BUDAPESTI CORVINUS EGYETEM	**ELNÖKI TESTÜLETI RENDELKEZÉS**	**10/2024.** Verziószám: **00.**

AZ INFORMATIKAI BIZTONSÁG SZABÁLYAIRÓL

Szakmai felelős:	**Sopronyi Tibor**	IT vezető
Szakmai ellenőrző:	**Bíró Barbara**	jogi vezető
Jogi ellenőrző:	**Borbás Zsuzsanna**	gazdasági jogi, beszerzési, munkajogi vezető
Döntéshozó:	**Elnöki Testület**	
Szerkesztésért és közzétételért felelős:	**Erős Anikó**	felsőoktatási szakértő

Verziószám	**Közzététel dátuma**	**Hatálybalépés dátuma**	**Verziókövetés**
00.	2024. 04. 29.	2024. 05. 01.	**Közzététel** ET-51/2024. (IV. 25.). sz. határozat

Tartalomjegyzék

A rendelkezés célja 3
Felelősségmegosztás 4
A rendelkezés hatálya 5
Rendelkezés külső partnerekre vonatkozóan 5
Informatikai eszközök és jogosultságok 6
Az informatikai biztonság tudatosítása, oktatása és képzése 11
Az alkalmazás (munkaviszony, munkavégzésre irányuló egyéb jogviszony, szerződéses jogviszony) megszűnésére, vagy megváltoztatására vonatkozó rendelkezések 12
Munkavállalói felelősségek 15
Rendszer és alkalmazás-hozzáférés felügyelete 15
A kommunikáció és az üzemeltetés irányítása 16
Az üzemelő szoftverek védelme 18
Egyetemi internethasználat szabályai 21
Informatikai biztonsági incidensek kezelése 24
Vegyes és zárórendelkezések 25
Melléklet(ek): 25
1. melléklet Jogosultságok felülvizsgálata 26
2. melléklet Corvinus mentési eljárásrend 27

AZ INFORMATIKAI BIZTONSÁG SZABÁLYAIRÓL

A rendelkezés célja

1. §

(1) Az Informatikai biztonság szabályairól szóló elnöki testületi rendelkezés (továbbiakban: IBSZ) célja mindazon rendszerszintű követelmények, előírások és eljárások, feladatok, tevékenységek meghatározása és egységes, magas szintű szabályozási keretbe foglalása, melyek által a Budapesti Corvinus Egyetem (a továbbiakban: Egyetem) informatikai biztonsága, rendeltetésszerű és biztonságos működése, továbbá az Egyetem által használt elektronikus rendszerek (továbbiakban: informatikai rendszer) sértetlensége és rendelkezésre állása, valamint az Egyetem által azokban kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása a kockázatokkal arányosan és folyamatosan fenntartható módon megvalósítható, megőrizhető, továbbá továbbfejleszthető.

(2) Az IBSZ célja továbbá:

a) Meghatározni azokat az adminisztratív, fizikai és logikai védelmi intézkedéseket, amelyek támogatják:

- a megelőzést és a korai figyelmeztetést,
- az észlelést,
- a reagálást,
- a biztonsági események kezelését,
- az események utólagos jelentését és elemzését.

b) Elősegíteni az Egyetemen belüli egységes informatikai biztonsági szemlélet kialakítását, a vonatkozó jogszabályokban foglalt informatikai biztonsági követelményeknek való megfelelés biztosítását, valamint azon hazai és nemzetközi szabványokban és módszertani ajánlásokban megfogalmazott legjobb gyakorlatoknak megfelelő működés kialakítását, amely kellő megelőző hatással bír és megbízható módon képes garantálni az Egyetem digitális információinak, adatainak védelmét, valamint azt, hogy az informatikai eszközök használata megfelelő biztonságtudatossággal és ellenőrzötten valósuljon meg.

c) A tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével meghatározni azokat a technikai és szervezési intézkedéseket, amelyek a kockázat mértékének megfelelő szintű adatbiztonságot garantálják, így különösen a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét, továbbá fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani.

Felelősségmegosztás

2. §

(1) Az informatikai biztonsággal kapcsolatos felelősség megoszlik elsősorban az Egyetem vezetősége, az Informatika és a többi szervezeti egység, valamint az egyes munkatársak között. A felelősségmegosztás elveit az alábbiakban tárgyaljuk.

a) A felső szintű felelősség az informatikai biztonság folyamatos biztosításáért, az informatikai biztonsággal kapcsolatos szabályozásokért, szervezeti célkitűzésekért az egyetemi informatikai biztonsági tudatosság megfelelő szintjének biztosításáért, valamint az informatikai biztonsági intézkedések bevezetéséért az Informatikát terheli. A Jog, Igazgatás, Szabályozás a GDPR szerinti adatbiztonsági követelmények becsatornázásával támogatja az Informatikát.

b) Az informatikai biztonság koordinálásának felső szintű vezetője az Egyetem kancellárja.

c) Az egyes szervezeti egységek szintjén a szervezeti egység vezetője felel személyesen az informatikai biztonság fenntartásáért.

(2) Feladatkörök szétválasztása
Az Egyetemen a következő informatikai biztonsági felelősségi körök definiálása szükséges:

a) Közvetlen felső vezetés (Kancellár) főbb feladatai:

– Az informatikai biztonsági feladatokkal kapcsolatos információk egyeztetése az Informatikával és a Jog, Igazgatás, Szabályozással.

– Az informatikai biztonsági feladatok végrehajtásához szükséges erőforrások biztosítása.

– Az informatikai biztonsági rendszer belső és külső auditálásának megbízásba adása a kancellár feladata.

b) Informatika, valamint Jog, Igazgatási, Szabályozás
Az Egyetem Informatikájának főbb informatikai biztonsági feladatai:

– Adatmentések felügyelete és naplózása.

– Az igényelt szoftverek vizsgálata, hogy az egyetemi környezettel kompatibilisek-e.

– Rendszernaplók, víruskeresési naplók, egyéb naplók figyelése.

– Az eszközök megfelelő működésének monitorozása (gépi vagy humán módszerekkel).

– Munkatársak bejelentései során incidensek monitorozása és javítása, szükség esetén bevonni a Jog, Igazgatás, Szabályozást.

– Biztonsági beállítások folyamatos felülvizsgálata és szükség esetén korrigálásuk.

– Rendszerhozzáférési jogok, hozzáférési policy-k és konkrét hozzáférési szabályok kialakítása és implementálása.

c) Szervezeti egység vezetők, valamint a beosztott alkalmazottak

– Az Egyetem minden vezetőjének meg kell követelnie beosztottjaitól és megbízottjaitól az informatikai biztonsági előírások betartását, valamint szabályszegés esetén a vonatkozó belső szabályozó dokumentumok szerinti rendben kezdeményeznie kell a felelősségre vonást.

A rendelkezés hatálya

3. §

(1) Személyi hatálya:

a) Az IBSZ személyi hatálya kiterjed az Egyetemmel munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban álló természetes személyekre (pl. óraadó oktatókra), továbbá az Egyetemmel szerződéses jogviszonyban lévő jogi személyekre és jogi személyiséggel nem rendelkező szervezetekre, akik közreműködnek az Egyetemnél keletkező, felhasznált, feldolgozott, tárolt, továbbított adatok kezelésében, továbbá akik az Egyetem által működtetett informatikai rendszerek kezelésében (fejlesztésében, üzemeltetésében, karbantartásában, javításában vagy felügyeletében) részt vesznek. A szerződéses jogviszonyban állókkal az IBSZ előírásait a megkötött szerződésben kell érvényesíteni.

b) Az IBSZ személyi hatálya kiterjed továbbá az Egyetem hallgatóira és jelentkezőire mindazon esetekben, amikor egyetemi informatikai rendszert használnak.

(2) Területi hatálya:

A rendelkezés területi hatálya kiterjed az Egyetem székhelyére, valamennyi telephelyére, működési területére.

(3) Tárgyi hatálya:

a) A rendelkezés informatikai rendszerekre vonatkozó előírásai az információkezelő és infokommunikációs eszközökre, valamint ezek elemeire vonatkoznak.

b) Nem tartoznak az IBSZ tárgyi hatálya alá a Campus Szolgáltatások feladatellátásához kapcsolódó biztonságtechnikai és elektronikus vagyonvédelmi rendszerek, azzal azonban, hogy ezek működtetésének informatikai vonatkozásaiban az IBSZ az irányadó.

Rendelkezés külső partnerekre vonatkozóan

4. §

(1) A biztonság kérdésének kezelése a külső kapcsolatokban:

a) Munkájuk során a külső partnerekkel, mint például szállítók, szolgáltatók (a továbbiakban külső partnerek) és az ügyfelekkel közvetlenül kapcsolatba kerülő munkavállalók részére tartott oktatások részévé kell tenni az informatikai biztonsági megfontolásokat, továbbá egyértelműen jelölni kell a kiadható információk körét.

b) Az ügyfelekkel való kapcsolattartás során csak azok az adatok, információk adhatók meg, amelyek feltétlenül szükségesek és nem sértik az Egyetem érdekeit.

c) Ügyfélre, ügyfélszerződésre vonatkozó adatok csak az ügyfél, továbbá meghatalmazottjának azonosítása után adhatók ki az azonosított személy részére.

(2) A biztonság kérdésének kezelése külső partnerrel kötött megállapodásokban:
Az IT vezető feladata és felelőssége gondoskodni arról, hogy az Egyetem informatikai rendszereit érintő, külső partnerekkel kötött szerződéseiben a felek informatikai biztonsággal kapcsolatos alábbi kötelezettségei és feladatai a szerződés tárgya által indokolt mértékben megjelenjenek:

a) titoktartási feltételek;

b) adatvédelmi és adatbiztonsági szabályok és követelmények a szerződésben érintett adatok vonatkozásában;

c) hozzáférési jogosultságok kezelése, logikai hozzáférés az Egyetem rendszereihez, hozzáférésre jogosultak köre;

d) az Egyetem jogosult a számára végzett tevékenység ellenőrzésére;

e) kommunikációs csatornák, eszkalációs útvonalak;

f) a partnertől elvárt biztonsági intézkedések;

g) biztonsági események kezelési módja;

h) az Egyetem hatályos belső szabályozó dokumentumai.

Informatikai eszközök és jogosultságok

5. §

(1) Informatikai eszközök elfogadható használata:

a) Az Informatika által biztosított szolgáltatások, rendszerek, erőforrások és eszközök elsősorban rendeltetésszerűen, az Egyetem céljainak megfelelően, oktatási és kutatási célra, valamint az ezt kiszolgáló szolgáltatások biztosítása érdekében használhatóak. Rendeltetésszerű használatnak azt a célt és felhasználási módot tekintjük, amelyre az Informatika eredetileg biztosította.

b) Ezen célok érdekében sem megengedett mások hasonló felhasználását zavarni, az egyetemi eszközöket átkonfigurálni, saját hálózati eszközzel helyettesíteni, bővíteni.

c) Az Egyetem engedélyezi a fentieken túli a magáncélú használatot, ameddig ez az a) pontban megjelölt használatot nem akadályozza, zavarja. Ilyen pl. az egyes file megosztások korlátozása és tiltása.

d) Az a) pontban leírt célok biztosítása érdekében az Informatika térben, időben vagy a felhasználás módjában korlátozhatja a magáncélú használatot, informatikai incidens esetében pedig az Egyetem céljainak megfelelő rendeltetésszerű használatot is.

e) Bármilyen informatikai incidens során az Informatika munkatársai rendkívüli ideiglenes intézkedésekkel korlátozhatják a forgalmat. Ennek kommunikálása az eset súlyosságától függően utólag is történhet.

(2) Jogosultságokkal kapcsolatos követelmények

a) Szabály a jogosultságok felügyeletéhez:

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

ab) Tartalmi rendszergazda meghatározása: Egy adott egyetemi informatikai rendszer egészét, vagy modulok esetében, egy részét jól ismerő munkavállaló, aki tisztában van a rendszer által végzett/támogatott üzleti folyamatokkal, üzleti és technológiai működéssel és aki a munkájával támogatja az Informatikát és a fejlesztési területet (Digitális Innováció, továbbiakban: DI) az üzemeltetés és a fejlesztés során. Az adott rendszer/modul tekintetében az adott szervezeti egység és az Informatika közötti kapcsolattartásért felelős, a modult mind informatikai, mind üzleti szempontból ismerő munkavállaló. A szükséges felhasználói számot tervezi és a szükséges licensz mennyiség rendelkezésre állását felügyeli.

ac) A munkavállalói jogosultságok naprakészen tartása a munkáltatói jogkört gyakorló vagy az általa megbízott munkavállaló feladata. Ez azt jelenti, hogy a munkáltatói jogkört gyakorlónak kell az új jogosultságokat megigényelnie, a jogosultságok elvételéről intézkednie, továbbá a folyamatosan biztosítandó jogosultságokat a munkáltatói jogkört gyakorlónak kell meghosszabbíttatnia. Az adott informatikai rendszer tartalmi rendszergazdája az, aki a kiosztandó jogosultságokat jóváhagyja, törléseket kérheti az éles üzemben használt rendszerek esetében. A tartalmi rendszergazdáknak pontos információkkal kell rendelkezniük az átaluk felügyelt rendszerben nyilvántartott jogosultságokról.

ad) A fejlesztés alatt álló, vagy teszt rendszerekben a fejlesztésért felelős terület, elsősorban a DI kérheti vagy hagyhatja jóvá a jogosultság igényléseket. A fejlesztés befejezése után ugyanígy a fejlesztésért felelős területnek kell kezdeményeznie a jogosultságok visszavonását is. Ezeket a jogosultságokat évente felül kell vizsgálnia a tartalmi rendszergazdának, az Informatika által biztosított információ alapján.

ae) A nem egyedileg a felhasználóhoz, hanem automatikusan, meghatározott logika alapján felhasználók nagyobb csoportjához rendelhető jogosultságok esetében meg kell határoznia minden esetben a tartalmi rendszergazdának az informatikai területtel közösen, hogy melyek a jogosultság kiosztásának feltételei.

b) Hozzáférés hálózatokhoz és szolgáltatásokhoz:

ba) Az egyetemi publikus szolgáltatások, hálózaton meghatározott módokon elérhetőek az egyetemen kívülről vagy belülről, egyetemi polgároknak és másoknak is.

bb) Az Egyetem publikus-azonosított hálózatát azok érhetik el, tetszőleges eszközről, akiket az Egyetem azonosítani tud, és ehhez jogosultsággal rendelkeznek.

bc) Az Egyetem védett hálózatába azok az eszközök és szolgáltatások tartoznak, amelyek csak az Egyetem azonosított, erre jogosult felhasználói számára elérhetőek. A felhasználás jellegétől függően ennek további szűkítése lehetséges szolgáltatásonként.

bd) Az Egyetem védett hálózatához, mind kívülről mind belülről csak az Informatika által felügyelt eszközzel lehet csatlakozni. Ez kívülről az Informatika által szolgáltatott VPN-kapcsolaton át valósul meg. Szigorúan tilos bármilyen ettől eltérő megoldás megkísérlése a munkavállalók és szerződött partnerek részéről is.

be) Az Egyetem internetelérést biztosíthat az egyetemi felhasználóknak saját (nem Informatika által felügyelt) eszközeiken (elsősorban Wi-Fi szolgáltatás), vendégeknek (pl. Rendezvény és Vendég Wi-Fi szolgáltatás továbbá partnerintézményeknek (pl. Eduroam). A csatlakoztatott eszközök az egyetemi hálózat elérése szempontjából nem biztonságosnak tekintendők, a védett hálózatot nem érik el.

bf) Felhasználóknak, külső partnereknek – akik nem rendelkeznek egyetemi hozzáférésekkel – tilos az Egyetem hálózatán külön engedélyezés nélkül szolgáltatást nyújtani, arra eszközeiket csatlakoztatni. Az engedélyt csak az IT vezető adhatja ki, legalább két munkanappal a használatot megelőzően.

c) Az Informatika munkavállalóinak jogosultságai:
Az Informatika munkavállalói minden olyan jogosultsággal rendelkeznek, amelyek az informatikai rendszerek, szolgáltatások adminisztrálásához szükséges. Ezek a jogosultságok indokolt esetben kiterjedhetnek a munkavállalók által létrehozott adatokhoz való hozzáférésre. Ilyen lehet a levelezés, a létrehozott file-ok, hálózati forgalom, internet forgalom stb. Az Informatika munkavállalóin kívül az Egyetemen senki sem rendelkezhet ilyen jogosultságokkal, mely kitételt az Egyetem minden munkavállalójának és vezetőjének el kell fogadnia. Továbbá az Egyetem minden munkavállalójának el kell fogadnia a fentieket, miszerint az Informatika megfelelően magas jogosultságokkal rendelkező munkavállalói minden informatikai rendszerben végrehajtott műveletről tudomással bírnak, és minden keletkezett adattal kapcsolatban információval rendelkeznek. Diagnosztikai, hibafeltárási,

működésanalitikai célból, továbbá az IBSZ betartásának/betartatásának érdekében az Informatika munkatársai rögzíthetik és elemezhetik a hálózati forgalmat, valamint a rendszerek naplóállományait.

(3) Munkavállalók regisztrálása és törlése

a) Regisztrálás:

aa) A munkavállalókat egyedi felhasználónévvel kell azonosítani. Csoportos felhasználóneveket nem célszerű használni, de bizonyos, kivételes esetekben megengedett. A kivételeket az IT vezető engedélyezheti.

ab) Új munkavállaló regisztrálásának előfeltétele az aláírt munkaszerződés vagy megbízási szerződés és a HR rendszerben (SAP) megadott szükséges adatok. Ennek hiányában csak a kancellár engedélyével regisztrálható új munkavállaló. A munkavállalók regisztrálása és a munkavállalói adatok módosítása a felhasználó kezelő rendszerben az Informatika munkavállalóinak feladata.

ac) Alapjogosultságként minden munkavállaló és hallgató rendelkezik a következő hozzáférésekkel: O365 (levelezés, Teams, Onedrive, SharePoint), az Egyetem hálózatának használata (ezen keresztül az internet elérése az Egyetem szolgáltatási területen belül), nyomtatási lehetőség stb. Ezeken kívül a többi jogosultságot a munkáltatói jogkört gyakorlónak kell megigényelnie.

ad) Hallgatók esetén a belépési jogosultságok a beiratkozást követően jönnek létre, és regisztrációt követően tudja használni az egyetemi belső rendszereket, valamint az O365 felhőben található alkalmazásokat és lehetőségeket is.

b) Munkavállaló törlése:

ba) Munkavállaló kilépése esetén a folyamat elindításáért a munkavállaló munkáltatói jogkört gyakorlója a felelős. A munkavállaló jogosultságai a kilépés utáni második napon törlődik szinte minden adata és hozzáférése. A levelezés és az O365 tárolt állományok 30 napig állíthatók vissza. A visszaállítás okozhat technikai nehézségeket, emiatt inkább az állományok átmozgatását addig javasoljuk, amíg a munkavállaló nem lépett még ki. Amennyiben valamilyen okból szükséges a kilépett munkavállaló jogosultságainak megtartása, akkor azt a munkáltatói jogkört gyakorlónak írásban kell jeleznie az IT vezetőnek, aki gondoskodik a jogosultságok meghosszabbításáról.

bb) A munkáltatói jogkört gyakorló vezető ezzel egyidejűleg – ha a kockázatok indokolják – soron kívül megtehet további informatikai védelmi intézkedéseket is (pl. visszaélés gyanúja esetén soron kívüli felfüggesztés elrendelése stb.).

c) Munkavállalói hozzáférés biztosítása

A jogosultságkezelési folyamatban az alábbi általános szabályok az irányadóak:

ca) Hozzáférést csak a szükséges mértékben és időtartamra szabad engedélyezni, olyan személyek számára, akiknek a feladataik ellátása és/vagy jogaik gyakorlása érdekében indokolt. A szükséges mértékre és időtartamra történő

korlátozás nemcsak a hozzáférés kockázatát minimalizálja, hanem a hozzáférő személy által viselt felelősséget is. Ennek felelőse a munkáltatói jogkört gyakorló vezető.

cb) Az Egyetem rendszereihez csak a jogosultságkezelési folyamat betartásával adható hozzáférés. A folyamat a következő:

- A jogosultság igénylést elindíthatja maga a munkavállaló is, ebben az esetben az első lépés a munkáltatói jogkört gyakorló vezető jóváhagyása, ezt követően minden esetben szükséges a tartalmi rendszergazda jóváhagyása éles alkalmazások esetében.
- Fejlesztés alatt álló teszt rendszer esetében a tartalmi rendszergazda helyett a fejlesztési terület is jóváhagyhatja a jogosultság igénylést.

cc) Külső partnerek vonatkozásában az Egyetem IT rendszereihez való hozzáférés csak érvényes szerződés alapján biztosítható. A hozzáférés igénylését ebben az esetben csak Egyetem alkalmazásában álló munkavállaló indíthatja el és szükséges a tartalmi rendszergazda jóváhagyása, ha a kért jogosultság éles használatban lévő rendszert érint. (éles és teszt környezetbe történő hozzáférés igénylés esetén is)

cd) Külső partnerek esetén a hozzáférési jog maximum egy évre adható, szükség esetén meghosszabbítható.

ce) Az Egyetem IT rendszereihez hozzáférési jogot kapott természetes személyek, jogi személyek és jogi személyiséggel nem rendelkező szervezetek a hozzáférési jogot a velük kötött szerződés és/vagy általuk tett titoktartási nyilatkozatok alapján gyakorolhatják.

cf) A hozzáférési jogosultságokkal történő visszaélés gyanúja esetén az Egyetem minden munkavállalója köteles haladéktalanul értesíteni a munkáltatói jogkört gyakorló vezetőjét, akinek haladéktalanul értesítenie kell az IT vezetőt és a Jog, Igazgatás, Szabályozás vezetőjét.

d) Hallgatói jogosultságok biztosítása és megőrzése

da) *Hallgatók jogosultságainak megadása:*
A hallgatók jogosultsága automatikusan jön létre, amikor a Neptun Egységes Tanulmányi Rendszerbe bekerültek. Naponta futó automatizmus létrehozza a hallgatói jogosultságokat az IDM rendszerbe és beállítja számára a megfelelő alapjogosultságokat. Ezek a létrejövő jogosultságok lehetőséget adnak az alábbi szolgáltatások használatára:

- Wi-Fi szolgáltatáshoz való hozzáférés
- O365 szolgáltatások használata (levelezés, Teams, Onedrive, Sharepoint)
- Az Egyetemi infrastruktúra (laborok) használat
- VPN
- Egyéb olyan szolgáltatások, amelyek az egyetemi identitáshoz köthetőek (pl: Moodle, Könyvtári adatbázisok, Eduroam)

Hallgató státusza	IDM jogosultság
Beiratkozott	Megadva
Aktív	Megadva
Passzív (szünetelő)	Megadva
Abszolvált	Utolsó aktív félévtől számítva a jogosultság 4 félévig megadva, utána törölve
Sikeres záróvizsgát tett	Utolsó aktív félévtől számítva a jogosultság 1 félévig megadva, utána törölve
Sikertelen záróvizsgát tett	Utolsó aktív félévtől számítva a jogosultság 1 félévig megadva, utána törölve
Oklevelet szerzett	Utolsó aktív félévtől számítva a jogosultság 1 félévig megadva, utána törölve
Elbocsátott	Törölve
Fokozatot szerzett	Törölve
Végzett	Törölve
Intézmény, képzés váltott, törölt	Törölve

db) *Hallgatók jogosultságainak időbeli megtartása:*
A hallgatói jogosultságokat célszerűségi és jogszabályi szempontok miatt is eltérő folyamattal kell kezelni, mint a munkavállalók jogosultságait.

Kivételek: Az 5. §(3)b) pont alapján lehetséges a jogosultságok megőrzése vagy meghosszabbítása is, amennyiben megfelelő indokkal erre igény érkezik.

Az informatikai biztonság tudatosítása, oktatása és képzése

6. §

(1) Annak érdekében, hogy a munkavállalók és a hallgatók felkészülhessenek a lehetséges belső- és külső fenyegetések felismerésére, az alapvető biztonsági követelményekről tudatossági képzést kell nyújtani az elektronikus informatikai rendszer felhasználói

számára. Az oktatásnak alkalmazkodnia kell a munkatárs által betöltött szerepkörhöz, az általa használt rendszerekhez.

(2) Informatikai biztonsági képzéseket kell tartani évente, frissítő jelleggel. A képzésekre a munkáltató jogkört gyakorló vezetőknek kell a munkavállalókat delegálni.

(3) Az Egyetem a munkavállalóinak munkakörüknek megfelelő informatikai biztonsági tudatosság növelését célzó belső képzését a képzési javaslatoka lapján éves rendszerességgel, továbbá tudatosító programok, figyelemfelhívó és ismeretterjesztő anyagok biztosításával folyamatosan végzi.

(4) Az informatikai biztonsági szempontból kiemelten kezelendő munkaköröket betöltő munkavállalók és hallgatók magas színvonalú szakmai tudásának fenntartásához szükséges képzéseken (pl.: tanfolyamok, szakirányú továbbképzések) való részvételét az Egyetem támogatja.

(5) Az Informatika proaktív módon felmérheti a munkavállalók és hallgatók informatikai biztonsági tudatosságát, továbbá képzettségét, akár valószerű szituációk (pl. adathalász levél küldése) előre bejelentett szimulációjával. Az ilyen felmérésen a feltárt hiányossággal bíró kollégák számára kötelező az ezzel kapcsolatos képzésen való részvétel.

Az alkalmazás (munkaviszony, munkavégzésre irányuló egyéb jogviszony, szerződéses jogviszony) megszűnésére, vagy megváltoztatására vonatkozó rendelkezések

7. §

(1) *Felelősségek az alkalmazás megszűnésekor:*
Az IT vezető felelőssége gondoskodni a kilépő munkavállalók informatikai jogosultságainak visszavonásáról és megszüntetéséről, amennyiben az automatikus jogosultság megszüntető folyamat nem elégséges. Az informatikai jogosultságok a kilépés utáni második napon a fiókkal együtt törlésre kerülnek. Ettől eltérő ütemezést a munkáltatói jogkört gyakorló vezető írásban igényelhet.

(2) *Vagyontárgyak visszaszolgáltatása:*

a) Az Egyetemről való távozás esetén a munkavállaló köteles a rábízott informatikai eszközöket visszaszolgáltatni az Egyetem részére. Az eszközöket minden esetben az Informatika szakembereinek kell leadni, akkor is, ha a vonatkozó szervezeti egység a továbbiakban igényt tart a használatára. Ebben az esetben a kilépő munkavállaló munkáltatói jogkört gyakorló vezetője írásban kell, hogy jelezze az Informatika felé, hogy mely másik munkavállalójának kívánja átadni az eszközt. Az Informatika minden leadott eszközt újra kell, hogy telepítsen, mivel el kell távolítani az előző munkavállaló profilját, valamint a telepített alkalmazásokat is. Ezt követően az egy ember – egy eszköz elv figyelembevételével újra kioszthatóvá az informatikai eszköz. Az eszköz visszaszolgáltatása esetén a Felhasználó nyilatkozik, hogy az általa használt eszközt úgy bocsátotta az Informatika rendelkezésére, hogy arról minden személyes jellegű dokumentumot törölt. Jelen pont szerinti nyilatkozat mintáját az Informatika adja ki. A nyilatkozatot a HR 5 évig megőrzi.

b) Az eszközök hiánytalan és hibátlan állapotban történő visszaszolgáltatása esetén ennek tényét az Informatika nyilvántartásában rögzíti és ezeket az adatokat átadja a Pénzügy vagyongazdálkodási egységének.

c) Amennyiben a munkavállaló nem számol el maradéktalanul a nyilvántartás szerint az általa használt eszközökkel, akkor az Informatika nem igazolja a kilépéskor az eszközök szabályos leadását és ezt jelzi a HR felé a kilépés dátuma előtt legkésőbb 2 munkanappal. Amennyiben a munkavállaló nem tud elszámolni a nyilvántartás szerint az ő leltárában lévő eszközökkel, akkor az Informatika által megállapított piaci áron meg kell térítenie az eszközök ellenértékét.

(3) *IT eszközök megváltoztatása vagy cseréje:*

a) Amennyiben az Egyetem által biztosított IT eszköz cserére kerül – akár meghibásodás miatt, akár a központi PC csere program keretén belül – akkor a korábban használt informatikai eszköz megvásárlására van lehetőség. Informatikai eszközt akkor lehet megvásárolni, ha az vagy 4 évnél régebben került üzembe helyezésre és nincs rajta elidegenítési tilalom, vagy olyan szintű műszaki állapotban van, hogy annak felhasználása továbbiakban nem lehetséges. Az eszközök árát minden esetben az Informatika szakértői határozzák meg a piaci árakat figyelembe véve, mely ár nem alkuképes.

b) Az Egyetem informatikai eszközgazdálkodásának alapelve az egy ember – egy számítógép elv. Ennek értelmében minden munkavállalónak egyetlen számítógép biztosítása jár. Ez alól lehetséges indokolt esetekben kivétel, amelyet minden esetben az IT vezetőnek kell írásban engedélyeznie. Az egy biztosított számítógép mindig notebook, vagyis hordozható számítógép.

(4) *Hozzáférési jogok megszüntetése:*

a) Minden munkáltatói jogkört gyakorló vezető azonnal köteles jelezni a beosztottjainak munkaviszony megszűntetésére irányuló szándékát a HR felé, akik ezt az információt továbbítják az Informatika felé, jelezve, hogy a munkavállaló meddig áll még alkalmazásban és milyen (esetleg csökkentett) jogosultságok szükségesek számára az átmeneti időszak alatt.

b) A munkáltatói jogkört gyakorló vezetők, egyéb szerződés esetén a szerződéskötők a munkavállaló kilépése, munka- illetve egyéb jogviszonyának megszűnése – például vállalkozó, kölcsönzött munkaerő – távozása esetén kötelesek jelezni az Informatika felé a távozás tényét és a szükséges intézkedéseket (hozzáférés korlátozása, felfüggesztése, e-mailek átirányítása stb.).

c) Az IT vezető feladata gondoskodni arról, hogy a kilépő munkavállaló informatikai jogosultságainak a munkáltatói jogkört gyakorló vezető által megadott szintre történő korlátozása a felmondási időre (vagy az ennek megfelelő időszakra) megtörténjen, valamint a jogviszony megszűnése napján véglegesen visszavonásra kerüljön, amennyiben ezzel ellentétes, legalább munkáltatói jogkört gyakorló által kezdeményezett írásos kérelem nem érkezik az Informatikára.

d) Hallgatók jogviszonyairól az 5§(3) d.) pont rendelkezik. Hallgatók részére is lehetséges jogosultságok hosszabbítása, amennyiben ez indokolt és a kérést oktató vagy munkáltató írásban eljuttatja az Informatikára, indoklással.

e) Privilegizált jogosultságok: minden olyan jogosultság ebbe a körbe tartozik, amely a munkavállalói vagy hallgatói jogoknál több jogot jelent (pl. rendszeradminisztrátor). Főbb szabályok a privilegizált jogosultságokkal kapcsolatban:

- A rendszerek adminisztrációjához kellő rendszergazdai jogosultságot csak a rendszergazdai feladatkörben foglalkoztatott munkatársak kaphatnak és csak a feladatkörüknek megfelelő rendszerekre érvényesen. A rendszergazdai jogosultságok legyenek egyértelműen személyhez kötöttek, a csoportos azonosítók használata tilos.
- A rendszergazdák az emelt szintű jogokat biztosító azonosítójukat csak a munkavégzéshez feltétlenül szükséges mértékben használják, minden más esetben a normál felhasználói azonosítójukkal dolgozzanak.
- Mindenképpen kerülni kell olyan rendszerek üzembe állítását, amelyek nem rendszergazda munkakörben dolgozó munkavállalók rendszergazdai jogosultságokkal történő felruházását igényelnék.
- Privilegizált (pl.: rendszergazdai) hozzáféréssel rendelkező munkavállaló távozása esetén az IT vezető – az adott rendszerben kezelt adatok biztonsági besorolása, illetve a hozzáféréssel kapcsolatos kockázat függvényében – gondoskodik arról, hogy a távozó munkavállaló által ismert jelszavakat a rendszergazdák dokumentáltan megváltoztassák.
- Rendszergazdai jogosultságokkal rendelkezhetnek felhasználók a 2022. januárjában életbe lépett, „Jogosultságok felülvizsgálata” című rendelkezésnek megfelelően. A rendelkezés az 1. számú mellékletben található.
- A munkavállalói jogosultságok korlátozását és visszavonását az Informatika a jegykezelő rendszerében rögzítve köteles végrehajtani.

(5) *Munkavállalói hozzáférési jogok átvizsgálása:*

a) A munkavállaló által igényelt jogosultságok indokoltságát és informatikai biztonsági megfelelőségét elsősorban a munkáltatói jogkört gyakorló vezetőnek vagy az általa megbízott munkavállalónak, vagy a tartalmi rendszergazdának kell évente legalább egyszer átvizsgálnia.

b) A már regisztrált munkavállalók adatainak helyességét és a részükre megadott jogosultságokat rendszeresen, legalább évente egy alkalommal át kell vizsgálni, azzal a céllal, hogy az adminisztráció során bekövetkezett hibákat/tévedéseket kiszűrjék. Az átvizsgálásnak kezdeményezése, az aktuális jogosultságok riportjának elkészítése és a megfelelő vezetők számára történő elküldése, majd a módosítás kérések végrehajtása az IT vezető felelőssége. Ellenőrizni kell az adatok helyességét, ki kell szűrni:

- a már kilépett, de esetleg a rendszerben bennmaradt munkatársakat,
- a megváltozott munkakör után megmaradt régi jogosultságokat,
- az ideiglenesen megadott, már lejárt jogosultságokat.

Munkavállalói felelősségek

8. §

(1) Titkos hitelesítési információk használata:

a) Minden munkavállaló a hozzá tartozó titkos hitelesítő információkat bizalmasan kezeli, más munkavállalóval nem oszthatja meg. Papír alapon nem tárolhatja.

b) Gondatlan hitelesítési információ használatból fakadó károkért a munkavállaló vállal felelősséget.

c) Amennyiben külső partnerektől kell jogosultságot szerezni az Egyetem munkavállalóinak, az Informatika szakértője az adott területi vezetővel együttműködve végezheti ezt a tevékenységet.

d) A munkavállalók számára nem javasolt titkosítatlan privát adattároló használata, például: felhő alapú adatcsere portálok, privát e-mail fiókok, fizikai adathordozó eszközök. Ezen privát eszközök közé tartoznak a munkavállalók személyes email fiókjai is. Az Egyetem által előfizetett és használható felhő alapú tárhelyre a tiltás nem vonatkozik.

(2) Munkavállalói jogosultságok nyilvántartása:
Az IT vezető felelőssége a jogosultságok nyilvántartása elektronikus rendszerekben, kivéve a nem központi autentikációval rendelkező rendszerekben (ilyen pl. a Neptun vagy az SAP). Papír alapon a jogosultságok nyilvántartása nem szükséges.

Rendszer és alkalmazás-hozzáférés felügyelete

9. §

(1) Az IBSZ célja meghatározni az Egyetem informatikai rendszereihez hozzáférést biztosító jelszavak és felhasználónevek kezelését, képzését, módosítását.

(2) Információhoz való hozzáférés korlátozása:

a) A jelszó: A jelszó az egyik fő eszköz arra, hogy a munkavállaló és a hallgató az informatikai rendszerekhez való hozzáférési jogosultságát érvényesítse, és az illetéktelen hozzáférést meggátolja.
<u>A jelszóhasználat fő szabályai:</u>

aa) A jelszó jogosulatlan személynek történő átadása vagy hozzáférhetővé tétele üzleti titoksértésnek minősül, ami munkajogi és büntetőjogi, hallgatók esetén fegyelmi és büntetőjogi felelősségre vonás alapját képezheti.

ab) A nem alapinfrastruktúra rendszerekben a jogosultságokat és jelszavakat a tartalmi rendszergazdák kezelik, az alapinfrastruktúra jelszavak kezelése az Informatika feladata.

ac) Csak a jelszóváltoztatási igényben szereplő munkavállaló vagy hallgató jelszavát lehet megváltoztatni, amennyiben a bejelentés írásba van foglalva és az arra jogosult személy kéri. Szóbeli bejelentésre a bejelentőn kívül más munkavállaló

vagy hallgató jelszavát tilos megváltoztatni, a szóbeli bejelentésről pedig generálódnia kell hibajegynek.

ad) A jelszavakat nyílt szöveg formájában tilos tárolni vagy bármilyen csatornán továbbítani, kivéve az első alkalommal létrejövő jelszó továbbítását elektronikus úton.

ae) A 9. §(3) pontban rögzített jelszó alkotási szabályok kötelező érvényűek.

(3) Jelszó alkotási szabályok:
Az Egyetem központi informatikai rendszereiben csak az alábbi paramétereknek megfelelő jelszó használható. A jelszó képzésének szabályai az alábbiak:

a) Minimálisan 8 karakter hosszú legyen.

b) Csak ékezetmentes betűből áll.

c) A jelszó nem lehet azonos a felhasználói azonosítóval.

d) Jelszó legyen összetett, mindenképp tartalmazzon legalább egy kisbetűt, legalább egy nagy betűt és legalább egy számot.

e) A jelszó módosításánál az új jelszó kialakításánál nem egyezhet meg az utolsó jelszóval.

f) A jelszó lejárata 1 év.

A kommunikáció és az üzemeltetés irányítása

10. §

(1) Változáskezelés

a) A változáskezelés irányító szervezete a Változáskezelési Bizottság (Change Advisory Board, CAB).

- A CAB tagjai a funkcionális / technikai szakterületek, a legfontosabb döntéshozói és az üzleti érdekelt felek képviselői. A CAB legfontosabb feladata, hogy a különböző szakterületek által indított módosítási kérelmeket értékelje és azok megvalósíthatósága kapcsán meghozza a szükséges döntéseket, figyelembe véve az Egyetem által meghatározott célokat, terveket, a rendelkezésre álló forrásokat.
- A CAB-ot az IT vezetőnek vagy a DI vezetőnek kell összehívnia, az ő feladatuk eldönteni, hogy mely esetekben tartják indokoltnak egy-egy változás CAB elé vitelét. Nem kell rendszeres időközönként a CAB-ot összehívni, csak akkor, ha a döntése szükséges a változások elindításához, vagy ha a változás folyamatában közös döntést igénylő pontig jutott.

b) Az alábbi esetekben mindenképpen szükséges összehívni a CAB-ot:

- Különösen nagy értékű fejlesztési feladat, amely legalább 30 millió forint.
- Olyan változás vagy fejlesztés, amely több szakterület feladatait is érinti.
- Olyan változás vagy fejlesztés, amely több, egymással kapcsolatban lévő rendszert is érint.

c) A CAB tagjai:
   - IT vezető
   - Pénzügyi terület képviselője (Pénzügyi vezető jelöli ki)
   - DI csapat vezetője
   - Az érintett szakterületek vezetője vagy képviselője

d) Nem szükséges a CAB-ot összehívni olyan ügyekben, amelyek technikai jellegű változások és nem érintenek alkalmazásokat, vagy csak speciálisan az Informatika hatáskörébe tartoznak. Ilyenek lehetnek pl. a szerver vagy a hálózati környezetet érintő változások, vagy pl. a levelezőrendszerrel kapcsolatos fejlesztések.

e) Informatikai rendszerekben, alkalmazásokban változás vagy fejlesztés csak abban az esetben indítható és hajtható végre, ha az IT vezető és a DI vezetője azt írásban jóváhagyja.

f) Amennyiben a változás vagy fejlesztés személyes adatok kezelését/tárolását is érinti, az adatvédelmi tisztviselő véleményét előzetesen ki kell kérni annak érdekében, hogy a vonatkozó adatvédelmi követelményeket azonosíthassa és a fejlesztés folyamatába becsatornázhassa („privacy by design”).

(2) Biztonsági vonatkozások:

a) Az IT vezető tesz javaslatot a változáskezelési eljárásokra, továbbá azok módosítására – figyelembe véve a biztonsági szempontokat. Amennyiben a változáskezelési eljárás érinti a CAB hatáskörét, akkor az IT vezető összehívja a bizottságot.

b) Az informatikai rendszerek változásait csak az IT vezető vagy az általa írásban meghatalmazott munkavállaló által írásban jóváhagyott változási kérelmek alapján szabad végrehajtani. A változásokat a végrehajtás után a végrehajtónak dokumentálni kell.

(3) Fejlesztési, teszt és éles rendszerek különválasztása

a) Fejlesztő (staging) környezetet külsős fejlesztő esetén minden esetben a fejlesztő köteles előállítani és üzemeltetni. Az Informatika külsős szerződött partnernek nem biztosít fejlesztői környezetet, kizárólag szolgáltatás szintű hozzáférést a tesztkörnyezethez – on-prem környezetben. Nem on-prem környezetben a fejlesztő felelőssége a fejlesztői környezet létrehozása és üzemeltetése, különösen akkor, ha a fejlesztés szolgáltatásban kerül megvásárlásra. Teszt és éles rendszer létrehozásában az Informatika szakemberei támogatást nyújtanak.

b) Az IT vezető biztosítja szükség esetén az elkülönített tesztelői és éles környezetekhez szükséges erőforrásokat. A teszt rendszeren az éles környezettel megegyező szintű védelmet kell biztosítani, beleértve a jelszavak használatát is.

c) Akár belsős, akár külsős szerződött partner végzi a fejlesztést, csak a kijelölt fejlesztői környezetben végezhetnek feladatokat, a fejlesztések új verzióit pedig kizárólag a tesztelői környezetekben tesztelhetik. Nem engedélyezett az éles környezetben történő tesztelés, ha az tesztelői környezetben is elvégezhető. A tesztelés végrehajtását

és eredményét dokumentálni kell jegyzőkönyv formájában. Kizárólag a dokumentáltan sikeres tesztet követően történhet meg az éles környezetre az adott fejlesztés kihelyezése.

d) Ahol nem áll rendelkezésre teszt környezet, az IT vezető vagy a DI vezető rendelkezhet úgy, hogy az éles rendszeren kerüljön bevezetésre egy-egy fejlesztés, ha tesztadatokkal ez nem elvégezhető.

(4) Rendszertervezés és elfogadás:
Nem az Informatika által indított beszerzések során megvásárolt és nem az Informatika által bevezetett, felügyelt alkalmazások és rendszerek dokumentációs eljárásairól a lebonyolító vagy igénylő területnek kell gondoskodnia. Ezekben az esetekben az Informatika csak az informatikai vonatkozású – elsősorban technológiai – kérdésekben nyilatkozik.

a) Az Informatika csak olyan rendszerek üzemeltetését veszi át, ahol a tervezési fázistól kezdve folyamatosan részt vett a projektben és pontos információkkal rendelkezik az üzemeltetési átvételre kijelölt rendszerről.

b) A teszteléshez szükséges infrastruktúrát biztosítja, szervezi és felügyeli.

c) A teszteléshez használt adatokat ugyanolyan szinten kell védeni, mint amit azok az éles környezetben kapnának.

d) Új rendszerek vagy rendszerek új verziói csak az Egyetem jóváhagyott tesztelési eljárásrendje alapján helyezhetők üzembe. Az üzembe helyezés tényét és körülményeit dokumentálni kell az üzemeltetői naplóban.

e) A tesztek befejezése után a fejlesztő jogosultságait vissza kell vonni az Egyetem rendszereiben, kivéve azokat, amelyeket támogatási, karbantartási szerződésben vállalt tevékenységeihez szükségesek. A teszt befejezését a tesztet végző szervezeti egység határozza meg.

f) Az új informatikai rendszerek munkavállalói átvételi tesztjét a megrendelő szervezeti egység erre megbízott munkavállalója hajtja végre (ehhez az Informatika szükség esetén támogatást nyújt), s annak eredményéről értesíti az Informatika kijelölt kapcsolattartóját.

g) Hasonlóan az informatikai változás vagy fejlesztés esetén követendő protokollhoz, amennyiben személyes adatok kezelését/tárolását is érinti az új rendszer, az adatvédelmi tisztviselő véleményét a vásárlást, de legkésőbb a használatba vételt megelőzően ki kell kérni annak érdekében, hogy a vonatkozó adatvédelmi követelményeket azonosíthassa.

Az üzemelő szoftverek védelme

11. §

(1) Szoftverek telepítése az üzemelő rendszerekre:

a) Biztosítani kell, hogy a szoftverek csak megfelelően képzett szakemberek által kerüljenek telepítésre és megváltoztatásra.

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

c) Gyártói támogatással nem rendelkező szoftverek üzletileg kritikus rendszerekben nem üzemeltethetők.

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

(2) Védelem a rosszindulatú és mobil kódok ellen:

a) Az Egyetem minden munkaállomásán víruskereső és vírusirtó funkcionalitással bíró védelmi szoftvert működtet, amelynek telepítése, biztonsági beállításainak konfigurálása az Informatika feladata és felelőssége.

b) Az Informatika szakértői folyamatosan felügyelik a vírusvédelmi rendszer rendelkezésre állását és működésének megfelelőségét.

c) Nem engedélyezett az Egyetem eszközeire az Informatika írásos jóváhagyása nélküli szoftvertelepítés vagy futtatás, kivéve, ha rendszergazda joggal rendelkezik az eszköz tulajdonosa.

d) Nem engedélyezett az Egyetem védelmi rendszereinek (tűzfal, vírusvédelmi rendszer, tartalomszűrő) megkerülése, azok működésének akadályozása vagy konfigurációjának módosítása.

e) Nem engedélyezett nem az Egyetem által jóváhagyott célból vagy módon az Egyetem által biztosított eszközökkel állományok futtatása, ismeretlen eredetű, internetről letöltött adatállományok adathordozón való behozatala.

f) Az Egyetem üzletmenetének keretében kívülről érkező adatállományokat megnyitás / futtatás előtt a vírusirtó szoftver automatikusan ellenőrzi. Az ehhez szükséges beállítások végrehajtása az Informatika feladata és felelőssége. Kétség esetén az állományt tartalmazó adathordozót az Informatika részére kell vírusellenőrzés céljából továbbítani.

g) Minden munkavállaló haladéktalanul köteles jelezni a vírusfertőzés gyanúja esetén az informatikai Helpdesk felé.

(3) Biztonsági mentés:

a) Az IT vezető gondoskodik arról, hogy az Egyetem által használt informatikai rendszerek és a bennük kezelt adatok biztonsági mentése az üzleti igényeknek megfelelően és dokumentált módon megtörténjen. A mentési eljárásrend kialakítása során a kezelt adatok bizalmassági besorolását is figyelembe kell venni. A mentési eljárásrendnek ki kell terjednie a mentéseket tartalmazó adathordozók kezelésére is. A mentési eljárásrendet az *2. melléklet* tartalmazza.

b) Az Informatika munkatársai végzik el a mentésekkel kapcsolatos beállításokat és ellenőrzik a mentések sikerességét. A mentésekről dokumentáció készül (mentési napló vagy logfájl). Amennyiben a mentés az adott informatikai rendszer leállításával

hajtható csak végre, arról az érintett terület tartalmi rendszergazdáival előzetesen egyeztetni szükséges.

c) A biztonsági mentésekben kezelt személyes adatokra az éles rendszerekben kezelt személyes adatokra vonatkozó megőrzési idők vonatkoznak, melynek érvényre juttatása érdekében az Informatika és a személyes adatokat kezelő szervezeti egység köteles együttműködni, igény esetén a Jog, Igazgatás, Szabályozás bevonásával.

(4) Hálózatbiztonság kezelése:

a) Az Egyetem hálózatának biztonságos kialakításáért, üzemeltetéséért, karbantartásáért, védelméért az IT vezető felel.

b) Az Egyetem hálózatait a nyilvános hálózatoktól el kell különíteni. Minden internet kijáratot tűzfallal kell védeni, amelynek beállításait csak az IT vezető által írásban kijelölt, munkaköri leírásban rögzített felelősséggel rendelkező munkavállalók módosíthatják.

c) Az Egyetem telephelyein vezetékes vagy vezeték nélküli hálózati és internethozzáférést kizárólag az Informatika munkatársai helyezhetnek üzembe és konfigurálhatnak.

d) Nem engedélyezett a felhasználók számára az Egyetem védelmi rendszereinek (tűzfal, proxy, tartalomszűrő eszköz vagy alkalmazás) megkerülése, azok működésének akadályozása vagy az IT vezető által nem kijelölt munkavállalóknak ezek konfigurációjának módosítása.

e) Nem engedélyezett a gyengeáramú hálózati kábelek átrendezése, cseréje, másik csatlakozóba való bekötése, a jelenlegi bekötés módosítása. Ezeket a feladatokat az Informatika munkatársai végzik, a helpdesknek történt bejelentés alapján.

f) Minden olyan rendszer üzemeltetése, amely hálózati szolgáltatást nyújt felhasználók szélesebb köre számára, az IT vezető jóváhagyásához kötött. Felhasználók szélesebb körének számít különösen a hálózaton bárki által elérhető szolgáltatás, az egyetemi polgárok által hálózaton elérhető szolgáltatás vagy az egyetemi polgárok egy csoportja (pl. egy adott kollégium) számára hálózaton elérhető szolgáltatások.

g) Az Egyetem a hálózati szolgáltatásokat nyújtó rendszerek védelmét a hálózati forgalom szűrésével is segíti. A hálózati szűrőszabályok kialakítása a rendszerek üzemeltetéséért felelős tartalmi rendszergazdákkal együttműködésben az Informatika feladata. A hálózati szűrőszabályok módosítását a hálózati biztonság növelése érdekében a IT vezető által írásban kijelölt, munkaköri leírásban rögzített felelősséggel rendelkező munkavállalók saját hatáskörben elvégezhetik. E körön kívülről érkező igények megvalósításához minimum feltétel, hogy a hálózati szolgáltatást nyújtó rendszer felelős tartalmi rendszergazdája az igényt dokumentáltan jóváhagyja.

(5) Figyelemmel követés (monitoring):

a) Audit naplózás

- Az IT vezető – rendszerenként, az adatgazdákkal egyeztetve – meghatározza a naplózandó tevékenységeket, a naplózás módját és célját, valamint a naplóállományok megőrzési idejét. Amennyiben törvény nem írja elő, vagy az adatvédelmi tisztviselő nem látja indokoltnak hosszabb megőrzési idő beállítását, a megőrzési idő maximum 6 hónap.
- A monitorozó rendszerhez és a naplógyűjtő- és elemző rendszerhez csatlakoztatni kell minden szervert és hálózati eszközt. A naplógyűjtő- és elemző rendszerben meg kell határozni azokat a kimutatásokat, figyeléseket, amelyeket automatikusan el tud a program végezni.

b) Rendszerhasználat figyelése

- Az Informatika munkatársai – az IT vezető által előírtak szerint – szoftvereszközökkel vagy manuálisan elvégzik a szükséges naplóállomány elemzéseket, és a szabálytalanságra vagy üzemzavarra utaló jeleket dokumentálják, kiértékelik, majd az eredményt jelzik az IT vezető részére.
- Amennyiben a naplófájlok elemzésének eredménye biztonsági incidens lehetőségét veti fel, azt jelenteni kell a Jog, Igazgatás, Szabályozás vezetőjének.

c) Hibák naplózása

- Az IT vezető (vagy az általa megbízott vezető) háromhavonta felülvizsgálja a Helpdesk rendszerben az egy hónapnál régebbi incidenseket, és megteszi a szükséges intézkedéseket azok elhárítására, a hibák besorolásának megfelelő prioritással.
- Az informatikai rendszerekben előforduló hibákat a dokumentált elemzéseket követően rögzíteni kell a Helpdesk rendszerben. Az Informatika munkatársai a hibákat hetente elemzi, és azonosítja a felmerülő vagy várható problémákat.

Egyetemi internethasználat szabályai

12. §

(1) Az Egyetem a hálózati infrastruktúrájához kapcsolódó eszközökön az internet magáncélú használatát nem tiltja. A használatra vonatkozó szabályokat az 5. §(2)b) pontja rögzíti.

(2) Elektronikus levelezés:

a) Jelen szakasz célja az Egyetem elektronikus üzenetküldő rendszerének, levelező rendszerének használatának szabályozása. A szabályozó meghatározza az elfogadható és helyes használatot, a használat során betartandó informatikai biztonsági szabályokat, és a használattal kapcsolatos feladatokat és felelősségeket.

b) A szabályozás kiterjed az Egyetem minden munkavállalójára és hallgatójára, valamint mindazon külső személyekre, akik az Egyetem elektronikus üzenetküldő rendszerének használatára engedélyt kaptak.

c) Az Egyetem nem tiltja a levelezőrendszer magáncélú használatát, ugyanakkor a felhasználásnak az alábbiakban részletezett korlátai vannak.

(3) Szabályok és eljárások az információátvitelre
A levelező rendszer, valamint a rendszerben előállított, elküldött, továbbított, megkapott, tárolt vagy archivált üzenet az Egyetem tulajdona és az Egyetem felügyelete alatt áll, ezeket az Egyetem a jelen pont szerint monitorozhatja, és tartalmába indokolt esetben szorosan a célhoz kötött módon betekinthet. Ilyen célok lehetnek pl.: az üzletmenet folytonosság biztosítása, bizonyítékok gyűjtése informatikai biztonsági incidensek és fegyelmi ügyek kivizsgálásakor, valamint az erre jogszabályban feljogosított hatóságoktól érkező kérések teljesítése. A betekintés során az Egyetem érvényre juttatja a fokozatosság elvét, melynek keretében amennyiben egy levél tárgyából/címzettjéből vagy más körülményből a levél megnyitása nélkül is kétségtelen, hogy akár a munkavállaló, akár harmadik személy személyes adatát is tartalmazza, a levél tartalmának megismerése tilos. Kivétel képez ez alól az az eset, amikor az Egyetemnek alapos gyanúja áll fenn, hogy a munkavállaló postafiókja az Egyetem jogos gazdasági érdekeit, üzleti hírnevét sértő adatokat tartalmaz, mely esetben külön érdekmérlegelési teszt elvégzését követően jogosult az Egyetem az ilyen e-mail tartalmát is megismerni. Ilyen esetben tájékoztatni kell az érintettet a postafiók ellenőrzéséről, biztosítani kell a személyes jelenlétét akár képviselője útján is, és az ellenőrzésről jegyzőkönyvet kell felvenni. Az ilyen ellenőrzésre minden esetben az Informatika vezetőjének és a Jog, Igazgatás, Szabályozás vezetőjének, vagy az általuk kijelölt személy jelenlétében kerülhet sor. Ahhoz, hogy az e-mail fiók ellenőrzése jogszerű legyen, az Egyetemnek előzetesen részletes tájékoztatást kell biztosítania a munkavállalók számára.

A tájékoztatóban ki kell arra, hogy:

a) milyen célból, milyen munkáltatói érdekek miatt kerülhet sor az e-mail fiók ellenőrzésére;

b) az Egyetem részéről ki végezheti az ellenőrzést;

c) milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete;

d) milyen jogai és jogorvoslati lehetőségei vannak a munkavállalóknak az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

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

Elektronikus levelek továbbítása esetén fontos ügyelni arra is, hogy. illetéktelen személyek részére ne kerüljön továbbításra bizalmas- vagy személyes adat.

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

(4) Az elektronikus üzenetküldő rendszer használata során nem megengedett:

a) indokolatlanul nagy mennyiségű és méretű üzenetek küldése (35 MB-nál nagyobb állományok levelezés útján történő továbbítása nem javasolt);

b) reklámok és hirdetések közzététele;

c) lánclevelek terjesztése, továbbítása;

d) olyan üzenetek, továbbá csatolt fájlok küldése, továbbítása, amelyek bármely módon történő jogszabálysértést vagy arra való felhívást tartalmaznak, sértik az Egyetem jó hírét.

(5) Megállapodások az információátvitelre

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

b) A munkavállaló tudomásul kell vegye, hogy az Egyetemnek nem áll módjában a hálózatának határain túl az elküldött üzenetek továbbításának útvonalát felügyelet alatt tartani, azok biztonságáról gondoskodni.

(6) Elektronikus üzenetküldés

a) Az Egyetem nevében folytatott üzenetváltásban kizárólag az erre a célra biztosított elektronikus levelezési cím, a munkavállalónak engedélyezett szolgáltatás használható. Más szervezet vagy szolgáltató által biztosított e-mail szolgáltatás hivatalos céllal nem használható.

b) A munkavállaló tudomásul kell vegye, hogy a leveleinek feladója, címzettje, és tárgya a technikai üzemeltetés során az Informatikai megfelelő jogosultságokkal rendelkező munkatársai részére látható lehet.

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

(7) Bizalmassági vagy titoktartási megállapodások

a) Az általános informatikai eljárásoknak megfelelően a bizalmas információt e-mailben vagy annak csatolmányában csak titkosított módon szabad küldeni.

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

c) Bizalmas információt tartalmazó üzenetet tilos levelezési listára küldeni.

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

Informatikai biztonsági incidensek kezelése

13. §

(1) *Informatikai biztonsági események jelentése*

a) Biztonsági esemény minden olyan nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az informatikai rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az informatikai rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, továbbá megsérül. Incidensnek minősül minden olyan esemény, amely nem része az Egyetem mindennapi üzletmenetének, elhárítása a normál hibaelhárítási folyamat keretében nem lehetséges és veszélyeztetheti az Egyetem informatikai rendszereinek, továbbá az azokban kezelt adatok biztonságát.

b) Minden munkavállaló köteles azonnal jelenteni az észlelt biztonsági eseményt (incidenst), továbbá a biztonsági eseményre utaló jeleket a munkáltatói jogkört gyakorló vezetőjének és az Informatikai Helpdesknek.

c) Biztonsági esemény bekövetkezése esetén a hozzá érkező jelzés vagy saját észlelés alapján az IT vezető vizsgálatot folytat le, szükség esetén bevonva a Jog, Igazgatás, Szabályozás vezetőjét.

d) Az adatvédelmi incidens kezelésére vonatkozó szabályokat az adatkezelés rendjéről szóló elnöki testületi rendelkezés rögzíti.

(2) *Biztonsági gyenge pontok jelentése*

a) Az Informatika munkatársai a hozzájuk érkező bejelentések, valamint az általuk észlelt események adatait szükség esetén jelzik az IT vezető részére.

b) A munkavállalók jelentési kötelezettsége kiterjed azokra a biztonsági esemény lehetséges bekövetkezésére utaló jelekre, amelyek az informatikai rendszerek biztonságát veszélyeztethetik. Ilyenek lehetnek például:

- a kéretlen emailek számának növekedése. Ebben az esetben a munkavállalónak blokkolnia kell a feladót a levelezőrendszerben, ezzel is tanítva a levelezőrendszert
- kéretlen, vírusgyanús e-mail csatolmányok érkezése;
- adatokhoz való illetéktelen hozzáférés lehetősége, adatok kiszivárgása az általuk használt informatikai rendszerekből;
- az informatikai eszközök (PC-k, hálózati eszközök, nyomtatók, perifériák) látható károsodása;

(3) *Informatikai biztonsági incidensek és javító fejlesztések kezelése*

a) Felelősségek és eljárások:

- Az IT vezető gondoskodik arról, hogy a nagy kockázatú biztonsági események kezelésére (pl.: nagy kiterjedésű vírusfertőzés, hálózati betörés, kritikus eszközök

megsemmisülése stb.) dokumentált eljárásrend álljon rendelkezésre, amelyet az Informatikamunkatársai ismernek és végrehajtását tesztelték.

- Az informatikai biztonsági vonatkozású bejelentés esetén a bejelentést fogadó munkavállaló haladéktalanul köteles azt az érintett rendszer(ek) rendszergazdája felé továbbítani.
- A rendszergazdák azonnal megkezdik az esemény kivizsgálását és megteszik a szükségesnek ítélt intézkedéseket. Más rendszereket is érintő intézkedések esetén az azok rendszergazdáival való előzetes egyeztetés szükséges.
- Amennyiben a veszélyforrás elhárítása sikeres, az eseményre vonatkozó Helpdesk bejegyzést az elhárítás menetével ki kell egészíteni.

b) Tanulságok levonása az informatikai biztonsági incidensekből:

- Az IT vezető jelentős esemény esetén azonnal, egyébként havonta, az Informatika munkavállalóinak bevonásával kiértékeli az informatikai biztonsági eseményeket, azok hatásait, annak jóváhagyásával kezdeményezi a szükséges intézkedések megtételét.
- Az értékelésről jegyzőkönyv készül – melyet tájékoztatás céljából megküldenek az adatvédelemmel megbízott szervezet részére –, amely a következő értékelés során összehasonlítás alapjául szolgálhat.

Vegyes és zárórendelkezések

14. §

(1) Jelen rendelkezés 2024. május 1-jén lép hatályba.

Melléklet(ek):

1. melléklet: Jogosultságok felülvizsgálata
2. melléklet: Corvinus mentési eljárásrend

1. melléklet

Jogosultságok felülvizsgálata

Több irányból, különösen az Akadémiai szervezeti egységektől érkező kéréseket figyelembe véve az Informatika elkezdte felülvizsgálni a notebookokhoz kapcsolódó jogosultságok rendszerét. Különböző forrásokból információkat gyűjtve (külföldi egyetemmel is felvéve a kapcsolatot) az oktató kollégák számára célszerűnek tartjuk annak bevezetését, hogy teljes rendszergazda (local administrator) hozzáférési lehetőséget biztosítsunk az általuk használt, egyetemi tulajdonban lévő hordozható számítógépre.

Ennek bevezetését az alábbi feltételek alapján kívánjuk kialakítani:

(a) Kizárólag egyetemi tulajdonban lévő hordozható eszközre adható ki a teljes rendszergazdai jogosultság (ebbe a kategóriába tartozik minden Informatika által biztosított eszköz, továbbá a pályázati pénzből vásárolt eszközök is)

(b) A rendszergazdai jogosultsággal rendelkező eszközök külön jelzést kapnak az informatikai nyilvántartási rendszerben

(c) Visszamenőleg, jelenleg használt eszközön is igényelhető a jogosultság, melyekre szintén vonatkozni fognak a felsorolt feltételek. A jelenleg használt eszközökön az Informatika elvégzi a szükséges változtatásokat (pl. BIOS jelszó megszüntetése). Ekkor a számítógép kikerül az egyetemi rendszerekből. Az új eszközök nem rendelkeznek operációs rendszerrel, továbbá semmilyen alkalmazás nincs rájuk telepítve, ezekről a rendszergazda jogosultsággal rendelkező munkatársnak kell gondoskodnia.

(d) A teljes rendszergazda jogosultsággal rendelkező kollégák szabadon telepíthetnek, távolíthatnak el alkalmazásokat az általuk adminisztrált számítógépeken, a szoftver jogitisztaságot betartva és vállalva a törvényes felelősséget.

(e) Megszűnik minden korlátozás az eszközön, szabadon konfigurálható minden.

(f) Ezek az eszközök kikerülnek az Informatika adminisztrálási környezetéből, így szoftveres karbantartásukról, esetleges újratelepítésükről a teljes rendszergazda jogosultsággal rendelkező felhasználónak kell gondoskodnia. Támogatásuk a saját tulajdonú eszközökkel azonos mértékben látja el az Informatika.

(g) Garanciális (fizikai) meghibásodás esetén továbbra is az Informatika munkatársai intézik a szervízelés folyamatát, amennyiben erre igény van.

(h) Biztonsági okokból a teljes rendszergazdai jogosultsággal rendelkező eszközök nem léphetnek be az egyetemi tartományba. A közös tárakat is csak VPN kapcsolaton keresztül lehet majd elérni.

(i) Biztonsági okokból a teljes rendszergazdai jogosultsággal rendelkező eszközök nem csatlakozhatnak az egyetemi vezetékes belső hálózatra, kizárólag a wifi-t és VPN-t használhatják

(j) Szükséges a fentiekkel kapcsolatban egy nyilatkozat aláírása. Ez részletesen tartalmazni fogja a feltételeket, korlátokat és lehetőségeket

A jogosultságot bármely oktató kolléga igényelheti, akinek az Intézetvezetője hozzájárul a jogosultság kiadásához. A hozzájárulás nélkül az ISZK nem hajtja végre a jogosultság módosítását. Az igényeket az alábbi elektronikus űrlapon tudja leadni. https://forms.office.com/r/ezftQj203B

Azon kollégák, akik nem kívánnak élni a teljes rendszergazda jogosultság lehetőségével, továbbra is a jelenlegi környezetben tudják használni az eszközeiket.

2. melléklet

Corvinus mentési eljárásrend

Oracle

Gyakoriság: Óránként log. Naponta inkrementális és hetente full mentés.
Módja: Oracleből időzítve
Megőrzési idő: 28 nap

Az alábbi rendszereket napi szinten mentjük:

Solaris alatt futó rendszerek

Módja: Operációs rendszerből időzítve
Megőrzési idő: 30 nap

TSMSRV

Módja: Operációs rendszerből időzítve; /save mentése a TSM szerveren
Megőrzési idő: 30 nap

SAP rendszerek

SAP ABP adatbázis HANA

Logmentés: max 15 percenként
Megőrzési idő: 365 nap

SAP ABT adatbázis HANA

Logmentés: max 15 percenként
Gyakoriság: hetente
Megőrzési idő: 365 nap

Alkalmazás- és webszerverek

Módja: Operációs rendszerből időzítve
Megőrzési idő: 30 nap

VMware virtuális gépek mentése

Módja: mentőszerverből való ütemezéssel
Megőrzési idő: 30 nap

VMware alatti adatbázisok mentése

Módja: mentőszerverből való ütemezéssel
Megőrzési idő: 30 nap