncepcionális támogatás, ötletelés (brainstorming), új perspektívák és megoldási javaslatok generálása.
- Kutatás és információfeldolgozás, nyilvánosan elérhető információk felkutatása, összefoglalása, elemzése és rendszerezése. A munkavállaló felelőssége a források és a tényállítások pontosságának ellenőrzése.

- Tartalomelőállítás (a munkavállaló felelős az előállított tartalomért)
    - Belső és külső kommunikációs anyagok (pl. e-mailek, hírlevelek, blogposztok, közösségi média bejegyzések) vázlatainak elkészítése.
    - Marketing- és értékesítési szövegek generálása.
    - Prezentációk és képzési anyagok tartalmának összeállítása.
    - Technikai dokumentáció, felhasználói kézikönyvek és API leírások egyes részeinek megfogalmazása.
- Szoftverfejlesztés támogatása, a vonatkozó különös szabályok betartásával kódrészletek generálása, kódoptimalizálás, hibakeresés és -javítás, tesztesetek generálása.
- Vizuális tartalmak létrehozása, prezentációkhoz, belső anyagokhoz vagy marketing kampányokhoz illusztrációk, grafikák, diagramok generálása. Minden ***MI*** által generált vizuális elemet egyértelműen meg kell jelölni.
- Adatelemzés, nagy mennyiségű, anonimizált vagy nem érzékeny adathalmazok mintázatainak feltárása, trendek azonosítása és összefoglaló riportok készítése.

28.3 Tiltott és szigorúan korlátozott felhasználás

Az ***MI***-eszközök használata során az alábbi tevékenységek szigorúan tilosak. Ezen szabályok megsértése súlyos fegyelmi következményekkel jár.

Abszolút tiltott tevékenységek (az AI Act alapján):

- Tudatküszöb alatti, manipulatív vagy megtévesztő technikák alkalmazása, amelyek célja a személyek viselkedésének torzítása oly módon, hogy az fizikai vagy pszichológiai ártalmat okozhat.
- A munkavállalók, ügyfelek vagy bármely más személy kor, fogyatékosság vagy gazdasági helyzet miatti sebezhetőségének kihasználása.
- Hatóságok általi, általános célú társadalmi pontozórendszerek (social scoring) alkalmazásában való közreműködés.
- Érzelmek felismerésére szolgáló rendszerek használata munkahelyi vagy oktatási környezetben, kivéve, ha az orvosi vagy biztonsági okokból elengedhetetlen.
- Az ***Egyetem*** belső szabályozása alapján tiltott tevékenységek:
- Bizalmas információk bevitelének tilalma, szigorúan tilos bármilyen, bizalmas információt, illetve az alább felsorolt adatot nem jóváhagyott, különösen nyilvánosan elérhető, az ***Egyetemmel*** szerződéses viszonyban nem álló MI-szolgáltató rendszerébe bevinni (akár prompt, akár állomány feltöltés formájában):
    - Személyes adat, bármely, a GDPR 4. cikk (1) bekezdése szerinti személyes adat (pl. név, e-mail cím, telefonszám).
    - Üzleti titok és védett know-how, az ***Egyetem*** vagy ügyfelei üzleti titoknak minősülő információi, beleértve a nem publikus pénzügyi adatokat, üzleti terveket, marketing stratégiákat, belső eljárásrendeket.
    - Ügyféladat, bármely, az ***Egyetem*** ügyfeleitől származó bizalmas információ, projektadat vagy adatbázis.
    - Védett forráskód, a vállalat vagy ügyfelei tulajdonát képező, nem nyílt forráskódú szoftverek forráskódja, algoritmusai, adatbázis sémái, API kulcsai és egyéb hozzáférési adatai.
- Foglalkoztatási döntések, tilos ***MI***-rendszert használni a munkavállalókkal vagy állásra jelentkezőkkel kapcsolatos döntések meghozatalára vagy előkészítésére, beleértve a toborzást, kiválasztást, teljesítményértékelést, előléptetést, fegyelmi eljárást vagy a munkaviszony megszüntetését. Az ilyen rendszerek használata az AI Act szerint magas kockázatúnak minősül, és szigorú feltételekhez kötött.
- Saját eredeti munkaként való feltüntetés, tilos az ***MI*** által teljes egészében vagy jelentős részben generált munkát (szöveget, kódot, vizuális anyagot) saját, eredeti szellemi alkotásként feltüntetni vagy benyújtani.

28.4 Felelősség, átláthatóság és dokumentáció

A munkavállaló közvetlenül felelős az általa használt ***MI***-eszközök által generált kimenet kritikájáért, ellenőrzéséért, és a végső munkatermékbe való beépítéséért. A munkavállaló nem hivatkozhat az ***MI*** "hibájára" a pontatlan, jogsértő vagy az ***Egyetem*** irányelveivel ellentétes tartalomért.

Az ***Egyetem*** felelőssége, hogy biztosítsa a biztonságos és jogszerű működés kereteit. Ez magában foglalja a megfelelő, biztonságos eszközök beszerzését, a jelen ***IBSZ*** kidolgozását és naprakészen tartását, a munkavállalók kötelező képzését, valamint a megfelelőség ellenőrzését.

28.5 Átláthatósági kötelezettségek

A külső és a belső kommunikációban egyértelműen jelölni kell, ha egy feladat elvégzéséhez vagy egy anyag elkészítéséhez jelentős mértékben ***MI***-t vettek igénybe.

Interakció jelzése, amennyiben egy ügyfél vagy külső felhasználó egy ***MI***-rendszerrel (pl. chatbot) lép interakcióba, erről egyértelműen és előzetesen tájékoztatni kell.

Minden, az ***Egyetem*** által publikált, mesterséges intelligencia által generált vagy jelentősen módosított tartalmat (szöveg, kép, hang, videó – ún. "deepfake") egyértelműen és felismerhetően meg kell jelölni (pl. vízjel, lábjegyzet).

28.6 Forrásmegjelölési és dokumentációs követelmények

Minden olyan belső dokumentumban, prezentációban vagy forráskódban, amely ***MI*** által generált elemeket tartalmaz, fel kell tüntetni a felhasznált ***MI***-eszköz nevét és lehetőség szerint a verziószámát. Ez nemcsak a szellemi munka tisztaságát szolgálja, hanem segít az esetlegesen felmerülő hibák vagy jogi problémák forrásának azonosításában is.

28.7 Irányítás, felügyelet és kockázatkezelés (AI Governance)

A Jóváhagyott *MI* rendszerek listája

Az ***Egyetemen***, kizárólag a hivatalosan jóváhagyott ***MI***-eszközök és -platformok használhatók munkavégzés céljából. A jóváhagyott eszközök naprakész listáját, az ***MI***-eszköz-nyilvántartást az IBK vezeti.

Az *MI* jártasság növelése

A munkavállalók megfelelő képzése és a folyamatos tudatosságnövelés a hatékony ***MI*** használat alapfeltétele.

Kötelező alapképzés

Minden új belépő munkavállaló számára kötelező egy ***MI***-tudatossági képzésen részt venni, amely bemutatja a jelen ***IBSZ*** legfontosabb pontjait, a főbb kockázatokat (különös tekintettel az adatvédelemre és a szellemi tulajdonra) és a felelős használat alapelveit.

Éves ismétlő képzés

Minden munkavállaló számára évente kötelező egy frissítő képzés, amely a technológiai és jogszabályi változásokra, valamint az elmúlt időszakban tapasztalt belső vagy külső incidensek tanulságaira fókuszál, és szól a dokumentum generálás és egyéb tervezési folyamatok során az ***MI*** rendszerek biztonságos, jogszerű és szakszerű használatáról.

29.Záró rendelkezések

1. Jelen szabályzatot a Debreceni Egyetem szenátusa a 2026. március 19. napján tartott ülésén, a 10/2026. (III. 19.) számú határozatával fogadta el. A szabályzat 2026. Március 20. napon lép hatályba. A szabályzat hatálybalépésével egyidejűleg a Szenátus 24/2022 (IV. 28.) számú határozatával elfogadott, korábban érvényben volt Információbiztonsági Szabályzat hatályát veszti.
2. Az elfogadást követő módosításokat lábjegyzetek jelzik.

30.Függelékek

Eljárásrendek
Adathordozók védelme eljárásrend
Azonosítás és hitelesítési eljárásrend
Biztonsági események kezelése eljárásrend
Biztonságtervezési eljárásrend
Ellátási lánc kockázatkezelési eljárásrend
Értékelés, engedélyezés és monitorozás eljárásrend
Fizikai és környezeti védelmi eljárásrend
Hozzáférés-felügyelet eljárásrend
Karbantartási eljárásrend
Készenléti tervezés (Üzletmenet-folytonossági) eljárásrend
Kockázatelemzési és kockázatkezelési eljárásrend
Konfigurációkezelési eljárásrend
Naplózás és elszámoltathatóság eljárásrend
Rendszer- és információsértetlenségi eljárásrend
Rendszer- és kommunikációvédelmi eljárásrend
Rendszer- és szolgáltatásbeszerzési eljárásrend
Személyi biztonság eljárásrend
Tudatosság és képzés eljárásrend
Eljárásrendhez kapcsolódó szabályozók
Biztonságértékelési terv
Felügyeleti stratégia
Kockázatkezelési stratégia, Kockázatelemzési módszertan

1. számú melléklet - Információbiztonsági Politika

Az ***Egyetem*** vezetése elkötelezett, hogy az ***Egyetem*** a működése és nyújtott szolgáltatásai területén a partnerei, ügyfelei és saját adatai védelmét, és az érdekelt felek információbiztonsági elvárásainak való folyamatos megfelelést meghatározó elemként kezeli. Az ***Egyetem*** által kezelt adatok és információk összessége kiemelt értéket képviselő vagyonelem, melyet védeni kell a különböző fenyegetések ellen, ezért az ***Egyetem*** törekszik, hogy e vagyonelemek tekintetében is időben állandóan megvalósuljon annak bizalmassága, sértetlensége, rendelkezésre állása.

Az ***Egyetem*** által nyújtott szolgáltatásokat magas színvonalon, modern és biztonságosan működő technológiával nyújtja, ahol felügyelt információbiztonsági folyamatokkal biztosítja a kezelt adatok, információk sértetlenségét, bizalmasságát és rendelkezésre állását.

Üzletmenet folytonosságának biztosítása és alapfeladatainak zavartalan ellátása érdekében minden szükséges információ- és adatvédelmi intézkedést megtesz, adatkezelési, információvédelmi folyamatait az adatvédelmi az információbiztonsági elvárásoknak megfelelően alakítja ki.

Az ***Egyetem*** működése és az általa nyújtott szolgáltatások teljesítése során elkötelezett a vonatkozó törvényi, valamint az irányadó szabványokban foglalt előírásoknak való maximális megfelelés iránt, így különösen a ***Kiberbiztonsági tv.*-ben** és a Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló 418/2024. (XII.23.) Korm.rendeletben, továbbá a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló 7/2024. VI. 24. MK rendeletben megfogalmazott irányelveknek, meghatározott iránymutatásoknak való megfelelés iránt, azáltal, hogy magára nézve a hivatkozott törvényeket és szabványokat kötelezően alkalmazandónak ismeri el.

Az ***Egyetem*** vezetése az ***IBP***-ben megfogalmazott elvek és követelmények teljesítését várja el az ***Egyetem*** összes munkatársától, beszállítóitól és minden egyéb érdekelt féltől. Az ***IBP*** hatálya kiterjed az ***Egyetem*** valamennyi folyamatára és szervezeti egységére, így különösen az ***Egyetem EIR***-jeire, mely magában foglalja az adathordozókat, alkalmazásokat, szoftvereket, hardver elemeket, a környezeti infrastruktúra elemeit és objektumait, a papír alapú dokumentumokat, továbbá minden eljárására, melyek hatással lehetnek az ***Egyetem*** adatvagyonára.

Az ***Egyetem*** információbiztonságának folyamatos magas színvonalú fenntartása érdekében az alábbi alapelvek figyelembevételével ***IBIR***-t vezet be és üzemeltet.

Az ***IBIR*** célja, hogy biztosítsa az ***Egyetem*** kezelésében lévő adatvagyon bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az ***EIR***-ek elemeinek sértetlenségét és rendelkezésre állását veszélyeztető, mindenkori fenyegetések kockázataival arányos, zárt, teljes körű és folyamatos, a rendszerek teljes életciklusára kiterjedő védelmét logikai, fizikai és adminisztratív védelmi intézkedések bevezetésével.

Az ***Egyetem*** az információbiztonság területén az alábbi alapelveket érvényesíti:

1. **Bizalmasság:** az ***EIR***-ben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
2. **Sértetlenség:** a tárolt adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség), a származás ellenőrizhető, megállapítható (letagadhatatlanság), illetve az ***EIR*** elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az ***EIR*** eleme rendeltetésének megfelelően használható.
3. **Rendelkezésre állás:** az ***EIR***-ek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók.

4. **A védelem teljes körűsége:** az erre vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén a következő három dimenzióban kell érvényesíteni:
    a) az összes rendszerelemre;
    b) a rendszerek architektúrájának összes rétegére mind az informatikai infrastruktúra, mind az alkalmazások szintjén;
    c) a központi, illetve a végponti informatikai eszközökre és környezetükre.
5. **A védelem zártsága:** az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedés végrehajtása megtörténik, és azok összességükben szabályozott és szerves egészet alkotnak.
6. **A védelem kockázatarányossága:** a védelem mértéke és költségei a felmért kockázatokkal arányosak. Cél a szükséges és elégséges védelmi költséggel elért maximális védelmi képesség.
7. **A védelem folyamatossága:** a kialakított védelmi intézkedések az időben állandóan változó biztonsági környezet és viszonyok mellett is megszakítás nélkül fennállnak a rendszer teljes életciklusa alatt.

Az *IBP* célja

a) Az ***Egyetem*** informatikai rendszerei által kezelt információk hitelességének, sértetlenségének, rendelkezésre állásának, funkcionalitásának megőrzésére és fenntartására irányuló intézkedések bevezetése.
b) Az ügyfél, partneri, munkatársi, szerződéses, és egyéb üzleti információk bizalmasságának megőrzése, különös tekintettel az ügyfelek bizalmas adatainak biztonságos kezelésére.
c) Az ügyfeleknek biztosított szolgáltatások jól definiált és magas minőségű információbiztonságának folyamatos biztosítása.
d) Az alkalmazott támogató informatikai, illetve információtechnológiai rendszerek információbiztonságának, illetve információtechnológiai biztonságának fenntartása, beleértve a jogszabályi követelmények előírásainak megfelelő biztosítását is.
e) Az ügyfeleknek nyújtott szolgáltatások üzemeltetése és fejlesztése érdekében alkalmazott támogató folyamatokra, illetve információtechnológiai rendszerekre vonatkozó mindenkori jogszabályi és egyéb szabályozási követelményeknek való megfelelőség folyamatos biztosítása.

Az ***IBP*** célja, hogy irányelveket adjon az ***IBF*** részére a biztonsági politikánál alacsonyabb szintű szabályozások kialakításához, a jelen és jövőbeli informatikai biztonsági döntéseik meghozatalához, illetve a biztonsági rendszer működtetői és a felhasználók számára a napi rendeltetésszerű tevékenységük gyakorlásához.

Az *Egyetem* a célok eléréséhez és fenntartásához alapvető eszköznek tekinti;

a) Az egyetemi üzleti és szolgáltatás működés folyamatos fejlesztését, a korszerű technológiák bevezetését, és alkalmazását;
b) A szolgáltatások folyamatos fejlesztését a szabályozási követelmények, az ügyfelek és a piac igényei alapján;
c) Folyamatos továbbképzéssel a legmagasabb szakmai kompetencia vagy színvonal elérését;
d) A feladatok és megbízások elvégzéséhez szükséges erőforrások felmérését és biztosítását;
e) Megfelelő és megbízható beszállítók, alvállalkozók kiválasztását és alkalmazását, amelyek elfogadják és teljesítik az információbiztonsági követelményeket;
f) A munkavégzés során – törekvéseink ellenére is - bekövetkező hibák kijavítását;

g) A tevékenységekre vonatkozó szakmai, adat- és információvédelmi, és egyéb jogszabályi követelmények – és ezek változásainak – folyamatosan figyelemmel kísérését, és azok maradéktalan betartását;

h) A védendő ügyfél és saját információs-, illetve adatvagyon fenyegetettségének és azok biztonsági kockázatainak rendszeresen, legalább évente történő felülvizsgálatát és újraértékelését, majd ennek megfelelően az információvédelmi előírások és eljárások aktualizálását;

i) A szolgáltatások feltételeinek folyamatos biztosításához a következő – kiemelkedő kockázatúnak értékelt – incidens kategóriák elfogadhatatlannak tartását és legnagyobb veszélynek értékelését:

- az ügyfelek adatainak jogalap nélkül nyilvánosságra kerülése;
- adatvesztések, amelyek mentésekből nem állíthatók vissza;
- hálózati betörés a támogató és szolgáltató informatikai, információtechnológiai rendszerekbe.