A
BUDAPESTI GAZDASÁGI EGYETEM
SZERVEZETI ÉS MŰKÖDÉSI SZABÁLYZATA

A
BUDAPESTI GAZDASÁGI EGYETEM
INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

Budapest 2016
(2016. október 15. napjától hatályos változat)

TARTALOMJEGYZÉK

1. BEVEZETÉS

A Budapesti Gazdasági Egyetem (a továbbiakban: Egyetem) informatikai rendszerének fejlesztése és üzemeltetése során kiemelt figyelmet fordít a kor követelményeihez igazodó biztonsági megoldások és eljárásrendek kialakítására, az aktuális szakmai ajánlásoknak megfelelő biztonsági szabályozási környezet létrehozására, az Egyetem dolgozói és hallgatói biztonság tudatosságának folyamatos növelésére.

Jelen Informatikai Biztonsági Szabályzat az ISO 27001 szerinti követelmények figyelembe vételével készült el, és a működési és szervezeti rendek, a felelősségi, nyilvántartási és tájékoztatási szabályok, a folyamatba épített ellenőrzési követelmények és szabályok meghatározása útján a fenti célok megvalósításához szükséges aktuális és naprakész szabályrendszert tartalmazza.

2. A SZABÁLYZAT CÉLJA ÉS HATÁLYA

2.1 A szabályzat célja

Jelen szabályzat célja, hogy egységes követelményrendszert állítson fel az Egyetem informatikai biztonsági irányítási rendszerére vonatkozólag. Továbbá értelmezéseket, iránymutatást adjon az Egyetem infokommunikációs eszközeit használók számára, rögzítve azokat a szabályokat, amelyeket a használat során követniük kell.

A szabályzat egységes szerkezetbe foglalja az alkalmazott információs rendszerekkel és azok felhasználóival szemben támasztott biztonsági követelményeket.

2.2 Személyi hatálya

Az Informatikai Biztonsági Szabályzat az informatikai biztonsággal összefüggő szabályzásokat, ezek dokumentálását, az ellenőrzésének leírását és ezek hivatkozásait tartalmazza, hatálya kiterjed az Egyetem polgáraira, (valamennyi érintett dolgozójára, hallgatójára), az Egyetem adataival dolgozó szerződéses alvállalkozókra és mindazokra, akik az Egyetem informatikai szolgáltatásait igénybe veszik, illetve az Egyetem informatikai rendszeréhez hozzáféréssel rendelkeznek.

2.3 Tárgyi hatálya

Az Informatikai Biztonsági Szabályzat kiterjed az informatikai rendszerben működtetett valamennyi hardver berendezésre, szoftverelemre és ezek dokumentációira (fejlesztési, szervezési, programozási, műszaki, üzemeltetési, biztonsági) és az informatikai rendszerben feldolgozott adatállományok teljes körére.

Az Informatikai Biztonsági Szabályzat magában foglalja

a) az informatikai rendszer elemeinek tervezését és új elemeinek bevezetését, üzemeltetését és használatát;

b) az informatikai biztonság meghatározását, általános célkitűzéseit és tárgykörét, valamint a biztonság és a védelmi intézkedések fontosságát abban a mechanizmusban, amely az információ megosztását teszi lehetővé;

c) a vezetőség álláspontját, hogy miként támogatja az informatikai biztonság céljait és elveit;

d) az informatikai biztonság menedzselésének (Informatikai Biztonsági Felelős és informatikai szervezet) általános és sajátos felelősségi köreinek meghatározását;

e) utalást azokra a dokumentációkra, amelyek támogatják a szabályzatot, pl. Informatikai rendszer üzemeltetésével kapcsolatos utasításokra és eljárásokra.

A szabályzatot az Egyetem a honlapján (http://www.uni-bge.hu) elérhetővé teszi az érintettek számára).

3. FOGALOMTÁR

Jelen szabályzatban az alábbi fogalmak értelmezése:

Adat: az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.
Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.
Adatbiztonság megsértése: az a cselekmény vagy mulasztás, amely ellentétben áll az adat védelmére vonatkozó biztonsági szabályokkal és amelynek következményei az adatot veszélyeztetik.
Adatgazda: az a személy, aki élve az Egyetem által biztosított jogosultságával, adatot osztályba sorol és felelős az általa besorolt adatok, továbbá az adatok feldolgozásához kapcsolódó rendszerek jogosultságainak kezeléséért.
Adatvédelem: az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik.
Adminisztratív védelem: szervezési és szabályozási úton megvalósított védelem.
Backup rendszer: az informatikai biztonság megvalósítása során az adatok rendelkezésre állását lehetővé tevő rendszer és program másolatokat őrző rendszer. Rendszerint minimális tartalékkal rendelkező informatikai rendszert is értenek alatta.
Bizalmasság: (szervezeti állapot) - az Egyetem olyan állapota, amely biztosítja, hogy az adatokhoz csak azok a meghatalmazottak férhessenek hozzá, akiknek a szervezet ehhez jogot adott.
(adat tulajdonság). Az Infotv. szerint a bizalmasság az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
Biztonság: olyan szervezeti állapot, melyben az adott szervezetnek a lehető legkisebb veszélyekkel kell számolnia, szolgáltatásait a vállalt/előírt feltételekkel és korlátozások nélkül képes nyújtani, a feladatait, funkcióinak ellátását illetően érdemi hatást gyakorló veszteség nem éri, a lehetséges fenyegetettségek bekövetkezési valószínűségéből és a lehetséges kárértékekből származtatott kockázat a szervezet számára elfogadhatóan alacsony és a kockázatkezelési eljárások eredményeként kialakuló maradvány kockázat a szervezet számára az elviselhető tartományban marad. A védeni kívánt informatikai rendszer olyan, az Egyetem számára kielégítő mértékű állapota, amely zárt, teljes körű, folytonos és a kockázatokkal arányos védelmet valósít meg. A biztonság az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek

a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.
Biztonsági követelmények: a kockázatelemzés eredményeként megállapított, elfogadhatatlanul magas kockázattal rendelkező fenyegető tényezők ellen irányuló biztonsági szükségletek együttese.
Biztonsági esemény: az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás, amelynek hatására az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült vagy megsérülhet.
Biztonsági osztályba sorolás: az adatnak az adatkezelés során a kezelés módjára, körülményeire, a védelem eszközeire vonatkozó védelmi szintet meghatározó besorolása, osztályozása.
Biztonsági rendszer: a biztonsági rendszer az informatikai biztonsági rendszerek összessége (logikai védelmet valósít meg, pl.: tűzfal, vírusvédelmi rendszer, jogosultág-nyilvántartó rendszer, stb.).
Egyenszilárdság: a biztonság az intézmény tevékenységét teljesen átfogja, és annak minden pontján azonos erősségű.
Egyetemi tevékenységi-, vagy érdekkörbe tartozó állományok, információk: a jelzett információk olyan eszközön tárolhatók, amelyen biztosítható, hogy illetéktelen személy nem fér hozzá az információkhoz (pl.: internetkávézóban található számítógép nem megengedett eszköz).
Elektronikus aláírás (digitális aláírás): az informatikai rendszerben kezelt adathoz rendelt, kódolással előállított olyan jelsorozat, amely az adat hitelességének és sértetlenségének bizonyítására használható.
Elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), együttese.
Elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.
Érintett: bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy.
Felhasználó: az a személy, szervezet vagy csoport, aki (amely) egy vagy több informatikai rendszert igénybe vesz feladatai megoldásához.
Felhasználói hitelesítés: a felhasználó hitelességének ellenőrzése (a belépéskor minden felhasználó ellenőrzése) és különböző azonosító eszközök (pl.: jelszó, chip-kártya, biometrikus azonosítás, stb.) alkalmazása.
Felhő alapú tárhelyszolgáltatás: elektronikus anyagok tárolására alkalmas szolgáltatás, amelyet a felhasználók internetes kapcsolaton keresztül érnek el. Az anyagok tárolása a szolgáltató eszközein elosztva, a felhasználó számára nem transzparens módon történik.
Folyamatosság: az egyetemi tevékenységek zavarmentes rendelkezésre állása.
Folytonos védelem: olyan védelmi megoldás, amely az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul.
Hálózat: számítógépek (vagy általánosabban informatikai rendszerek) összekapcsolása és az összekapcsolt rendszerek legkülönbözőbb komponensei közötti adatcserét megvalósító logikai és fizikai eszközök összessége.
Hitelesség: egy adat hiteles, ha tartalma és tulajdonságai az elvárttal megegyeznek, illetve az adat az elvárt forrásból származik, és a származás ellenőrizhető.

Hozzáférés: olyan eljárás, amely valamely informatikai rendszer használója számára – jogosultságának függvényében – meghatározott célra, helyen és időben elérhetővé teszi az informatikai rendszer erőforrásait, elérhetővé tesz a rendszerben tárolt adatokat.
Illegális szoftver: az a szerzői jog védelme alatt álló szoftvertermék, amelynek a legalitás igazolásához szükséges dokumentumok (licenc, számla, szállítólevél, ajándékozási szerződés, stb.) nem mindegyike áll rendelkezésre, valamint a szoftver használata nem felel meg a licenc szerződés előírásainak.
Illetéktelen személy: olyan személy, aki az adat megismerésére nem jogosult.
Informatikai biztonság: az Egyetem informatikai rendszerének olyan kielégítő állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve az informatikai rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.
Informatikai biztonsági dokumentációs rendszer: többszintű, egymásra épülő rendszer, amely magába foglalja a biztonságpolitikai elvektől a szabályzatokon keresztül a munkautasítások szintjéig az informatikai biztonsági irányelveket, teendőket, szereplőket, azok feladatait, jogait, kötelességeit és felelősségeit.
Informatikai biztonsági incidens: minden olyan nem kívánt, illetve nem várt eseményt, amelyek nagy valószínűséggel veszélyeztetik az Egyetem tevékenységét és fenyegetik az informatikai biztonságot.
Informatikai rendszer: információs-, ügyviteli-, egyetemi folyamat vagy szolgáltatás működését támogató elektronikus adatfeldolgozó eszközök és eljárások, és a kapcsolódó folyamatok összessége. A hardver-, szoftver-, kommunikációs eszközök és ezek kezelő / kiszolgáló szervezeteinek olyan együttese, amelyet az intézmény üzletpolitikájával összhangban céljai megvalósítására használ.
Információ-feldolgozó eszköz: minden olyan számítástechnikai, telekommunikációs és egyéb kategóriájú elektronikai eszköz, mely képes a betáplált (input) adatokat manipulálni és a folyamat végén eredményeket, kimenő adatokat (output) produkálni – az azt használó személy számára értelmezhető formában.
Incidens: minden olyan informatikai vonatkozású esemény, ami nem része a normál működésnek és a felhasználókat akadályozza feladataik ellátásában. A szolgáltatási hiba típusú incidensek a szolgáltatási szintek csökkenésével járnak (vagy ezzel fenyegetnek), míg a szolgáltatási igény típusú incidensek általában valamilyen eszköz vagy információ biztosítását, módosítások végrehajtását igénylik. Egy incidensnek lezárásáig többféle állapota lehet.
Információs vagyon: adatok, információk, szellemi, erkölcsi javak összessége.
Információvédelem: az informatikai rendszerek által kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme.
Jogosultság: a lehetőség megadása az informatikai rendszerben végzendő tevékenységek végrehajtására.
Kártékony kód: nem kívánt eseményt kiváltó utasítások kódsorozata.
Katasztrófa: az informatikai rendszer folyamatos és rendeltetésszerű működésének megszakadása.
Kensington zár: hordozható eszközökön található foglalat és egy jellemzően acélsodronyból álló drótból és kulcsos vagy számzárás zárszerkezetből álló lakat, melynek használatával fix ponthoz rögzíthetők az eszközök.
Kockázat: az informatikai fenyegetettség mértéke, amely valamely fenyegető tényezőből ered és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat két részből, a kárnagyságból és a bekövetkezés gyakoriságából tevődik össze. Az Infotv. szerint a

kockázat a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.
Kontrollok-óvintézkedések: mindazok a fizikai-, adminisztratív-, technikai-, technológiai módok, eljárások, amelyeket védelmi célból tettek meg és a kockázatot csökkentik.
Kritikus és biztonsági frissítés: a szoftver gyártója által kritikus vagy biztonsági frissítésként besorolt szoftvermódosítás.
Különleges személyes adat:
a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;
Külső fél: Lásd „Külső személy".
Külső személy: az Egyetemmel szerződéses kapcsolatban álló személy vagy szervezet, aki vagy amely az Egyetem informatikai rendszerével kapcsolatba kerülhet.
Külső szolgáltató: az egyetemi informatikai infrastruktúrától különálló infrastruktúrával rendelkező szervezet (pl: Office365.).
Legális szoftver: az a szerzői jog védelme alatt álló szoftvertermék, amely legalitásának igazolásához minden szükséges dokumentum (licenc, számla, szállítólevél, ajándékozási szerződés, stb.) rendelkezésre áll, valamint a használata a szoftver licenc szerződés előírásainak megfelelő módon történik.
Megbízható forrás: elektronikus anyagok olyan kibocsátója (küldője, publikálója), amelyben a felhasználó megbízik vagy egy külső hitelesítési szolgáltató megbízhatónak jelölte.
Megbízható működés: az informatikai rendszerek, és az általuk kezelt adatok által hordozott információk rendelkezésre állásának és funkcionalitásának védelme.
Mentés: informatikai folyamat, amelynek során az informatikai rendszerben digitálisan tárolt vagy használatban lévő fontos adathalmazokról egy speciális eszközzel egy speciális adathordozóra (mentési médium) másolatokat készítenek.
Mobil eszköz: a hordozható eszközök kategóriájába különböző eszközök tartoznak: hordozható számítógépek (laptop), táblagépek, tenyérszámítógépek (PDA), mobiltelefonok, adathordozók (USBpendrive, stb.).
Mobil kód: olyan szoftver vagy kód, mely általában egy távoli számítógépről, hálózaton keresztül letöltve, határozott telepítési vagy indítási procedúra nélkül fut vagy futtatható a kliens gépen. Ilyenek például a scriptek (JavaScript, VBScript), Flash animációk, Java kisalkalmazások, MS Office dokumentumok makrói, ActiveX vezérlők.
MS (rövidítés): Microsoft.
Nem mozdítható tárgy: rögzített tárgy, amelynek eltávolításához különleges eszköz, szerszám használata szükséges.
Rendelkezésre állás: az informatikai rendszer tényleges állapota, amely megvalósul, ha a rendszer szolgáltatásai egy meghatározott időben hozzáférhetők és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva. Az Infotv. szerint a rendelkezésre állás annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
Sértetlenség: az adat olyan tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes, ép, módosulatlan. Informatikai rendszer tulajdonság, amely adott, ha a rendszerben kezelt adatokat, illetve az adatkezelést megvalósító összes többi rendszer komponenst csak az arra jogosultak és csak dokumentáltan változtatják meg, emellett minden

egyéb (véletlen vagy szándékos) módosulás kizárt — vagyis az adatok és feldolgozási folyamataik pontosak és teljesek. Az Infotv. szerint a sértetlenség az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
Személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés.
Távoli kapcsolat: belső hálózati erőforrások elérése, külső hálózatból titkosított kommunikációs csatornán keresztül. Távoli kapcsolatnak minősül a VPN hozzáférés. Nem minősül távoli kapcsolatnak a levelezési fiókba való belépés.
Teljes körű védelem: teljes körűnek nevezik az informatikai rendszer védelmét, ha az informatikai rendszer összes elemére kiterjed.
Üzleti titok: a működéshez, az üzletmenethez és a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette.
Védelmi intézkedés: a fenyegetettség bekövetkezési valószínűsége, illetve a bekövetkezéskor jelentkező kár csökkentésére szervezési- vagy technikai eszközökkel tett intézkedés.
Védelmi rendszer: a védelmi rendszer az informatikai rendszer megfelelő szintű biztonságának garantálása érdekében alkalmazott fizikai-, logikai- és adminisztratív védelmi intézkedések összessége.
Védendő dokumentum: az adatkezelési szabályzat alapján minősített dokumentum.
Védendő információ: az adatkezelési szabályzat alapján minősített információ.
Végpontvédelem: olyan komplex megoldás, amely védelmet nyújt a kártékony programok okozta adatvesztés ellen, vírusvédelmet, kémprogram-elhárítást, behatolásvédelmet, illetve eszköz- és alkalmazáskezelést valósít meg, ezáltal biztosítja a rendszerek és fontos adatok rendelkezésre állását.
Vírus: olyan program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Többnyire rosszindulatú, más állományokat használhatatlanná, sőt teljesen tönkre is tehet.
Vírusvédelmi rendszer: a vírusvédelmi rendszer és a hozzá kapcsolódó védelmi mechanizmusok feladata az informatikai rendszerhez kapcsolódó vírusok felkutatása, működésük, aktív vagy passzív károkozásuk megakadályozása, illetve – lehetőség szerint – megsemmisítésük.
VPN: Virtuális magánhálózat egy meglévő számítógéphálózaton, általában nyílt internet hálózaton felépített kapcsolat. A VPN-en keresztül átmenő adatok titkosítva vannak, az eredeti hálózaton nem értelmezhetők.
Zárt védelem: Zártnak nevezik az informatikai rendszer védelmét, ha az összes releváns fenyegetést figyelembe veszi.

4. AZ INFORMATIKAI RENDSZER ÁLTALÁNOS BIZTONSÁGI ALAPELVEI – INFORMATIKAI BIZTONSÁGI POLITIKA

a) Az Egyetem az általa kezelt adatok, valamint informatikai rendszere tekintetében a felmerülő kockázatokkal arányos egyenszilárdságú védelmet alakít ki.

b) Az alkalmazott informatikai rendszerek és azok üzemeltetési rendje biztosítják a rendszer és a rendszerben feldolgozandó adatok rendelkezésre állását, hitelességét, sértetlenségét és titkosságát azok teljes feldolgozási folyamatában.

c) Az Egyetem az információvédelem területén biztosítja az informatikai rendszer gyártói ajánlásoknak és biztonsági követelményeknek történő megfelelését.

d) Az Egyetem az információ-feldolgozás és az informatikai szolgáltatások folyamatosságának biztosítására mentési eljárást működtet az adatok biztonsági másolatának készítésére.

e) Az Egyetem az informatikai biztonsági megoldásokat úgy alakítja ki, hogy azok a rendszerek mindennapi alkalmazásának és üzemeltetésének hatékonyságát a lehető legkisebb mértékben befolyásolják.

f) Az informatikai rendszer alkalmazására és üzemeltetésére vonatkozó szervezeti és működési rendeket, nyilvántartási és tájékoztatási szabályokat, az informatika alkalmazásából eredő biztonsági kockázatok figyelembevételével úgy alakítja ki, hogy a felelősségi körök és az egyértelmű személyes felelősségek meghatározhatók legyenek.

g) A felelősségek meghatározása mellett kiemelt hangsúlyt kap a biztonsági tudatosság szintjének folyamatos fejlesztése.

h) Az Egyetem informatikai biztonsági szabályzati rendszerét a vonatkozó jogszabályok, hazai és nemzetközi szabványok és ajánlások alapján alakítja ki.

i) Az Egyetem kiemelt figyelmet fordít a használt szoftverek jogtisztaságára, mindent megtesz a jogtiszta szoftver használat érdekében és az illegális használat, illetve másolás ellen.

5. FELELŐSSÉGEK, HATÁSKÖRÖK, ELKÖTELEZETTSÉGEK AZ IT BIZTONSÁG TERÜLETÉN

5.1 Általános

a) Az Egyetem minden munkatársa, hallgatója, valamint minden, az Egyetemmel szerződésben lévő informatikai alvállalkozó és természetes személy köteles

   i. az Informatikai Biztonsági Szabályzat rendelkezéseit, munkaterületére meghatározott előírásokat betartani és betartatni,

   ii. munkaterületén az adatbiztonságot és üzleti titkokat megtartani, az adatvédelemmel érintett adatok nyilvánosságra hozatalát megakadályozni.

b) Az Egyetem minden munkatársa és hallgatója köteles

   i. az Informatikai Biztonsági Szabályzatban előírt ellenőrzések és az auditok sikeres megvalósítását elősegíteni és támogatni;

ii. tudomásul venni, hogy az informatikai szervezet Főosztályvezetője és Osztályvezetői, valamint az Informatikai Biztonsági Felelős előzetes bejelentés nélkül ellenőrizheti az informatikai biztonsághoz kapcsolódó utasítások, szabályzatok betartását.

5.2 Kancellár

5.2.1 Elkötelezettség

Az Egyetem kancellárja elkötelezett az informatikai biztonság megvalósításában, külön is hangsúlyozva, hogy

a) legyen alkalmas az informatikai rendszer a feldolgozott adatok titkosságát, hitelességét, sértetlenségét, valamint magas szintű rendelkezésre állását garantálni,

b) álljon rendelkezésre az Egyetem működését biztosító informatikai háttér,

c) legyenek biztosítottak a működés fenntartásához és az informatikai fejlesztésekhez szükséges erőforrások.

5.2.2 Felelősség

Az Egyetem kancellárja kinyilvánítja az informatikai biztonságért való felelősségét

a) egy olyan informatikai biztonsági szervezeti struktúra létrehozásáért, amely az informatikai biztonság szabályzati rendszerének kidolgozója, és a megfogalmazott biztonsági eljárások működtetésének ellenőrzője és értékelője,

b) a felhasználók elkötelezettségének megteremtéséért az informatikai biztonság követelményeinek érvényesítésére, a biztonságtudatosság erősítése és a szabályzatok betartása érdekében; a felhasználók felelősségének megállapításáért, és a mulasztások szükség szerinti szankcionálásáért.

5.2.3 Képviselet

A kancellár biztosítja az informatikai biztonsági követelmények és eljárások kidolgozását, azok megvalósításának ellenőrzését az Informatikai Főosztályvezetőn és az Informatikai Biztonsági Felelősön keresztül.

5.3 Informatikai Főosztályvezető

5.3.1 Felelőssége

Az Informatikai Főosztályvezető felelősséggel tartozik az informatikai rendszer működtetéséért.

Az Informatikai Főosztályvezető az Egyetem kancellárjának támogatásával viseli a teljes felelősséget az informatikai biztonság szervezési szintű megvalósításáért, valamint támogatja az informatikai védelmi intézkedések meghatározását.

5.3.2 Jogosultsága

Az Informatikai Főosztályvezető jogosult

a) az informatikai rendszer teljes körű ellenőrzésére;

b) az informatikai biztonságot érintő minden szabályzat, utasítás és dokumentum véleményezésére.

c) az informatikai biztonságot érintő kérdésekben – szükség esetén a kancellárral egyeztetett – utasítás adására

5.3.3 Feladata

a) az informatikai rendszer Informatikai Biztonsági Szabályzatnak megfelelő működtetése;

b) a biztonsági elvárások érvényesítése az informatika szervezet üzemeltetési feladatainak végrehajtása során;

c) az általa érzékelt vagy ismert kockázatokról az Informatikai Biztonsági Felelőst tájékoztatni;

d) az informatikai biztonságot érintő dokumentumok és utasítások előterjesztése és véleményezése.

5.4 Informatikai Főosztály Osztályvezetői

5.4.1 Felelőssége

Az osztályvezető felelősséggel tartozik az irányítása alatt álló terület tevékenységéért.

Az Informatikai Osztályvezetők az Informatikai Főosztályvezető irányításával végzik munkájukat, felelősök a területükön a biztonság valamint a védelmi intézkedések megvalósításáért.

5.4.2 Jogosultsága

Az osztályvezető jogosult

a) a felügyelete alatt álló informatikai rendszer(ek) ellenőrzésére;

b) az informatikai biztonságot érintő szabályzatokra, utasításokra és dokumentumokra vonatkozóan javaslattételre.

c) az informatikai biztonságot érintő kérdésekben – szükség esetén az informatikai főosztályvezetővel egyeztetett – utasítás adására.

5.4.3 Feladata

a) a felügyelete alatt álló informatikai rendszerek Informatikai Biztonsági Szabályzatnak megfelelő működtetése;

b) a biztonsági elvárások érvényesítése az informatikai szervezet üzemeltetési feladatainak végrehajtása során;

c) az általa érzékelt vagy ismert kockázatokról az Informatikai Biztonsági Felelőst tájékoztatni;

d) az informatikai biztonságot és a tevékenységi területét érintő dokumentumok és utasítások előterjesztése és véleményezése.

5.5 Informatikai Biztonsági Felelős (a továbbiakban: IBF)

Az Informatikai Biztonsági Felelős az Egyetem Informatikai Főosztályával együttműködésben látja el feladatait, kinevezés, vagy megbízás alapján.

5.5.1 Felelőssége

Az Informatikai Biztonsági Felelős felelősséget vállal:

a) az Informatikai Biztonságpolitika, az Informatikai Biztonsági Szabályzat kidolgozásáért és szakmai tartalmáért;

b) az informatikai biztonsághoz kapcsolódó utasítások, szabályzatok és tervek kidolgozásáért, azok összhangjáért és a betartásának ellenőrzéséért

c) az informatikai biztonság tudatosításáért;

d) a biztonsági előírásokat megsértőkkel szemben szükséges intézkedések kezdeményezéséért;

e) az informatikai biztonságot érintő rendszerek ellenőrzéséért.

5.5.2 Jogosultságai

Az Informatikai Biztonsági Felelős jogosult

a) az Informatikai Biztonsági Szabályzat előírásainak betartását bármely szervezeti egységnél ellenőrizni;

b) az informatikai rendszer működtetésével, fejlesztésével, valamint az üzleti feldolgozásokkal kapcsolatos valamennyi dokumentumba betekinteni;

c) az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezni a Kancellárnál.

5.5.3 Feladata

1. Az Informatikai Biztonsági Felelős általános feladatai:

   a) közreműködik az informatikai biztonságot érintő rendszerek megvalósításában;

   b) előkészíti az Egyetem informatikai biztonsági tervét, figyelembe véve az Egyetem fejlesztési és informatikai stratégiai terveit;

   c) kezdeményezi új adatvédelmi eszközök vagy megoldások beszerzését;

   d) véleményezi az Egyetem informatikai fejlesztéseit az informatikai biztonság szempontjából;

   e) biztosítja a veszélyforrások körében bekövetkező változások folyamatos követését, és ezek alapján kezdeményezi a szükséges intézkedések meghozatalát;

   f) felméri az információtechnológia használatából adódó biztonsági kockázatokat a tervezés, beszerzés, üzemeltetés és az ellenőrzés területén;

   g) elvégzi, felülvizsgálja és aktualizálja az informatikai biztonsági rendszert;

   h) biztosítja az adat- és információvédelmi feladatok folyamatos belső ismertetését, a képzési terv kidolgozását és oktatását;

   i) elkészíti jelentését az informatikai infrastruktúra elvárt biztonságos működésének a teljesüléséről éves rendszerességgel; a jelentés tartalmazza a biztonság szempontjából kritikus mérések eredményeit is az alábbiak szerint:

A minimálisan szükséges kontroll pontok az alábbiak:

Mérendő terület	Mérendő mennyiség	Beszámolóban
IT tevékenység	Szerverszobába való belépések naplózása	Nem
	Rendszergazdai hozzáférések (logikai) naplózása	Nem
Incidens	Észlelt behatolási kísérletek száma	Igen
	Bejelentett jelszó kompromittálódások száma	Igen
	Bejelentett vírusriasztások száma	Igen
Mentési rendszer	A teszt-visszatöltések száma, eredményei	Igen
	Visszatöltések száma, eredményei	Igen
Rendelkezésre állás	Rendszerek kieséseinek száma, ezek oka, időtartama	Igen
Kapacitásinformációk	Kritikus rendszerekre vonatkozó teljesítményadatok jelentős változása	Igen
	Tárolási kapacitásokra vonatkozó információk	Igen
Ellenőrzések eredményei	Feltárt hiányosságok, és azok megszüntetésére vonatkozó intézkedések	Igen
Oktatás helyzete	IT biztonsági oktatásban részt vett személyek száma	Igen
IT biztonsággal kapcsolatos fegyelemsértések	IT biztonságot megsértő személyekre vonatkozó fegyelmi statisztikák	Igen
Az IT biztonsági rendszer összesített értékelése	Az IT biztonsági rendszer szintjére vonatkozó megállapítások, javaslatok	Igen

j) elkészíti a veszélyforrás elemzés eredménye alapján a következő évi munkatervét.

2. Az Informatikai Biztonsági Felelős ellenőrzési feladatai:

a) elkészíti és végrehajtja az Informatikai Biztonsági Szabályzat alapján az éves informatikai biztonsági ellenőrzési programot;

b) ellenőrzi az informatikai biztonsági előírások betartatását;

c) elvégzi a teljes informatikai rendszer biztonságának éves összefoglaló értékelését, és ennek eredményéről a Kancellárt írásban tájékoztatja.

3. Az Informatikai Biztonsági Felelős dokumentációs feladatai:

a) felülvizsgálja az Informatikai Biztonságpolitika, Informatikai Biztonsági Szabályzat dokumentumokat és azok kapcsolódó dokumentumait legalább 2 évente és javaslatot tesz azok módosítására;

b) véleményezi az informatikai biztonság tárgykörébe tartozó szabályzásokat, utasításokat;

c) a szabályzatok módosításának szakmai elkészítéséhez az Informatikai Biztonsági Felelős jogosult igénybe venni az informatikai szervezet munkatársait, az Informatikai Főosztályvezető jóváhagyásával.

5.6 A felelősségek meghatározásához kapcsolódó dokumentumok

Az alábbi dokumentumokat jelen szabályzat mellékletei tartalmazzák:

Felhasználói nyilatkozat – 1. sz melléklet

Titoktartási nyilatkozat – 2. sz. melléklet

Az egyetem informatikai biztonságára vonatkozó, illetve ahhoz kapcsolódó jogszabályok felsorolása – 3. sz. melléklet

6. INFORMATIKAI BIZTONSÁGI SZABÁLYOK

6.1 Az informatikai biztonság vezetői irányítása

Az Egyetem célja, hogy a szakmai követelményekkel és a vonatkozó jogszabályokkal összhangban biztosítsa a Szenátus által elfogadott iránymutatást és vezetői támogatást az informatikai biztonság megvalósításához.

6.1.1 Informatikai biztonsági szabályok

Az Informatikai Biztonsági Politikában (4.pont) meghatározott alapelvek, a kapcsolódó megfelelőségi követelmények, és a kockázatfelmérés eredménye alapján ki kell alakítani az Egyetem informatikai biztonsági szabályozási rendszerét. A szabályozási rendszer kialakítása és naprakészen tartása az Informatikai Biztonsági Felelős feladata.
Az informatikai biztonsági szabályzatokat, illetve azok kivonatát minden munkatárs, hallgató és az olyan külső érdekelt felek felé kommunikálni kell, akiknek a feladatára hatással van, az ahhoz szükséges mértékben.

6.1.2 Az informatikai biztonsági szabályzatok felülvizsgálata

Az informatikai biztonsági szabályzati rendszerbe tartozó szabályzatokat legalább két évente felül kell vizsgálni, illetve az informatikai rendszer jelentős változásai esetén. A felülvizsgálat az Informatikai Biztonsági Felelős feladata.

7. AZ INFORMATIKAI BIZTONSÁG KERETRENDSZERE

Keretrendszeren az informatikai biztonság kialakításában, működtetésében résztvevő munkatársak, szabályozások, alkalmazások, informatikai biztonsági rendszerek egészét értjük.

7.1 Belső keretrendszer

Az Egyetem célja egy olyan menedzsment keretrendszer kialakítása, mely képes az informatikai biztonság megvalósítására, működtetésére és felügyeletére.

7.1.1 Informatikai biztonsági szerepek és felelősségek

Az informatikai biztonsággal kapcsolatos felelősségeket meg kell határozni, és személyekhez kell rendelni. A szerepkörökhöz kapcsolódó felelősségeket a 3. fejezet tartalmazza, illetve ezen szabályzat további feladatokat is meghatároz az egyes fejezetekben.

7.1.2 Feladatkörök szétválasztása

Meg kell előzni az Egyetem informatikai vagyonelemeinek jogosulatlan, vagy véletlen módosítását, illetve az azokkal történő visszaélést.
Az egymással összeférhetetlen feladatköröket és felelősségi területeket szét kell választani. Alapelv, hogy egy tevékenység végrehajtását és annak ellenőrzését, illetve egy tevékenység kérelmezését és jóváhagyását ne végezze ugyanaz a személy.
Továbbá az informatikai rendszerek fejlesztését és üzemeltetését, valamint az adatbázisok és egyéb infrastruktúra elemek rendszergazdai tevékenységét lehetőleg ne végezze ugyanaz a személy. Amennyiben létszám okok miatt a tevékenységek szétválasztása nem oldható meg, abban az esetben kiegészítő kontrollokat kell alkalmazni. (pl. a tevékenység független személy által történő felügyelete)

7.1.3 Kapcsolat a hatóságokkal

Az Informatikai Biztonsági Felelősnek, a Kancellár tájékoztatása mellett kapcsolatot kell tartania az illetékes hatóságokkal.

7.2 Mobil eszközök és távmunka

Az Egyetem célja, hogy biztosítsa a hordozható eszközök biztonságos használatának feltételeit, valamint a biztonságos távoli munkavégzést.

7.2.1 Hordozható eszközök használatának szabályozása

A mobil eszközök használatával járó kockázatok csökkentése érdekében az Egyetem a következő intézkedéseket írja elő:

- A hordozható eszközökben levő adattárolókon az eszközök titkosítási funkcióját (amennyiben van ilyen) be kell kapcsolni, ha azok bizalmas vagy szigorúan bizalmas információt, illetve egyetemi dolgozók, vagy hallgatók személyes adatait tartalmazzák;
- Erős jelszavakat (10.4.3 fejezet szerint), vagy legalább 4 jegyű PIN kódot vagy biometrikus azonosítást kell használni;
- Az eszköz naprakész vírusvédelemmel kell rendelkezzen (amennyiben van ilyen);
- Az eszköz operációs rendszere minden kritikus és biztonsági frissítéssel kell rendelkezzen, ennek hiányában a hálózathoz való hozzáférést az Egyetem korlátozhatja;
- A felhasználó tudomásul veszi, hogy amennyiben él az Egyetem informatikai rendszere távoli elérésének lehetőségével, ezzel együtt jár az eszköz adattartalmának távoli törlési lehetősége. Ilyen távolból történő adattörlést az informatikai üzemeltetés csak indokolt esetben, a felhasználó bejelentése alapján az Informatikai Főosztályvezető engedélyével végezhet, melyet írásban indoklással dokumentálni kell;
- Az Egyetem közalkalmazottai olyan mobil eszköz elhagyása, elvesztése vagy másnak tartós használatra való átadása esetén, amelyen be van állítva valamilyen egyetemi informatikai

szolgáltatás elérése, kötelesek bejelentést tenni a helyi informatikai szervezetnek a szolgáltatás és az eszköz közti kapcsolat törlése érdekében;

A felhasználó saját tulajdonában levő mobil eszközökre vonatkozó technikai követelmények biztosításáért a felhasználó tulajdonos felel. Az Egyetem tulajdonában levő eszközökre vonatkozóan a feltételek biztosítását az üzemeltetésért felelős szervezet biztosítja.

Mobil eszközök fizikai védelme

A hordozható eszközök mobilitásuknál fogva fokozott veszélynek vannak kitéve a fizikai biztonságukkal kapcsolatos fenyegetettségekkel szemben. A hordozható eszközök fizikai biztonsága érdekében az alábbi szabályokat kell betartani:

a) Mobil eszközt, illetve egyetemi információt tartalmazó adathordozót tilos felügyelet nélkül hagyni. Repülőn, autóbuszon, vagy vasúton történő szállítás esetén a hordozható eszközöket kézipoggyászként kell szállítani. A folyamatos felügyeletet ez alatt is biztosítani kell.
b) a gyártó előírásait mindig be kell tartani az eszköz védelme érdekében;

7.2.2 Távmunka

A biztonságos távoli munkavégzés érdekében csak titkosított csatornán (mobil internet, felhasználó otthoni internet), és olyan eszközzel szabad az Egyetem informatikai rendszerébe távoli kapcsolatot indítani, amely végpontvédelemmel rendelkezik (amennyiben az eszközre elérhető ilyen megoldás).
A távmunka során is hozzáférhető, feldolgozott, illetve tárolt információ védelme érdekében a következő kontrollokat kell működtetni:

a) az eszköz naprakész vírusvédelemmel kell rendelkezzen,
b) az eszköz operációs rendszere minden kritikus és biztonsági frissítéssel kell rendelkezzen, ennek hiányában a hálózathoz való hozzáférést az Egyetem korlátozhatja,
c) a kapcsolódás csak korszerű technológiákra épülő titkosított kommunikációs csatornán keresztül engedélyezett,
d) a távoli használat naplózásra kerül.

A távoli karbantartási és diagnosztikai tevékenységeket is a távoli munkavégzésnél meghatározott kontrollok alkalmazása mellett kell végezni.
A karbantartást és rendszertámogatást végző személyek belépési jogosultságait kizárólag a szerződésben rögzített, illetve esetileg igényelt karbantartás idejére lehet engedélyezni.

8. AZ EMBERI ERŐFORRÁSOK BIZTONSÁGI KOCKÁZATAINAK MINIMALIZÁLÁSA

8.1 A jogviszony kezdete előtti követelmények

Az Egyetem célja annak biztosítása, hogy közalkalmazottai és szerződéses munkatársai megértsék informatikai biztonsággal kapcsolatos felelősségeiket, és alkalmasak legyenek azon szerepkörök és feladatok ellátására, amelyekben foglalkoztatják őket.

A pályázó munkatársakról alkalmazás előtt – a leendő munkahelyi vezető vagy az IBF igénye esetén – informatikai biztonsági szempontú referencia ellenőrzést kell végezni a Humánpolitikai Osztály közreműködésével.

Az Informatikai Biztonsági Szabályzatban kerültek szabályozásra az informatikai biztonsági feladatok és felelősségek, az közalkalmazottak ennek tudomásul vételét a jogviszony kezdetekor aláírásukkal elismerik. A munkatársak általános feladatait a munkaszerződés, és az adott munkaköri leírás tartalmazza.
A szerződéses munkavállalókkal kötött szerződésekben meg kell határozni az informatikai biztonságra vonatkozó felelősségeket mind a szerződött fél, mind az Egyetem oldaláról. Amennyiben a munkavégzés kapcsán szükséges, a szerződés mellékleteként kell beépíteni a Titoktartási Nyilatkozatot.

8.2 A munkaviszony fennállása során betartandó követelmények

Az Egyetem célja, hogy biztosítsa, hogy a munkatársak tisztában legyenek az informatikai biztonsággal kapcsolatos felelősségeikkel, és azoknak megfelelően járjanak el.

8.2.1 Vezetői felelősség

Az Egyetem minden vezető beosztású munkatársának meg kell követelnie, hogy a beosztott munkatársak tartsák be a hatályos informatikai biztonsági szabályzatokat és eljárásrendeket, az abban foglaltak szerint járjanak el.

8.2.2 Az informatikai biztonság tudatosítása, oktatása és képzése

Az Egyetem minden munkatársának a munkaköréhez kapcsolódó hatályos szabályzatokat ismernie kell, azok változása esetén frissítenie kell az ismereteit.
Minden személynek, aki az Egyetem informatikai rendszeréhez hozzáféréssel rendelkezik, a munkavégzés megkezdése előtt, és ezt követően évente, vagy amikor a szabályozásban, illetve az információs rendszerben bekövetkezett változás azt indokolja, informatikai biztonsági ismereteket fejlesztő oktatásban és képzésben kell részesülnie. Az informatikai biztonsági oktatás megszervezése az Informatikai Biztonsági Felelős feladata.

A biztonságtudatossága vonatkozó képzéseken jelenléti ívet kell vezetni, és a képzésen résztvevőkkel a képzés megtörténtét igazolni kell. A képzések jelenléti ívét az Informatikai Biztonsági Felelős kell megőrizze a képzést követő 1 évig.

8.2.3 Fegyelmi eljárások

Az Informatikai Biztonsági Szabályzat, illetve a kapcsolódó szabályozó dokumentumokban foglaltak megsértése esetén a szabályzat megszegőjével szemben az Egyetem Kancellárjának döntése szerint, lehetséges felelősségre vonási eljárást kezdeményezni, vagy érvényesíteni kell a vonatkozó szerződésben meghatározott következményeket, továbbá meg kell vizsgálni az egyéb jogi lépések szükségességét.
A szabályok kevésbé súlyos megsértése esetén a szabálysértő személyt írásban figyelmeztetni kell. A szabálysértés súlyosságának megítélése az Informatikai Biztonsági Felelős és az Informatikai Főosztályvezető javaslata alapján a Kancellár döntése. A figyelmeztetés az Informatikai Biztonsági Felelős feladata.

8.3 A jogviszony megszűnése és megváltozása

Az Egyetem célja, hogy meghatározza az Egyetemmel fennálló közalkalmazott és egyéb jogviszonyok megszűnése esetén továbbra is fennálló informatikai biztonsági felelősségi köröket.

8.3.1 A jogviszony megszüntetéséhez vagy megváltoztatásához kapcsolódó felelősségek

A közalkalmazotti jogviszony, illetve az egyéb szerződéses jogviszony megszűnése vagy megváltozása után is a titoktartási kötelezettség – amennyiben erről a titoktartási nyilatkozat és/vagy a szerződés másképpen nem rendelkezik – fennáll.
A jogviszony megszűnésével vagy megváltozásával egyidejűleg a munkatárs közvetlen felettesének intézkednie kell a személynek az informatikai rendszerekben levő hozzáférési jogosultságainak visszavonásáról. A jogosultságok visszavonását automatizmusok támogatják, amely rendszerekben ez megvalósítható.
A hozzáférési jogosultság visszavonását követően más felhasználónak a távozott felhasználó levelezéséhez, illetve saját személyes könyvtárához teljes hozzáférést az Informatikai Főosztály biztosíthat. Feladatai ellátásában tartósan korlátozott közalkalmazott esetében, a közalkalmazott munkahelyi vezetőjének írásbeli kérése alapján más felhasználónak az alkalmazott levelezéséhez, illetve saját személyes könyvtárához hozzáférést az Informatikai Főosztály biztosíthat.
A jogviszony megszűnésével vagy megváltozásával érintett munkatárs kötelessége gondoskodni

a) legkésőbb az utolsó munkanapon az elektronikus levelező rendszerben automatikus válaszüzenet beállítása, mely értesítést tartalmaz a jogviszony megszűnéséről és a továbbiakban a feladatot ellátó személy elérhetőségeiről,
b) valamint az informatikai rendszerekben tárolt személyes adatainak törléséről.

A kilépést megelőző átadás átvételi folyamat részét kell, hogy képezze az informatikai rendszerben tárolt elektronikus dokumentumok átadás-átvétele is, mivel az Egyetemmel fennálló jogviszony megszűnését követően a felhasználó személyes könyvtárához és a postafiókjához való hozzáférést az informatikai üzemeltetés megszűnteti. A kilépő munkavállaló nyilatkozata alapján a hozzáférés más részére beállítható.

A jogviszony megszűnésekor meg kell előzni, hogy az érintett személy veszélyeztesse az informatikai rendszerek biztonságát.

9. A VAGYONELEMEK KEZELÉSE

9.1 A vagyonelemekért viselt felelősség

Az Egyetem célja, hogy azonosítsa és nyilvántartsa az informatikai vagyonelemeket, és meghatározza azok védelméhez kapcsolódó felelősségeket. A személyi használatba adott vagyonelemek felhasználónak történő használatba adásáról átadás-átvételi jegyzőkönyv készül.

9.1.1 Vagyonnyilvántartás

Az információs vagyonelemeket és az információ feldolgozó eszközöket azonosítani kell, és műszaki szempontból nyilván kell tartani. A nyilvántartás vezetéséért az Informatikai Osztályvezetők felelősek. Az Informatikai Biztonsági Felelős alkalomszerűen ellenőrzi a nyilvántartás megfelelőségét.

A nyilvántartásnak tükröznie kell a rendszerek aktuális állapotát. Az egyes rendszerelemek változásának időpontjában a nyilvántartást aktualizálni kell.
A nyilvántartásnak tartalmaznia kell az informatikai rendszer szoftver és hardver elemeit. Az elemekről az egyértelmű azonosításhoz szükséges, – hardver elemek esetén az alapvető konfigurációt is tartalmazó, szoftver elemeknél a verzió egyértelmű azonosítását lehetővé tevő – adatokat kell rögzíteni.

9.1.2 A vagyonelemek felelősei

A vagyonnyilvántartásban szereplő minden vagyonelem esetén az Egyetem Eszközök és források leltározási és leltárkészítési szabályzata 3. számú mellékletében foglaltak szerint kell eljárni.

9.1.3 A vagyonelemek elfogadható használata

Az információ feldolgozó eszközök használatára vonatkozó szabályok az alábbiak:

a) A Felhasználó köteles az eszközöket és a szoftvereket rendeltetésüknek megfelelően használni.
b) A Felhasználó köteles a tőle elvárható gondossággal eljárni az eszközök használata során. Az eszközöket védeni köteles rongálás vagy szándékos károkozás ellen.
c) A Felhasználó felelős az informatikai eszközök állagmegóvásáért, és köteles figyelmeztetni azon Felhasználókat, akik nem a jelen szabályzat szellemében járnak el.
d) A Felhasználó a rábízott eszközöket nem adhatja kölcsön harmadik személynek, kockáztatva így az eszköz épségét, és az esetlegesen rajta lévő adatok biztonságát és sértetlenségét.
e) A Felhasználó bármilyen hibát vagy sérülést észlel, azonnal jelentenie kell a helyi informatikai szervezetnek.
f) A Felhasználó a használatába adott eszközökön a munkavégzéséhez szükséges feladatokat végezheti, magán célokra csak korlátozott mértékben használhatja azt.
g) A Felhasználó az általa használt számítógépre programot nem telepíthet, és nem törölhet. Ilyen jellegű igény esetén értesítenie kell a helyi informatikai szervezetet.

Az egyes rendszerek felhasználói dokumentációi tartalmazzák a felhasználók által elérhető biztonsági funkciókat és azok hatékony alkalmazási módját.

Az Egyetem a felhasználók számára az egyetemi hálózaton keresztül Internet hozzáférést biztosít. Az egyetemi hálózat és az Internet használata során szigorúan tiltott tevékenységek az alábbiak:

a) minden olyan tevékenység, ami a hatályos jogszabályokba ütközik, különös tekintettel az alábbiakra: mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; szoftver szándékos illegális terjesztése;
b) profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése;
c) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, módosítása, megrongálása, megsemmisítésére irányuló tevékenység;

d) a hálózat biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése (pl. vírusok, trójai programok, hacker eszközök, férgek);
e) hálózati forgalom lehallgatása, megfigyelése, kivéve, ha ez az adott munkakörhöz kapcsolódik;
f) a szolgáltatások blokkolását, lassítását célzó támadás, az azonosítási, illetve biztonsági intézkedések megsértésére irányuló kísérlet, valamint az egyéb azonosítóhoz, számítógéphez vagy hálózathoz történő illetéktelen hozzáférési kísérlet;
g) tilos továbbá:
    i. sértő, társadalomra veszélyes, jó erkölcsbe ütköző szöveg, kép, ábra vagy egyéb formájú információ publikálása, letöltése;
    ii. az interneten elérhető szolgáltatást, bármilyen törvényt, szabályozást, szabványt, nemzetközi egyezményt vagy díjszabást sértő módon használni;
    iii. bármelyik számítógép-hálózat biztonságát rombolni, illetve gyengíteni, más felhasználó jogosultságát jogosulatlanul használni;
    iv. bármilyen internetes végpontra, illetve hálózati eszközre jogosulatlanul csatlakozni, vagy ezzel próbálkozni;
    v. bármely végpont működését megzavarni vagy azt az Egyetem hálózatáról vagy annak igénybevételével szándékosan túlterhelni (DOS támadás);
    vi. engedély nélkül egyetemi tulajdonú eszközöket internetes számítógép erőforrás megosztásokhoz (például: gyógyszerkutatás, SETI számításokhoz, RSA törésekhez) használni;
    vii. a hálózatot a szerzői jogvédelem alá eső anyagok átvitelére használni (még közvetetten is), ha az átvitel során mások szerzői joga sérül;
    viii. tilos kikapcsolni a munkaállomásra telepített biztonsági szoftvereket, eszközöket;
    ix. az internet segítségével egyetemi tevékenységi-, vagy érdekkörbe tartozó állományok, információk kijuttatása, külső kiszolgálókra való feltöltése, illetve bármilyen módon történő megosztása (kivéve az Egyetem által igénybe vett külső szolgáltatások);

9.1.4 A vagyonelemek visszaszolgáltatása

Minden munkatárs vissza kell szolgáltassa a használatában levő összes olyan informatikai vagyonelemet, melyet az Egyetem biztosított, legkésőbb a közös megegyezés alapján meghatározott időpontban vagy azon a napon, amikor megszűnik az Egyetemmel fennálló közalkalmazotti vagy egyéb szerződéses jogviszonya. A Vagyonelemek visszaszolgáltatása az átadás-átvételi jegyzőkönyv alapján történik.

9.2 Információosztályozás

Az Egyetem célja, hogy az általa kezelt, illetve feldolgozott információ a szervezetben betöltött fontosságával arányos védelemben részesüljön, és az Egyetem munkatársai az előírt védelmi szint által meghatározott módon járjanak el.

9.2.1 A Szervezet által kezelt információ osztályozása

Az Egyetem működése során az informatikai rendszerben az adatok kezelése a mindenkor hatályos jogszabályoknak megfelelően kell, hogy történjen.
Az információ biztonsági osztályba sorolásának és az ezzel kapcsolatos védelmi intézkedéseknek figyelembe kell venniük az igényeket arra vonatkozóan, hogyan osszák meg kölcsönösen az információt, vagy milyen módon korlátozzák azt, mi a teendő a jogosulatlan hozzáférés vagy az információrongálás esetén.
A biztonsági szintek alapján osztályozott adatokat az Egyetem szempontjából megállapított értékükkel és érzékenységükkel, vagy az adat sértetlenségével és rendelkezésre állásával kifejezve kell címkézni.
Az informatikai rendszerben feldolgozott és tárolt üzleti és egyéb adatok osztályba sorolásáért az illetékes Adatgazda felel.
Adatgazdák a szervezeti egységek vezetői, akik a náluk keletkezett adatok vonatkozásában felelősek az osztályozásért, valamint az adatokat kezelő rendszerek tekintetében döntenek a jogosultságok megadásáról. Az adatok osztályozását az Informatikai Biztonsági Felelős felülvizsgálja, és amennyiben nem ért egyet az osztályozással egyeztetést kezdeményez az érintett adatgazdával. Egyet nem értés esetén az Informatikai Főosztályvezető dönt.

Információ osztály	Meghatározás	Javasolt tárolási hely
PUBLIKUS	Az Egyetem azon adatai, amelyek mind az Egyetemen belül, mind azon kívül szabadon megismerhetőek.	fájl szerveren, illetve O365 tárhelyen, honlapon
ÜZLETI	Az Egyetem azon adatai, amelyekhez az Egyetem munkatársai szabadon hozzáférhetnek, de harmadik (külső) félnek a Kancellár, Rektor, vagy az Informatikai Főosztályvezető engedélye nélkül nem adhatók át.	O365 tárhelyen, fájl szerveren a szervezeti egység közös könyvtárában
BIZALMAS	Az Egyetemen belül is csak szűk körben hozzáférhető adatok köre, az adatok kezelése, feldolgozása során kiegészítő védelmi intézkedések (pl. titkosítás) alkalmazására lehet szükség.	fájl szerveren, jogosultság beállításokkal korlátozott hozzáféréssel

Az informatikai rendszer elemeinek biztonsági osztályba sorolását, az informatikai rendszerben feldolgozott és tárolt adatok biztonsági osztályba sorolásával összhangban, a megbízható védelem szempontjából az alábbi biztonsági osztályok egyikébe kell besorolni:

a) alap biztonsági osztály – ha az informatikai rendszer elemén publikus biztonsági osztályba sorolt adatok feldolgozása, illetve tárolása történik, vagy az informatikai rendszer elemének kiesése az informatikai rendszer leállását nem okozza.

b) kiemelt biztonsági osztály – ha az informatikai rendszer elemén Üzleti, vagy Bizalmas biztonsági osztályba sorolt adatok feldolgozása, illetve tárolása történik, vagy az informatikai rendszer elemének kiesése az informatikai rendszer részleges vagy teljes leállását okozza.

Az informatikai rendszer elemeinek és a biztonsági beállításainak elvárt védettségi szintjét, valamint a biztonsági beállításokra vonatkozó adatok különleges kezelésének szükségességét az elemek, illetve az adatok besorolásának függvényében az Informatikai Biztonsági Felelős feladata meghatározni.
Az informatikai rendszer kiemelt biztonsági osztályba sorolt elemei esetében hibatűrő megoldásokat javasolt alkalmazni mindazon rendszerek esetében, ahol ezt a biztonsági kockázat szintje megköveteli.

9.2.2 Az információk megjelölése

A Bizalmas osztályba sorolt információt tartalmazó kimenő adat adathordozóját célszerű a megfelelő osztályozási címkével ellátni.

A BIZALMAS besorolású adatokat lehetőleg titkosítva kell mobil eszközön tárolni.

Az Informatikai Főosztályvezető felelős azért, hogy az Egyetem informatikai rendszerére, vonatkozó fejlesztési és üzemeltetési dokumentációkat elkülönítve tárolják, és bizalmas minősítésű dokumentumként kezelve védjék az illetéktelen hozzáféréstől.

9.3 Adathordozók kezelése

Az Egyetem célja, hogy megelőzze az általa kezelt, illetve felügyelt adathordozókon tárolt információ jogosulatlan nyilvánosságra kerülését, módosítását, eltávolítását vagy megsemmisítését.

Amennyiben adathordozót tartalmazó eszközt javításra el kell szállítani az Egyetemről, abban az esetben a helyi Informatikai Osztályvezető előzetesen mérlegeli, hogy az adathordozó kiszerelésre kerüljön-e.

9.3.1 A cserélhető adathordozók kezelése

Az Egyetem által alkalmazott információ osztályba sorolási módszernek megfelelő eljárásokat kell működtetni a cserélhető adathordozók kezelésére. Az adathordozók kezelése során az adathordozó által tartalmazott adatok minősítésének megfelelően kell eljárni.

A felhasználók felelőssége, hogy a használatukban levő mobil adathordozókat megvédjék.

A mentésre, archiválásra szolgáló adathordozók tartalmáról nyilvántartást kell vezetni, azok kezelésére vonatkozó részletes eljárásokat a Mentési utasítás tartalmazza.

Bármely újrahasználható adathordozó tartalmát helyreállíthatatlanul törölni kell, ha arra már nincs szükség és az adathordozót az Egyetemtől elviszik (pl. selejtezés). Felelős az érintett Informatikai Osztályvezető.

Minden adathordozót biztonságos és védett környezetben kell tárolni a gyártói előírások szerint.

A felhasználóknak harmadik féltől kapott adathordozó használata esetén a használatot megelőzően az adathordozón vírusellenőrzést kell végrehajtson. Mobil adathordozóról

közvetlenül nem szabad indítható állományt futtatni. Ahol megoldható, ott az informatikai rendszerek ezt kikényszerítik.

9.3.2 Adathordozók selejtezése

Az adathordozókat, ha már nincsenek használatban, illetéktelen hozzáféréstől védett módon kell elhelyezni.
Az érzékeny információt tartalmazó adathordozókat biztonságos és védett módon kell tárolni, illetve oly módon kell az adatokat törölni, hogy azok visszaállítása ne legyen lehetséges.

Minden olyan adathordozót biztonságosan és dokumentáltan kell leselejtezni/újrahasznosítani, amelyekre az Egyetemnek már nincs szüksége.

A selejtezett nem újraírható eszközöket (pl. CD, DVD) fizikailag meg kell semmisíteni.

9.3.3 Adathordozó eszközök szállítása

Az információt tartalmazó adathordozókat a szállításuk során védeni kell a jogosulatlan hozzáféréstől, visszaéléstől vagy megrongálódástól.
Adathordozók szállítását az Egyetem ezzel megbízott munkatársa, vagy szerződött partnere végezheti, ez utóbbi esetben lezárt csomagban kell szállítani.

10. HOZZÁFÉRÉS FELÜGYELET

10.1 A hozzáférés-felügyelettel kapcsolatos követelmények

Az Egyetem célja, hogy az információhoz és az információ-feldolgozó eszközökhöz való hozzáférést korlátozza az arra jogosultak körére. A Felhasználó részére az informatikai rendszerekbe belépést engedélyezni csak és kizárólag abban az esetben szabad, ha a Felhasználó valamilyen módon azonosítja magát, és a rendszer hitelesíti.

10.1.1 Hozzáférés-felügyeletre vonatkozó szabályok

Az elvárható biztonsági szint biztosítása érdekében a Felhasználók hozzáférési jogait más-más személy határozza meg, és állítja be az informatikai rendszerben.
Az informatikai rendszereknek alkalmasnak kell lenni a felhasználók személyhez köthető azonosítására.
A jogosultságokat a munkavégzéshez minimálisan szükséges mértékű jogosultságokra kell korlátozni, a szükséges és elégséges ismeret elvének megfelelően.

Csoportos felhasználói fiók, vagy egy azonosító több felhasználó által történő használatát csak abban az esetben szabad engedélyezni, ha a rendszer a használatra más lehetőséget nem biztosít.
A felhasználók különböző adminisztrációs rendszerekben érvényes jogosultságait, hozzáféréseit nyilván kell tartani. A nyilvántartásért az Informatikai Főosztályvezető felel.

10.1.2 Hozzáférés hálózatokhoz és hálózati szolgáltatásokhoz

A felhasználók számára csak olyan hálózatokhoz és hálózati szolgáltatásokhoz való hozzáférést szabad elérhetővé tenni, amelyek használata szükséges és engedélyezett a számukra.

10.2 A felhasználói hozzáférések kezelése

Az Egyetem célja, hogy csak az arra jogosult felhasználók számára biztosítsa a hozzáférést a rendszerekhez és szolgáltatásokhoz, továbbá célja, hogy megelőzze a jogosulatlan hozzáférést. A hozzáférések igénylési folyamata e-mailben vagy elektronikus űrlap használatával történik.

10.2.1 Felhasználói fiókok létrehozása és törlése

A felhasználók és a hozzáférési jogok kiadását szabályozott módon kell megvalósítani. A jogosultsági igényeket a felhasználó közvetlen felettese igényli és az Informatikai Osztályvezető intézkedik a beállításról. A beállítás megtörténtéről az informatikai szervezet visszajelzést küld a felhasználónak és felettesének.

10.2.2 Felhasználói hozzáférés beállítása

A hozzáférési jogok beállítását az Egyetem informatikai üzemeltetési munkatársai végzik. Az új belépők automatikusan megkapják a szervezeti egységükhöz kapcsolódó csoport tagsághoz kapcsolodó jogosultságokat, valamint a 4. sz. mellékletben megjelölt Alap jogosultságokat.

10.2.3 Kiemelt (privilegizált) hozzáférési jogok kezelése

A kiemelt hozzáférési jogok kiadását és használatát korlátozni kell.
Az adminisztrátori felhasználói fiókokat üzemszerűen nem szabad használni. A rendszer adminisztrálási teendőket végző felhasználók külön felhasználói és adminisztrátori nevesített fiókkal rendelkeznek.
Abban az esetben, amennyiben a felhasználó az általa használt eszközön kiemelt (rendszergazdai) jogosultságot kap, teljeskörűen felel az eszközre az átadást követően telepítésre kerülő programok jogtisztaságáért, a programok frissítéséért, illetve az eszköz kártékony kód mentességéért. Ilyen esetben az Egyetem informatikai szervezetének munkatársai nem felelnek az eszköz nem megfelelő működéséért, az esetleges adatvesztésért.
A nem nevesített felhasználói fiókok (administrator, root, technikai fiókok stb.) jelszavát zárt borítékban a Gazdasági Igazgatóságon levő páncélszekrényben kell tárolni, felvételüket dokumentálni kell, és használat után új jelszót kell megadni.
A kiemelt jogok ellenőrzését évente kell elvégezni. Az ellenőrzés az Informatikai Biztonsági Felelős feladata.

10.2.4 A felhasználók titkos hitelesítési információinak kezelése

A hitelesítésre szolgáló jelszavak kiosztásakor a jelszót átvevő(k) jogosultságát az informatika munkatársának ellenőriznie kell.
A jelszó kezdeti értékét a felhasználónak az első bejelentkezéskor meg kell változtatnia. Amennyiben a rendszer ezt lehetővé teszi, a kezdeti jelszóváltoztatást ki kell kényszeríteni.

10.2.5 A felhasználói hozzáférési jogok átvizsgálása

A felhasználók hozzáférési jogosultságait évente felül kell vizsgálniuk az Informatikai Biztonsági Felelősnek és a Szervezeti Egységek Vezetőinek.
A kiemelt hozzáférési jogokat az Informatikai Biztonsági Felelős félévente felülvizsgálja.

10.2.6 A hozzáférési jogok visszavonása vagy módosítása

Az informatikai rendszerhez való hozzáférési jogokat, azonnal vissza kell vonni a felhasználó jogviszonyának megszüntetésekor, illetve annak változásakor módosítani kell a változásnak megfelelően. Amennyiben a rendszerben rögzítettől eltérő dátumú, vagy részleges jogosultság visszavonására van szükség, azt a megszűnő jogviszonyú felhasználó közvetlen felettese kell, hogy a jogosultsag@uni-bge.hu címre küldött e-mail-ben vagy elektronikus űrlap használatával jelezze.

10.3 Felhasználói felelősségek

Az Egyetem elvárja, hogy a felhasználók felelősen álljanak hozzá saját hitelesítési információik védelméhez.

10.3.1 Titkos hitelesítési információk használata

A felhasználóktól meg kell követelni, hogy a titkos hitelesítési információkat a szabályzatokban rögzített elvárásoknak megfelelően használják. Erre fel kell hívni a figyelmet az informatikai biztonsági oktatások során.
A felhasználói jelszavakat nem szabad más tudomására hozni. Lehetőleg meg kell jegyezni, vagy olyan módon rögzíteni, hogy az lehetőleg más számára ne legyen összekapcsolható a rendszerrel, amelyhez belépésre jogosít.

10.3.2 Rendszerhasználati szabályok elfogadtatása

A felhasználók jogviszonyuk létrejöttekor aláírásukkal, vagy elektronikus úton igazolják, hogy elfogadják a rendszerhasználat feltételeit, többek között azt, hogy az Egyetem a rendszerhasználatot az adatvédelmi szabályoknak megfelelően figyelheti, rögzítheti, naplózhatja, továbbá, hogy a rendszer jogosulatlan használata tilos, és büntetőjogi, illetve polgári jogi felelősségre vonással jár.

A rendszergazda felelőssége, felelősség kizárás
Az Egyetem informatikai szervezete és a rendszergazdák nem vállalnak felelősséget azért, hogy a rendszer a felhasználó speciális elvárásainak megfelelően hibátlanul, megszakításmentesen működjön.
Az Egyetem informatikai szervezete és a rendszergazdák nem felelnek a felhasználót ért azon károkért, amelyek a rendszer használatával kapcsolatban fellépnek, kivéve, ha azt a rendszergazdák, vagy az általuk a rendszer kezelésével megbízott személy szándékos magatartása idézte elő.

10.4 Operációs rendszerek és alkalmazások jogosultságkezelése

Az Egyetem célja, hogy megelőzze a jogosulatlan hozzáférést az informatikai rendszerekhez, alkalmazásokhoz, valamint a rendszerekben tárolt adatokhoz.

10.4.1 Információhoz való hozzáférés korlátozása

A jogosultságkezelési szabályoknak megfelelően kell korlátozni az információhoz és az alkalmazási rendszerek egyes funkcióihoz való hozzáférést.
Az informatikai rendszerek kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kell kezelni és megőrizni. Érvényesíteni kell a

jóváhagyott jogosultságokat az információhoz és a rendszer erőforrásaihoz való logikai hozzáférésnél.
Egyedileg azonosítani és hitelesíteni kell a felhasználókat, és a felhasználók által végzett tevékenységet.

10.4.2 Biztonságos bejelentkezési eljárások

Ahol a jogosultságkezelési szabályok előírják és a technológia lehetővé teszi, ott a rendszerekhez és alkalmazásokhoz való hozzáférést biztonságos bejelentkezési eljárással kell megvalósítani. Ennek megfelelően a bejelentkezés során a rendszer nem szolgáltathat olyan információkat, amelyek a jogosulatlan bejelentkezést elősegítik, vagy támpontot adnak, hogy mely bejelentkezési adatok nem megfelelőek. A hitelesítési folyamat során a jelszót el kell rejteni a képernyőn, például „*" karakter használatával.

10.4.3 Jelszókezelő rendszer

Az informatikai rendszereknél titkosítva kell tárolni a jelszavakat, kulcsokat és hozzáférési kódokat.
A rendszerek felhasználói által alkalmazott jelszavakkal szembeni minimális követelmények:

a) a legutóbbi három jelszóval nem egyezhet meg az új jelszó,
b) jelszóélettartam minimum 1, maximum 180 nap
c) Minimum jelszó követelmény: hossza 8 karakter, komplexitása legyen a felsorolt 4 követelményből 3: kisbetűk, nagybetűk, számok és különleges karakterek.

Egyes rendszerek, illetve kiemelt felhasználók esetén az Informatikai Biztonsági Felelős ettől eltérő követelményeket is meghatározhat.
A szervereken az adminisztrátori fiókok használatánál azonosításra lehetőség szerint hardver tokent kell használni.
A felhasználóknak adott kezdeti jelszavak (új jelszó) cseréjét – amennyiben a rendszer támogatja – ki kell kényszeríteni.
Elfelejtett jelszó esetén új jelszót csak a felhasználó megfelelő beazonosítását követően (pl. személyesen, visszahívással vagy a felhasználó mobiljára küldött SMS-sel) szabad átadni.
A jelszavak esetleges kompromittálódását az Informatikai Biztonsági Felelős felé jelezni kell, és a jelszavakat haladéktalanul cserélni kell.

10.4.4 Kiemelt jogokkal rendelkező segédprogramok használata

A rendszer- és alkalmazásszintű kontrollokat megkerülni képes, kiemelt jogokkal rendelkező segédprogramokat kizárólag Rendszergazdák használhatják az Informatikai Főosztályvezető által engedélyezett módon, melyet az Informatikai Biztonsági Felelős is jóváhagyott.
A rendszer- és alkalmazásszintű kontrollokat megkerülni képes, kiemelt jogokkal rendelkező (pl. rendszergazdai joggal futó) segédprogramok használatát naplózni kell.

Az Egyetem által használt alkalmazások forráskódja bizalmas minősítésű. A forráskódhoz az Informatikai Főosztályvezető, illetve az általa meghatalmazott személy férhet hozzá.

10.5 KÜLSŐ SZOLGÁLTATÓ ÁLTAL BIZTOSÍTOTT ALKALMAZÁSOK

10.5.1 Egyetem által előfizetett felhő alapú szolgáltatások

Az Egyetem a kommunikáció, valamint az irodai munka elősegítésére felhő alapú szolgáltatással rendelkezik. Az előfizetés lehetővé teszi többek között e-mail postafiók, tárhely, kommunikációs eszköz, valamint irodai programcsomag használatát.
Az Egyetem minden munkatársa számára egyéni, névre szóló postafiókot biztosít, az Egyetemre utaló címmel (vezeteknev.keresztnev@uni-bge.hu). Ezen postafiók esetén:

- Hivatalos kommunikációra ezt az e-mail fiókot kell használni.
- Tilos a levelek automatikus továbbítása külső e-mail címekre.
- Az Egyetem az e-mail lehetőséget alapvetően a munkavégzéshez biztosítja, de ésszerű keretek között a magáncélú használat is megengedett.

Az Egyetem a hallgatók számára felhő alapú szolgáltatás keretében e-mail postafiók, tárhely és irodai programcsomag lehetőséget biztosít. A szolgáltatás igénybevételének részletes szabályait az Egyetem honlapján elérhető tájékoztató tartalmazza.

Az Egyetem által biztosított e-mail címről Tilos jogszabályba, vagy jó erkölcsbe ütköző, illetve politikai, vagy izgató tartalmú leveleket küldeni. Az Egyetem fenntartja a jogot ahhoz, hogy a levelezésen technológiai szűrést alkalmazzon a nem kívánt tartalmú levelek kiszűrésére.

10.5.2 Egyéb felhő szolgáltatások

Az Egyetem informatikai rendszerén keresztül egyéb felhőszolgáltatások igénybevételére is van lehetőség. Az egyetemi tevékenységhez kapcsolódó anyagokat az Egyetem által biztosított infrastruktúrán kell tárolni, kezelni, kivéve, ha azt az Egyetem által biztosított szolgáltatások nem támogatják.

11. TITKOSÍTÁS (KRIPTOGRÁFIA)

Az Egyetem célja, hogy amennyiben szükséges, alkalmas és hatásos titkosítással védje az információk bizalmasságát, hitelességét, illetve sértetlenségét.
Amennyiben szükséges, biztonságosnak tekinthető kriptográfiai eljárásokat és műveleteket kell alkalmazni.
Az alkalmazandó eljárásokat az adott helyzet és a védendő információk kritikusságának mérlegelését követően az Informatikai Biztonsági Felelős határozza meg az Informatikai Főosztályvezetővel történt egyeztetés alapján.
A titkosító kulcsok használatára, védelmére és élettartamára vonatkozó szabályokat szükség esetén az Informatikai Biztonsági Felelős határozza meg.

12. FIZIKAI ÉS KÖRNYEZETI BIZTONSÁG

Az Egyetem célja olyan biztonsági követelmények előírása, amelyek az informatikai rendszerekhez történő jogosulatlan fizikai hozzáférés, rongálás, vagy működésük megzavarásának elkerüléséhez szükségesek.

A fizikai biztonsági kontrollok az informatikai biztonsági védelmi rendszer alapját alkotják, mivel ezek hiánya gyengíti a logikai és adminisztratív biztonsági intézkedéseket.

12.1 Létesítmények védelme

12.1.1 Fizikai biztonsági zónák

Meg kell határozni az Egyetem létesítményeinek fizikai határait, és azon belül ki kell jelölni azokat a területeket, ahol védendő információ, illetve információ-feldolgozó eszköz tárolható. Az Informatikai Főosztályvezető felelős azért, hogy a biztonsági besorolás által meghatározott fizikai biztonsági követelmények teljesüljenek. A besorolás elvégzése és a megfelelőség ellenőrzése az Informatikai Biztonsági Felelős feladata.
Az informatikai biztonság szempontjából az Egyetem az alábbi táblázatban szereplő fizikai védelmi besorolású zónákat határozza meg:

Biztonsági besorolás	Meghatározás
Kiemelt zóna	Olyan zóna, amely üzleti vagy annál magasabb biztonsági osztályba sorolt információt tároló, feldolgozó, vagy továbbító infokommunikációs eszközöket tárol. Az Egyetem informatikai igényeit biztosító központ infrastruktúra elhelyezésére szolgáló terület.
Irodai zóna	Az Egyetem irodái, ahol üzleti vagy annál magasabb biztonsági osztályba sorolt információ kezelése, feldolgozása történik.
Nyilvános zóna	Minden, az előző kategóriákba nem sorolható zóna, bárki által szabadon látogatható vagy igénybe vehető terület.

Az egyes zónákban csak olyan adat és információ tárolható, melynek védelmi igénye nem haladja meg az adott zóna biztonsági besorolását.
A kiemelt zónának jól definiált határral kell rendelkeznie, illetve a nyilvánosságtól elzártnak kell lennie.
Az épület átalakítások, karbantartások során, az informatikai eszközök elhelyezésének megváltoztatása esetén a fizikai védelmi szempontokat az Informatikai Biztonsági Felelősnek felül kell vizsgálnia.

12.1.2 Fizikai beléptetési intézkedések

A Kiemelt zónába való belépést az Informatikai Osztályvezetők engedélyezik az arra jogosult személyeknek.
A Kiemelt zónák zárva tartandók, belépni csak belépőkártyával, kulccsal vagy egyedi kód megadásával lehetséges.
A belépésre jogosult személyekről, és a belépőkártyákról illetve kódokról naprakész nyilvántartást kell vezetni, és a nyilvántartás adatait legalább 1 évig meg kell őrizni.
A Kiemelt biztonsági besorolású helyiségeket olyan beléptető rendszerrel kell felszerelni, amely képes kikényszeríteni a belépésre jogosultak egyedi azonosítását vagy ennek hiányában belépési naplót kell vezetni.
A kiemelt biztonsági zónához a fizikai hozzáférési jogokat évente legalább egyszer az Informatikai Biztonsági Felelősnek felül kell vizsgálnia.
Amennyiben lehetséges a kiemelt zóná(k)ban a belépésekről kamera felvételt kell készíteni, melyet a jogszabályok szerint megengedett ideig kell megőrizni, az esetlegesen bekövetkező események

kivizsgálásának támogatására. A kamera felvétel készítéséről a belépőket jól látható módon tájékoztatni kell. A felvételek felhasználását dokumentálni kell.

12.1.3 Irodák, helyiségek és létesítmények védelme

Az Egyetem irodáinak, egyéb helyiségeinek és létesítményeinek a fizikai védelmi intézkedéseit az Informatikai Biztonsági Szabályzatban meghatározott követelményeket figyelembe véve kell megtervezni, azokat alkalmazni kell.
A kiemelt biztonsági besorolású helyiségeknek feltűnésmentesnek kell lennie, az épületeken kívül, vagy belül semmi sem jelezheti azok jelenlétét.
Tilos a kiemelt biztonsági besorolású géptermekből előzetes engedély nélkül informatikai eszközöket kivinni! Valamennyi kivinni szándékozott informatikai eszközre vonatkozóan a kivitel tényét követni kell.
A kulccsal nyitható helyiségek kulcsai csak az arra jogosult személyeknek adhatóak ki.
Az irodákat, ha abban munkatárs nem tartózkodik, zárva kell tartani.

12.1.4 Külső és környezeti fenyegetésekkel szembeni védelem

A természeti katasztrófák, a rosszindulatú támadás vagy a balesetek kockázatait fel kell mérni, a magas kockázatok csökkentésére védelmi intézkedéseket kell meghatározni, és azokat alkalmazni kell.
A kiemelt biztonsági besorolású helyiségek ajtóit semmilyen körülmények között sem szabad kitámasztani, vagy nyitva hagyni!
A kiemelt biztonsági besorolású helyiségben tilos veszélyes vagy éghető anyagokat tárolni!
A központ infrastruktúra elhelyezésére szolgáló helyiséget úgy kell kialakítani, hogy a csővezetékek (pl. víz, csatorna, kondenzvíz, tűzi víz) rongálódásából származó károkkal szemben védve legyenek.

12.2 Berendezések biztonsága

Az Egyetem célja, hogy megelőzze a vagyonelemei elvesztését, károsodását, valamint az informatikai rendszerek segítségével nyújtott szolgáltatások folytonosságának megszakadását. Ezen célok megvalósítását az e fejezetben felsoroltak támogatják:

12.2.1 Munkavégzés biztonsági területeken

A kiemelt biztonsági zónákban csak az arra jogosult személyek tartózkodhatnak. Az eseti belépési engedéllyel rendelkező személyek (külső támogatók stb.) csak egy arra jogosult személy kíséretében közlekedhetnek.
A külső fél által végzett tevékenységet felügyelnie kell a helyi Informatikai Osztályvezető által kijelölt munkatársának.

12.2.2 Berendezések elhelyezése és védelme

Kockázatokkal arányos biztonsági kontrollokat kell kidolgozni az IT infrastruktúra elemeinek (pl. szerverek, központi switch-ek) a potenciális környezeti fenyegetésekből (pl. lopás, tűz, robbanás, füst, víz, por, vibráció, elektromágneses sugárzás, kémiai behatások, elektromos tápellátás zavarai) eredő kockázatainak csökkentésére. Az alap infrastruktúra részét képező eszközöket zárható szekrénybe kell elhelyezni, (pl. tantermi switch) vagy külön eszköz nélkül nem elérhető magasságba (pl. Wireless router, access point). Az eszközök elhelyezéséről és védelméről a helyi Informatikai Osztályvezető gondoskodik. Az épület átalakítások, karbantartások során, az informatikai eszközök

elhelyezésének megváltoztatása esetén a fizikai védelmi szempontokat az Informatikai Biztonsági Felelősnek felül kell vizsgálnia.

12.2.3 Közműszolgáltatások

Biztosítani kell az IT infrastruktúra kritikus elemeinek (pl. szerverek, központi switch-ek) védelmét áramszünet, illetve egyéb elektromos üzemzavarok ellen. A berendezés gyártói specifikációinak megfelelő tápellátást kell biztosítani.
A tápellátás folytonosságát folyamatos üzemű, a tevékenységhez méretezett szünetmentes tápegységek („UPS") alkalmazásával kell biztosítani.

12.2.4 Adatkábelek védelme

Biztosítani kell a gerinchálózati kábelek jogosulatlan lehallgatás és/vagy rongálás elleni védelmét, kábelcsatorna használatával, illetve a kábelútvonalak kialakításakor a kábelek falban, álmennyezet fölött, illetve a nyilvános területek elkerülésével történő elvezetésével.

12.2.5 Berendezések karbantartása

Az Egyetem informatikai eszközeit a gyártó előírásai szerint kell karbantartani folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében.

12.2.6 Vagyonelemek eltávolítása

Az Egyetem telephelyeiről az Informatikai Osztályvezetők előzetes engedélye nélkül nem szabad berendezéseket, vagy szoftvereket kivinni.
A ki és beszállításról szállító leveleket kell készíteni, és a Vagyonnyilvántartásban nyilván kell tartani az eszköz helyét.

12.2.7 Berendezések és vagyonelemek biztonsága a telephelyen kívül

A telephelye(ke)n kívüli használt berendezéseket védeni kell a külső fenyegetésektől. Az eszközök fizikai védelméről a berendezésekért felelős, azokat használó személyeknek kell gondoskodniuk.

12.2.8 Berendezések selejtezése vagy újrafelhasználása

Az adatosztályozás alapján magas biztonsági szintbe sorolt adatokat (pl. üzleti titok, különleges személyes adat) tároló informatikai berendezéseket fizikailag meg kell semmisíteni, vagy az adatokat a hagyományos törlés funkció helyett helyreállíthatatlanságot biztosító törlési technikákkal kell törölni leselejtezés, vagy újrafelhasználásra való átadás előtt. A törlési mechanizmusnak az információ minősítési kategóriájával arányos erősségűnek kell lennie.
Amennyiben használt informatikai eszközt harmadik fél számára kell átadni (pl. laptopok javítása), az érintett Informatikai Osztályvezető hoz döntést az eszköz adathordozóján levő adatok minősítése alapján hogy az eszköz javításra kiadható-e, illetve az adathordozóról az összes adatot, helyreállíthatatlanul törölni kell-e.

12.2.9 Őrizetlenül hagyott felhasználói berendezések

A személyes használatra átadott eszközök megfelelő védelmét biztosítani kell minden felhasználónak.
Az eszközök az Egyetem területén kívül csak zárt helyiségben hagyhatóak felügyelet nélkül. Ha közös használatú helyiségben szükséges felügyelet nélkül hagyni, akkor az eszközt lehetőleg el kell zárni.

Az Egyetem informatikai eszközeit (munkaállomások, szerverek) jelszavas képernyővédővel kell ellátni. A védelemnek 15 perc felhasználói inaktivitás után automatikusan be kell kapcsolnia. A képernyővédők beállításait az informatikai üzemeltetés végzi.

12.2.10 Üres asztal és tiszta képernyő irányelve

Az Egyetem által kezelt dokumentumokra és a cserélhető adattároló eszközökre alkalmazni kell a tiszta asztal szabályt, azaz az íróasztalokról el kell zárni a védendő információkat tartalmazó dokumentumokat és adattároló eszközöket hosszabb munkaszünet idejére, illetve a munkanap végén.
Az Egyetem szerverein, munkaállomásain a tiszta képernyő szabályt kell alkalmazni, azaz az eszközök képernyőjén védendő dokumentumokat úgy szabad olvasni, illetve szerkeszteni, hogy azokat illetéktelen személyek ne olvashassák el.

13. ÜZEMELTETÉS BIZTONSÁGA

13.1 Üzemeltetési eljárások és felelősségi körök

Az Egyetem célja, hogy az információ feldolgozó eszközök helyes és biztonságos üzemelését biztosítsa.

13.1.1 Dokumentált üzemeltetési eljárások

Az üzemeltetési eljárásokat dokumentálni kell, és hozzáférhetővé kell tenni minden olyan munkatárs számára, akinek ez a munkavégzéséhez szükséges.
Az üzemeltetési feladatok meghatározása és szabályozása az Informatikai Főosztályvezető, és az Informatikai Osztályvezetők feladata.
Az informatikai eszközökön futó programokat, nem beleértve a rendszerek részét képező segédprogramokat nyilván kell tartani. Az Egyetem informatikai eszközein az Informatikai Főosztályvezető vagy valamelyik Informatikai Osztályvezető által jóváhagyott programok használhatóak.

13.1.2 Változásfelügyelet

Dokumentált és engedélyezett módon kell kezelni minden az informatikai rendszert érintő szoftvert, illetve hardvert érintő lényeges változtatást.

13.1.3 Kapacitáskezelés

A szükséges rendszerteljesítmény biztosítása érdekében az erőforrások használatát nyomon kell követni, optimalizálni kell és a jövőbeni kapacitásszükségletet előre kell jelezni. Évente fel kell mérni a meglévő kapacitásokat és a várható kapacitás igényeket, illetve év közben nyomon kell követni az informatikai rendszerek kihasználtságát, és a beszerzési időt figyelembe véve jelezni kell az Informatikai Főosztályvezetőnek, ha kapacitásbővítésre van szükség.
Ezen feladatok elvégzéséért az érintett Informatikai Osztályvezető felel.
Új informatikai rendszer tervezése esetén az érintett Informatikai Osztályvezető feladata a szükséges kapacitás igény meghatározása.

13.1.4 A fejlesztési, a tesztelési és az üzemi környezetek elkülönítése

Ahol van rá mód, el kell különíteni a fejlesztési, tesztelési és éles üzemi környezeteket, hogy csökkenteni lehessen a jogosulatlan hozzáférés vagy a változtatás kockázatát az éles üzemi környezetben.

13.2 Védelem a rosszindulatú szoftverek ellen

Az Egyetem célja, hogy az általa kezelt információ és az általa használt információ feldolgozó eszközök védettek legyenek a rosszindulatú szoftverek ellen.

13.2.1 Intézkedések a kártékony szoftverek ellen

Az Egyetem olyan központilag menedzselt vírusvédelmi szoftvert működtet minden, az Egyetem tulajdonát képező munkaállomáson és szerveren, amely legalább naponta központilag automatikusan frissíti az adatbázisát.
Minden felhasználó felelős azért, hogy csak megbízható forrásból származó elektronikus állományokat futtasson, és megbízható honlapokat látogasson.
A felhasználók a vírusvédelmi szoftvert nem kapcsolhatják ki. Vírusriasztás esetén nem szabad a számítógépen a munkát folytatni, a riasztást jelenteni kell az informatikai szervezet munkatársainak.
A felhasználó köteles az informatikai szervezet munkatársa által közölt tevékenységek végrehajtására, melyek többek között az alábbiak lehetnek:

a) a munkaállomás hálózatról történő leválasztása,
b) a munkaállomás kikapcsolása,
c) a riasztás részletes adatainak ismertetése,

A kártékony szoftverek elleni védekezés érdekében a technikai intézkedéseket ki kell egészíteni megfelelő felhasználói tudatossági képzéssel.
A mobil adathordozókat a használat előtt ellenőrizni kell, hogy van-e rajta kártékony kód.
A munkaállomások kártékony kód mentességének biztosítása érdekében az Informatikai Főosztály munkatársainak hetente, automatikus fájlrendszer-ellenőrzést kell beállítani. Az ellenőrzés időpontját úgy kell meghatározni, hogy az a felhasználók munkavégzését ne akadályozza.

13.3 Mentés

Az Egyetem célja, hogy megelőzze az általa kezelt adatok sérülését, vagy megsemmisülését.

13.3.1 Információk mentése, mentések tárolása

Az adatokról, szoftverekről és rendszerképekről a Mentési utasításnak megfelelően kell mentéseket készíteni.
A mentésekre, archiválásokra, a mentett állományok tesztelésére, visszaállítására vonatkozó részletes szabályokat a Mentési utasítás tartalmazza.
A munkaállomásokon illetve a személyi használatra kiadott eszközökön tárolt adatok mentésre nem kerülnek automatikusan, a felhasználó felelőssége, hogy az ilyen eszközökön, munkaállomásokon az Egyetemi tevékenységgel kapcsolatos adatokról mentés készüljön. Ezen adatok tárolására az Egyetem által biztosított felhő alapú tárhelyszolgáltatást használja.
Személyes jellegű adatok tárolása a munkaállomásokon illetve a személyi használatra kiadott eszközökön ésszerű mértékig megengedett, de az ilyen jellegű adatok sérüléséért, helyreállíthatatlanságáért az informatikai szervezet felelősséget nem vállal. Ezen adatok mentéséről a felhasználónak kell gondoskodnia.

13.4 Naplózás és megfigyelés

Az Egyetem célja, hogy megfelelő naplóállományokkal rendelkezzen az informatikai rendszerekben keletkező kritikus események kivizsgálásához, elemzéséhez.

13.4.1 Eseménynaplózás

A felhasználói tevékenységekre, a rendellenes működésre, a hibákra és az informatikai biztonsági eseményekre vonatkozó eseményeket naplózni kell, azokat meg kell őrizni. A naplózást az Informatikai Biztonsági Felelőssel történt egyeztetés alapján az Informatikai Főosztályvezető által megbízott munkatárs állítja be.
A naplózandó események körét az Informatikai Biztonsági Felelős határozza meg. Minimálisan az alábbi eseményeket kell naplózniuk a rendszereknek, ha a rendszer ezt lehetővé teszi:

a) A sikeres és sikertelen belépési kísérleteket
b) A felhasználók adatkezelési tevékenységét,
c) Felhasználók kezelését (új felhasználó felvétele, meglévő felfüggesztése, aktiválása),
d) Jogosultságok kezelését (jogosultságok megadása, módosítása, visszavonása),
e) A szoftverek konfigurációjában végzett változásokat,
f) A tűzfalon zajló változásokat,

A naplóadatoknak tartalmazni kell legalább, ha azok elérhetőek:

a) A felhasználó, eszköz egyértelmű azonosításához szükséges azonosító adatokat,
b) az esemény idejét,
c) az esemény releváns adatait

13.4.2 Naplóinformációk védelme

A napló adatokat védeni kell a módosítástól és a jogosulatlan törléstől a rendszer megfelelő biztonsági beállításaival. A rendszergazdai jogosultsággal történő tevékenységeket naplózni kell. A biztonsági naplókat és rendszerhasználati naplókat az Egyetem minimum 3 hónapig őrzi.

13.4.3 Monitorozás

Az Egyetem az informatikai rendszer biztonságos üzemeltetése érdekében megfigyeli a rendszer főbb paramétereit. A monitorozó rendszert úgy kell beállítani, hogy a főbb paraméterek előre meghatározott kritikus szint elérésekor az üzemeltető munkatársak riasztást kapjanak.
A paraméterek meghatározása az Informatikai Osztályvezetők feladata.

13.4.4 Óraszinkronizálás

Az Egyetem a rendszerek rendszeridejét automatikusan szinkronizálja egy központi órajel forrással. Az ilyen módon szinkronizált belső rendszerórákat kell használni a naplóbejegyzések időbélyegeinek előállításához, az egységes referencia idő miatt.

13.5 Az üzemelő szoftverek felügyelete

Az Egyetem célja, hogy az üzemelő rendszerek sértetlenségét biztosítsa.

13.5.1 Szoftverek telepítése az üzemelő rendszerekre

Az Egyetem informatikai eszközeire szoftvert csak az informatikai üzemeltetéssel foglalkozó munkatársak, illetve az Informatikai Főosztályvezető által meghatalmazott személyek telepíthetnek. Tilos telepítést nem igénylő, nem engedélyezett szoftverek futtatása is a munkaállomásokon.
Az Egyetem informatikai eszközein futtatható, engedélyezett szoftverek listáját az Informatikai Biztonsági Felelős vezeti.
Az informatikai rendszer elemeit úgy kell konfigurálni, hogy azokon csak a szükséges szolgáltatások legyenek elérhetők.

13.6 A szoftveres sebezhetőségek felügyelete

Az Egyetem célja, hogy megelőzze a rendszerei szoftveres sebezhetőségének kihasználását.

A szoftverek sérülékenységeire vonatkozó információkat figyelni kell, melyért az üzemeltetési munkatársak felelősek. A sérülékenységek kijavítására vonatkozó megjelenő javításokat lehetőség szerint minél hamarabb telepíteni szükséges. A javítások telepítéséért az Informatikai Osztályvezetők felelnek a saját területükön. A személyi használatba adott eszközökre a frissítések telepítése az eszköz felhasználójának felelőssége.
Az éles üzemi rendszerek ellenőrzésére vonatkozó informatikai auditokat körültekintően meg kell tervezni úgy, hogy az audit tevékenység az Egyetem működésével kapcsolatos folyamatokat ne zavarja.

14. KOMMUNIKÁCIÓ BIZTONSÁGA

Az Egyetemrésze a magyar akadémiai hálózatnak (HBONE) és ezen keresztül teljes jogú tagja a világ Internet társadalmának. A HBONE kapcsolatot szolgáltató üzemelteti. Oktatási, kutatási céllal a karok üzemeltetik a hálózati kijáratokat a HBONE felé, a szolgátató megbízásából. A kari informatikai szervezetek feladata, hogy érvényesítsék azokat a szabályokat („HBONE dokumentumok", „a szolgáltató felhasználói szabályzata"), amelyek a HBONE-ra és az arra kapcsolódó intézményekre vonatkoznak.

14.1 Hálózatbiztonság

Az Egyetem célja, hogy biztosítsa az általa üzemeltetett, illetve felügyelt adathálózatokon keresztül továbbított információ védelmét.

14.1.1 Hálózati intézkedések

A hálózatokat menedzselése és felügyelete az Informatikai szervezet feladata.
Az Egyetem hálózatán levő informatikai eszközök azonosítása a hálózaton egyedi azonosító alapján történik, amennyiben technikailag ez lehetséges.
A hálózatra csatlakoztatott eszközökhöz menedzsment hozzáférés csak hitelesítést követően engedélyezett.

14.1.2 A hálózati szolgáltatások biztonsága

Az Egyetem belső hálózatához távolról kapcsolódni (VPN, távoli asztal, egyéb titkosított protokollon keresztül) csak az Informatikai Főosztályvezető engedélyével lehetséges.

Az Egyetem belső hálózatához kapcsolódó eszközökről külső hálózathoz csak az intézmény határvédelmi eszközein felügyelt interfészeken keresztül szabad kapcsolódni.
Az eszközökön a távdiagnosztikai és konfigurációs portokat korlátozni kell, ezen portok használatát, amennyiben lehetséges naplózni kell. A kollégiumokban, közösségi terekben lévő vezetékes és az Egyetem területén elérhető vezeték nélküli hálózatokat csak azonosítást követően lehet igénybe venni.

14.1.3 Elkülönítés a hálózatokban

Az Egyetem az alábbi hálózati elkülönítéseket alkalmazza:

Vezetékes hálózat
A karok hálózatai között nem teljes átjárás biztosított. Az átjárhatóság szabályrendszerét az Informatikai Főosztályvezető az Informatikai Biztonsági Felelőssel közösen határozza meg.

Vezeték nélküli (WiFi) hálózatok típusai:

Eduroam – nemzetközi, egyetemi azonosítóval rendelkezők által használható hálózat, mely Internet elérést biztosít.
Vendég hálózat – napi változású, jelszóval védett Internet elérést biztosító hálózat az Egyetem vendégei számára
Ad-hoc – projektekre vagy eseményekre, adott időszakra, üzembe helyezett hálózatok, ad-hoc jelszóval védve

14.2 Információátvitel

A titoktartási megállapodásokat írásban kell megkötni.
A titoktartási megállapodások szövegének tükröznie kell az informatikai biztonsági követelményeket, amennyiben a megállapodást aláíró fél az Egyetem informatikai rendszeréhez hozzáférést kap.
Az információátvitelt az Egyetem Adatkezelési szabályzatában foglaltakkal összhangban kell elvégezni.

14.2.1 Az információcserére vonatkozó szabályok

Az információt védeni kell az információcsere során minden típusú kommunikációs eszköz használata esetén.
Az információcserére vonatkozó megállapodásokban rendelkezni kell a biztonsági elvárásokról az adott információ osztálynak megfelelően:
A rendszereknek meg kell gátolniuk az együttműködésen alapuló számítástechnikai eszközök (pl. kamerák, mikrofonok) távoli aktiválását.
Külső felekkel rendszeres információcsere csak jogszabály, illetve előzetes megállapodás (pl. szerződés) alapján megengedett.
Az Egyetem által kezelt személyes adatokat és üzleti titkokat tartalmazó állományok intézményen kívülre elektronikus formában történő továbbítása csak a Kancellár engedélyével lehetséges, kivétel ez alól a jogszabály által kötelező és a fenntartó által kért adatszolgáltatás.

14.2.2 Elektronikus információ átvitel

Az elektronikus formában lévő információkat a besorolásuknak megfelelően kell védeni. Személyes adatot és üzleti titkot tartalmazó adatokat elektronikus formában az Egyetemen kívülre csak titkosítottan szabad továbbítani.

15. RENDSZEREK BESZERZÉSE, FEJLESZTÉSE ÉS KARBANTARTÁSA

Az informatikai rendszerek és szolgáltatások beszerzését a rendszerek teljes életciklusában informatikai biztonsági szempontból felügyelni kell.
A rendszer életciklus szakaszai a következők:

a) követelmény meghatározás;
b) fejlesztés vagy beszerzés;
c) megvalósítás vagy értékelés;
d) üzemeltetés és fenntartás;
e) kivonás (archiválás, megsemmisítés).

15.1 Az információs rendszerek biztonsági követelményei

Az Egyetem célja, hogy az információs rendszerei teljes életciklusának szerves része legyen az informatikai biztonság.

15.1.1 Informatikai biztonsági követelmények

Új informatikai rendszerek fejlesztésére, beszerzésére vagy létező rendszerek továbbfejlesztésére vonatkozó követelmények meghatározásakor az informatikai biztonsági követelményeket is meg kell határozni.
A nyilvános hálózatokon keresztül szolgáltatott alkalmazások által átvitt információt védeni kell a visszaéléstől, és a jogosulatlan közzétételtől vagy módosítástól különös tekintettel az adatbekéréssel járó szolgáltatások esetében.

15.2 Biztonság a fejlesztési és támogatási folyamatokban

Az Egyetem célja, hogy az informatikai biztonságot az informatikai rendszerek fejlesztési életciklusába is beillesszék.

15.2.1 Biztonságos szoftverfejlesztés szabályozása

Az Egyetem számára fejlesztett szoftverek és rendszerek fejlesztése során meg kell határozni az informatikai biztonsági követelményeket, melyekért az Informatikai Biztonsági Felelős és az Informatikai Főosztályvezető felelős.

15.2.2 Rendszerek változásfelügyeleti eljárásai

A fejlesztési életciklus során végrehajtandó rendszerváltoztatásokra változáskezelési eljárást kell alkalmazni, mely alapján az egyes verziók közti változtatások egyértelműen követhetők, az aktuálisan használt verzió egyértelműen meghatározható.

Ha az Egyetem informatikai rendszerében, vagy működési környezetében változtatást végeznek, akkor a magas kockázatú változtatásokat elkülönített tesztkörnyezetben vizsgálni kell. Az

alkalmazásokat meg kell vizsgálni és tesztelni kell, hogy megbizonyosodjunk arról, hogy a változtatásnak nincsen kedvezőtlen hatása az informatikai rendszer működésére és biztonságára.

A szükséges változtatásokat a változáskezelési folyamat szerint kell végrehajtani.

Az Egyetem elvárja a részére fejlesztést végző külső partnerektől, hogy biztonságos fejlesztési környezetet működtessenek. A fejlesztési környezet biztonságáról, illetve ennek biztosításáról a külső partner az Egyetemmel létrejövő szerződéssel egy időben kell nyilatkozni.

A szoftverfejlesztés során el kell végezni az üzleti és a biztonsági funkciók tesztelését. A fejlesztés befejezését követően a fejlesztő cégnek nyilatkoznia kell az informatikai biztonsági előírásoknak történő megfelelőségről. A tesztelés megtörténtét és eredményeit az Informatikai Biztonsági Felelős ellenőrzi.

A rendszerek átvételi kritériumait a követelmények meghatározásakor kell rögzíteni. A kritériumok meghatározása az Informatikai Főosztályvezető és az Informatikai Biztonsági Felelős közös feladata.

15.3 Tesztadatok

Az Egyetem célja a tesztelésre használt adatok védelmének biztosítása.

15.3.1 Tesztadatok védelme

A tesztadatokat gondosan kell kiválasztani, védeni kell, és a használatukat felügyelni kell. A teszt rendszerben lévő adatokat az éles üzemben levő adatokkal azonos szinten kell védeni és kezelni.

16. BESZÁLLÍTÓI KAPCSOLATOK

Az Egyetem a rendszerek fejlesztésében és üzemeltetésében közreműködő személyekkel, illetve szervezetekkel kivétel nélkül szerződéses viszonyban áll.
A szerződésekben az informatikai biztonsági kötelezettségeket rögzíteni kell, beleértve a titoktartási nyilatkozatot.

16.1 Informatikai biztonság a szállítói kapcsolatokban

Az Egyetem célja, hogy a szállítók számára hozzáférhető információkat és vagyonelemeket védje.

16.1.1 Informatikai biztonság szabályozása a szállítói kapcsolatokban

A szállítóknak az Egyetem vagyonelemeihez való hozzáférésének módját, valamint az informatikai biztonsági követelményeket a szállítókkal kötött szerződésekben kell rögzíteni.

16.1.2 A biztonsági elvárások szerepeltetése a szállítói megállapodásokban

Minden olyan, a szállítókkal kötött szerződésnek ki kell térnie minden lényeges informatikai biztonsági követelményre, amely esetekben a szállítók hozzáférést kapnak a szervezet informatikai rendszeréhez.
A szerződésben rögzíteni kell:

a) az Informatikai Biztonsági Szabályzatra való hivatkozást;
b) az Egyetem vagyonának védelmét,
c) valamennyi rendelkezésre bocsátandó szolgáltatás leírását és annak minimálisan elfogadható szintjét;
d) azokat az óvintézkedéseket, amelyek biztosítják a rosszindulatú szoftverek elleni védekezést;
e) a külső partner nyilatkozata arról, hogy biztonságos fejlesztési környezetet működtet.

16.2 A szállítói szolgáltatásnyújtás irányítása

Az Egyetem célja, hogy szolgáltatási megállapodásokban rögzített biztonsági és szolgáltatási szinteket a szállítók biztosítsák.

16.2.1 A szállítói szolgáltatások figyelemmel kísérése és átvizsgálása

Az Egyetem a szerződéses feladatok teljesítésekor, de legalább évente értékeli a szolgáltatás minőségét és a szerződéses követelményeknek való megfelelőségét. Az értékelés az adott szolgáltatásra vonatkozó szerződésben megjelölt egyetemi kapcsolattartó feladata.
A harmadik felektől igénybe vett szolgáltatásokkal kapcsolatos változtatásokat az adott szolgáltatásra vonatkozó szerződésben megjelölt egyetemi kapcsolattartó kezeli.

17. INFORMATIKAI BIZTONSÁGI INCIDENSEK KEZELÉSE

17.1 Az informatikai biztonsági incidensek és javítások kezelése

Az informatikai biztonsági incidensek formalizált kezelése fontos részét képezi az informatikai biztonsági irányítási rendszernek, hiszen az informatikai biztonsági incidensek sok esetben az irányítási rendszer valamelyik részének javítandó hiányosságára vezethetőek vissza.

17.1.1 Felelősségek és eljárások

Ki kell dolgozni az informatikai biztonsági incidensek kezelésének formalizált és dokumentált folyamatait. Az informatikai biztonsági események megfelelő kezeléséért az Informatikai Biztonsági Felelős felel. Amennyiben szükséges az esemény kezelésébe bevonhatja az Informatikai Főosztályvezetőt is.

17.1.2 Informatikai biztonsági incidensek jelentése

Valamennyi közalkalmazott, illetve egyéb jogviszony alapján munkát végző személy, valamint hallgató haladéktalanul köteles az általa észlelt informatikai biztonsági incidens bekövetkeztét, vagy ha erre utaló jelet, vagy veszélyhelyzetet észlel bejelenteni az informatikai szervezetnek.

17.1.3 Informatikai biztonsági hiányosságok jelentése

Valamennyi közalkalmazott, illetve egyéb jogviszony alapján munkát végző személy, valamint hallgató haladéktalanul köteles jelenteni az Egyetem informatikai szervezetének, ha az informatikai rendszerekkel kapcsolatos bármilyen biztonsági hiányosságot, vagy problémát észlelt, vagy feltételezett, valamint ha olyan adatokhoz van hozzáférése, amelyhez a munkája, tevékenysége révén nem lenne jogosult. Az ilyen módon megszerzett információ bármilyen jellegű felhasználása tilos.

17.1.4 Az informatikai biztonsági események felmérése és döntéshozatal

Az érintett Informatikai Osztályvezető dönt arról, hogy a bejelentett informatikai biztonsági esemény incidensnek minősül-e. Amennyiben incidens történt, tájékoztatja az Informatikai Biztonsági Felelőst és az Informatikai Főosztályvezetőt.
Az incidensek vizsgálata során a rendelkezésre álló adatok, információk alapján kell a további lépésekről a döntést meghozni.

17.1.5 Válasz az informatikai biztonsági incidensekre

Az incidensekre adandó válaszlépéseket az érintett Informatikai Osztályvezető döntése alapján az Informatika kijelölt munkatársa teszi meg. Az incidensre reagálás magában foglalja az előkészületet, az észlelést, a vizsgálatot, a megszüntetést és a helyreállítást.

17.1.6 Tanulás az informatikai biztonsági incidensekből

Az informatikai biztonsági incidensek megoldását ki kell értékelni az Informatikai Biztonsági Felelősnek és az Informatikai Főosztályvezetőnek. A kiértékelés alapján, amennyiben szükségesnek látják, javaslatot kell tenniük a jövőbeni incidensek bekövetkezési valószínűségének és káros hatásának csökkentése érdekében.

17.1.7 Bizonyítékok összegyűjtése

Informatikai biztonsági incidens kezelése során törekedni kell arra, hogy bizonyítékokat gyűjtsünk annak érdekében, hogy amennyiben jogi útra kell terelni az incidens kezelését, az összes lehetséges bizonyíték rendelkezésre álljon.

18. A MŰKÖDÉSFOLYTONOSSÁG BIZTOSÍTÁSÁNAK INFORMATIKAI BIZTONSÁGI VONATKOZÁSAI

Az Egyetem célja, hogy a működése folytonosságát biztosító szabályzataiba, folyamataiba beépítse az informatikai biztonsági tevékenység folytonosságát biztosító folyamatokat.

Az Egyetem előre nem látható kedvezőtlen helyzetekben is a normál helyzetekben elvárt, jogszabályokból fakadó informatikai biztonsági követelményeket kell, hogy teljesítse.

Az Informatikai Főosztályvezető felelős azért, hogy egy rendszerösszeomlás, kompromittálódás vagy hiba esetén az informatikai rendszerek az utolsó ismert állapotba kerüljenek helyreállításra, és azokat újraindítsák, valamint az utolsó mentésből az adatok is helyreállításra kerüljenek.

18.1 Tartalékok

Az Egyetem célja, hogy az információ feldolgozó eszközök rendelkezésre álljanak az elvárt követelményeknek megfelelően.

18.1.1 Információ feldolgozó eszközök rendelkezésre állása

Az Egyetem működésének biztosításához, az elvárt követelményeknek elegendő informatikai erőforrással kell rendelkezni. Ezek meghatározását az Informatikai Főosztályvezető és az Informatikai Biztonsági Felelős végzi, a Kancellár jóváhagyásával.

19. MEGFELELŐSÉG

19.1 Megfelelés a jogi és szerződéses követelményeknek

Az Egyetem célja elkerülni az informatikai biztonsággal kapcsolatos jogszabályi, szabályozói vagy szerződéses kötelezettségek, illetve bármilyen más informatikai biztonsági követelmény megsértését.

19.1.1 A vonatkozó jogszabályi és szerződéses követelmények azonosítása

Az Egyetemre vonatkozó minden jogszabályi, hatósági előírást és szerződéses kötelezettséget azonosítani kell. A követelmények betartásáért – különös tekintettel az Egyetem Szerződéskötési rendjéről szóló szabályzatára – a szervezeti egységek vezetői felelősek. A szerződések eredeti példányait a Gazdasági Igazgatóság tárolja.

19.1.2 Szellemi tulajdonjogok

Az Informatikai Főosztályvezető feladata arról gondoskodni, hogy az informatikai eszközökön olyan szoftverek legyenek, amelyek használatára a szervezet jogosult.

Az informatikai rendszerbe telepített valamennyi szoftver jogtisztaságát bizonyító szerződéseknek rendelkezésre kell állniuk, és azokat nyilván kell tartani. Ezért az informatikai szervezet osztályvezetői felelnek.
Minden külső céggel kötött szerződés keretében kidolgozott Alkalmazás (szoftver) esetében a szerzői jogokra vonatkozó előírásokat a szerződésbe bele kell foglalni.
Évente felül kell vizsgálni az Egyetem informatikai rendszerében kezelt állományokat, és ki kell szűrni a nem jogszerűen ott tárolt jogvédett tartalmakat. A feladat felelőse az Informatikai Biztonsági Felelős.
Évente meg kell vizsgálni az Egyetem informatikai rendszerében telepített szoftvereket, hogy a felhasználói licenc feltételekkel összhangban kerültek-e telepítésre. A feladat felelőse az Informatikai Biztonsági Felelős.
Az Egyetem számítógépein szerzői jogvédett tartalmakat csak a jogszabály adta lehetőségek mértékéig szabad tárolni, kezelni.
Az Egyetem informatikai szervezete által biztosított szoftvereken felül, a felhasználó külön kérésére, munkavégzés céljából telepített szoftverek jogtisztaságáért az adott felhasználó felelős. Ezekről a szoftverekről nyílvántartást kell vezetni, ezért az Informatikai szervezet osztályvezetői felelnek.

19.1.3 Az informatikai dokumentumok védelme

Az Egyetem informatikai rendszerével kapcsolatos dokumentumokat védeni kell az elveszéstől, a megsemmisüléstől, a hamisítástól, a jogosulatlan hozzáféréstől. Az információk megőrzésének időtartamát és adattartalmát a törvények, és egyéb jogszabályok alapján kell meghatározni. Az informatikai rendszerre vonatkozó dokumentumokat a kötelező megőrzési időszak lejártával, ha a szervezet számára már nem szükségesek, helyreállíthatatlan módon kell megsemmisíteni.
A védelem megvalósítása az Informatikai Biztonsági Felelős és az Informatikai Főosztályvezető feladata.

19.1.4 A személyes adatok védelme

A személyes adatokat a vonatkozó jogszabályok és az Egyetem Adatvédelmi szabályzata szerinti védelemben kell részesíteni, és csak a jogszabályi előírások, valamint az Egyetem Adatvédelmi szabályzatában rögzítettek betartásához szükséges módon és ideig lehet azokat kezelni.
Az egyetemi tevékenységgel nem összefüggő, személyes, adótitoknak minősülő adatokat tartalmazó állományokat nem szabad a munkaállomásokon tárolni.

19.2 Informatikai biztonsági vizsgálatok

Az Egyetem célja biztosítani, hogy az informatikai biztonságot a hatályos informatikai biztonsági irányelvekkel és szabályzatokkal összhangban valósítsák meg és működtessék.

19.2.1 Az informatikai biztonság független vizsgálata

Az Egyetem az informatikai biztonság felügyeletével és megvalósításával kapcsolatos megközelítését (pl. informatikai biztonsági intézkedési célok, intézkedések, irányelvek, szabályzatok, folyamatok, eljárások) esetenként független vizsgálatnak vetheti alá.

19.2.2 A műszaki megfelelés vizsgálata

Az informatikai rendszert évente ellenőrizni javasolt a biztonság megvalósítását előíró szabványoknak történő megfelelés szempontjából. A műszaki megfelelőség ellenőrzése magába foglalja a hardver és szoftver védelmi intézkedések megvalósításának helyességét.

Bármilyen műszaki megfelelőség-ellenőrzést csak az erre felhatalmazott személyek végezhetnek, vagy külső szerződő fél esetén az Egyetem munkatársai legalább felügyelik azt.

A biztonsági szint mérésének eszközei és módszerei

A technikai szintű auditok
A biztonság szintje mérésének egyik leghatásosabb módszere a technikai audit jellegű felmérés:

a) az IT rendszer internet felőli sérülékenységeinek vizsgálata;
b) az IT rendszer intranet felőli sérülékenységeinek vizsgálata.

Technikai szintű auditot az Egyetemnél kétévente, vagy egy új rendszer bevezetésekor a fenyegetettségek felmérésével egy időben kell elvégezni, a végrehajtásért az Informatikai Biztonsági Felelős és az Informatikai Főosztályvezető együttesen felelős.

Működés-folytonossági és katasztrófa-elhárítási tesztek
A működés-folytonosság biztosítása érdekében visszaállítási- és a katasztrófa-elhárítási terveket évente, elemenként tesztelni kell. A tesztelés eredményét a tervezésbe, illetve a szóban forgó eljárásokba (mentés, karbantartás, stb.) vissza kell csatolni.
A működés-folytonossági eljárásrendet a ténylegesen bekövetkező incidensek esetén lehet 'élesben' alkalmazni, az itt fellelt hiányosságokat, a megszerzett tapasztalatokat a tervekbe vissza kell csatolni (a tanulságok összegyűjtése az incidens-jelentések részévé teendő). A tesztelés megtervezését, koordinálását az Informatikai Főosztályvezető végzi, a tesztek végrehajtásáért az informatikai szolgáltatások rendszergazdái felelősek.

Az informatikai rendszer monitorozása
Az informatikai rendszer kritikus elemeit, illetve biztonsági eszközeit folyamatosan monitorozni kell. A monitorozásnak minimálisan az alábbi témákra kell kiterjednie:

a) határvédelmi incidensek, és hálózati illegális tevékenység. Felügyeletet ellátó személy: Határvédelmi rendszergazda;
b) vírusvédelmi incidensek, vírusvédelmi rendszerek állapota (vírus DB és motor verziója eszközönként). Felügyeletet ellátó személy: Vírusvédelmi rendszergazda;
c) jogosultság kezelési incidensek. Felügyeletet ellátó személy: Jogosultságkezelésért felelős rendszergazda;
d) mentési feladatok sikeres/sikertelen végrehajtása. Felügyeletet ellátó személy: Mentésért felelős rendszergazda;
e) külső felhasználók tevékenységei, távoli elérések naplózása. Felügyeletet ellátó személy: Informatikai Biztonsági Felelős;
f) rendszergazdák tevékenységei. Felügyeletet ellátó személy: Informatikai Biztonsági Felelős
g) biztonsági riasztórendszerek naplózása (UPS, tűzvédelem, stb.). Felügyeletet ellátó személy: Informatikai Biztonsági Felelős.

19.2.3 Szállítók megfelelésének vizsgálata

Az Egyetem rendszeresen – legalább évente - ellenőrzi a szerződő felek szerződéses, jogszabályi illetve egyéb szabályozói követelményeknek való megfelelését.

20. ZÁRÓ ÉS HATÁLYBA LÉPTETŐ RENDELKEZÉSEK

E szabályzat a Szenátus általi elfogadás napján lép hatályba, rendelkezéseit a hatálybalépését követő naptól alkalmazni kell.

E szabályzat hatálybalépésével egyidejűleg hatályát veszíti a korábbi Informatikai Biztonsági Szabályzat.

Budapest, 2016. október 14.

Prof. Dr. Heidrich Balázs
rektor

Budapesti Gazdasági Egyetem
Budapest

Dr. Dietz Ferenc
kancellár

Záradék:

A Szabályzatot a Szenátus 2016. október 14-i ülésén a 2016/2017. tanévi (X. 14.) 7. számú határozatával fogadta el. Hatályos 2016. október 15. napjától.

1. sz. melléklet – Felhasználói nyilatkozat

Felhasználói nyilatkozat

A Budapesti Gazdasági Egyetem Informatikai Biztonsági Szabályzatát áttanulmányoztam, megértettem, tudomásul veszem és magamra nézve kötelezőnek tekintem. Tudomásul veszem, hogy a fenti szabályzat megsértése esetén az Egyetem ellenem eljárást kezdeményezhet.

Dátum

.....

Felhasználó

2. sz. melléklet – Titoktartási nyilatkozat

Titoktartási nyilatkozat

Alulírott

Magánszemély/Egyéni vállalkozó:
Név:
Anyja neve:
Szül. hely és idő:
Személyi azonosító okmány száma:
Lakcím:

Gazdálkodó szervezet[1]:
Cégnév:
Székhely:
Adószám:
Cégjegyzékszám:

kijelentem, hogy a Budapesti Gazdasági Egyetem (BGE) Informatikai Biztonsági Szabályzatának külső partnerekre vonatkozó részeit megismertem, azokat magamra nézve kötelezőnek ismerem el. A BGE-n végzett munkám teljesítése során megismert, az Egyetem tevékenységéhez kapcsolódó minden olyan adat, tény, információ, stb. (a továbbiakban: adat), amelynek a nyilvánosságra hozatala, illetéktelenek által történő megszerzése vagy felhasználása az Egyetem, illetve az Egyetem polgárai jogszerű személyes-, pénzügyi-, gazdasági- vagy biztonsági érdekét sértené vagy veszélyeztetné – és amelyet jogszabály egyébként más titokfajtának nem minősít – az Egyetem üzleti titkát képezik. A tudomásomra jutó titko(ka)t, adato(ka)t a vonatkozó jogszabályokra és az Egyetemmel kötött szerződésben vagy megállapodásban rögzítettekre figyelemmel kezelem. Titoktartási kötelezettségem körében a tudomásomra jutott adatokat illetéktelen részére hozzáférhetővé nem teszem, nem közlöm, át nem adom, nyilvánosságra nem hozom, fel nem használom.
Tudomásul veszem, hogy a titoktartási kötelezettségem időkorlátozás nélkül áll fenn, függetlenül attól, hogy milyen munkakörben és kinek a megbízottja, illetve munkavállalója vagyok. Tudomásul veszem továbbá, hogy a titoktartási szabályok megsértéséért – az egyéb jogi következményeken túl – felek egymással szemben kártérítési felelősséggel is tartoznak.

Dátum:

.....
aláírás

[1] *A megfelelő (magánszemély/egyéni vállalkozó/gazdálkodó szervezet) rész kitöltendő, a nem releváns törölhető.*

3. sz. melléklet – Az Egyetem informatikai biztonságára vonatkozó, illetve ahhoz kapcsolódó jogszabályok

- 2011. évi CCIV. törvény a felsőoktatásról
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Avtv.)
- Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK Irányelve a személyes adatok kezelése vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.
- 331/A/2001. számú adatvédelmi biztosi állásfoglalás: a munkáltató csak az érintett hozzájárulásával tekinthet be a munkavállaló munkahelyi e-mail címén történő levelezésébe.
- 570/A/2001. számú adatvédelmi biztosi állásfoglalás: a munkáltató csak akkor ismerheti meg a munkavállaló internet-használatával kapcsolatos adatait, ha előzetesen felhívta a figyelmét az ezzel kapcsolatos korlátozásra és az ellenőrzés lehetőségére.
- 2001. évi XXXV. törvény az elektronikus aláírásról
- 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről.
- 2015. évi CXLIII. törvény (kbt.) a közbeszerzésekről.
- 171/2010. (V.13.) Kormányrendelet a kormányzati informatika koordinációjáról és a kapcsolódó eljárási rendről
- 2012. évi I. törvény a munka törvénykönyvéről
- 2012. évi C. törvény a Büntető Törvénykönyvről
- 2013. évi V. törvény a Polgári Törvénykönyvről

4. sz. melléklet – alap jogosultságok

- levelezés
- egyetem honlapja védett tartalmak elérése
- egyetemi wifi-hez csatlakozás lehetősége