PANNON EGYETEM

INFORMATIKAI SZABÁLYZAT

1. MELLÉKLET
INFORMATIKAI BIZTONSÁGI AJÁNLÁS

TARTALOMJEGYZÉK

I. Célkitűzés

A jelen Informatikai biztonsági ajánlása (továbbiakban ITB) az **MSZ ISO/IEC 27001: 2006 szabvány** figyelembevételével készült. Az ITB tartalmazza az Informatikai biztonságpolitika alapelveit, az információbiztonsági rendszer célkitűzéseit és megvalósítandó feladataihoz szükséges intézkedéseket.

1. Célok meghatározása

Az ITB célja, hogy általános informatikai biztonsági előírásokat és szabályokat javasoljon a Pannon Egyetem (továbbiakban Egyetem) informatikai vagyontárgyainak védelmével kapcsolatosan és megalapozza a teljes egyetemi, informatikai biztonsági rendszer kiépítését. Ezen belül javaslatot tesz a szabályok, utasítások végrehajtására és a végrehajtás ellenőrzéséért felelős szerepköröket meghatározására.

További célok:

a) stabil, biztonságos, hatékony informatikai infrastruktúra kialakításával garantált minőségű és ellenőrizhető hozzáférés biztosítása az egyetem informatikai hálózatához és az azon nyújtott szolgáltatásokhoz az egyetemi felhasználók számára (a számítógépes hálózati kapcsolatok és információs szolgáltatások biztosítása),
b) az egyetemen folyó információszerzés és szabad áramlás elősegítése, oktatási, kutatási és fejlesztési, valamint tudományos és kulturális feladatok informatikai eszközökkel való támogatása,
c) az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
d) egyetemi üzletmenet folytonosságának biztosítása,
e) a titok-, vagyonvédelemre vonatkozó előírások betartása (hálózat, terminálok, adatok),
f) stabil adatkezelő és nyilvántartó rendszerekre vonatkozó védelem biztosítása, hardveres és szoftveres adattárolás és adatvédelem biztosítása,
g) biztonságos hálózat és terminál üzemeltetése,
h) NIIFI hálózatának használatára vonatkozó szabályzatok betartása.

2. Az információbiztonsági rendszer kiépítésének előnyei

a) Bizalmasság, sértetlenség, rendelkezésre állás alapelvek teljesülése,
b) A bizalom, a biztonság és az imázs növekedése,
c) a költségcsökkentés,
d) a hatékonyságnövelés,
e) a konkurenciával, többi egyetemmel szembeni versenyelőny,
f) az információval való visszaélés minimalizálása,
g) az egyetemi üzletfolytonosság biztosítása és
h) az informatikai kockázat kezelése és csökkentése.

II. Fogalmak, rövidítések

Adatállomány: 2011. évi CXII.tv. alapján: egy nyilvántartásban kezelt adatok összessége.
Adatgazda: adatállomány tulajdonosa és kezelője, aki az adott adatkezelésre vonatkozó döntési jogosultsággal rendelkezik, a 8/2012. (II.16.) LÜ utasítás alapján.
Adatbiztonság: a személyes adatok jogosulatlan kezelése, különösen megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások és eljárási szabályok összessége, az adatkezelésnek az az állapota, amelyben a kockázati tényezőket - és ezzel a fenyegetettséget - a szervezési, műszaki megoldások és intézkedések a legkisebb mértékűre csökkentik. 8/2012. (II./16.) LÜ utasítás.
Alapbiztonsági fokozat: általános informatikai feldolgozás alapján. Különösen személyes adatok, pénzügyi adatok, üzleti titkok.
Betekintési és megismerési / olvasási jogosultság vagy hozzáférés: az a jogkör, amelynek birtokában a jogosult számára elérhetővé, megismerhetővé válnak az adott adatállományban kezelt adatok vagy az informatikai rendszeradatok. A betekintési jogosultsággal az érintett adatokat másolni, továbbítani, kezelni vagy törölni tilos.
Biztonságos munkaterület vagy környezet: különösen olyan irodák, szerverszobák vagy egyéb helységek, ahol informatikai eszközökkel való munkavégzéskor biztosítani kell a munkát végző személy és az informatikai eszközök sértetlenségét. Különösen a vezetékezés, eszközhasználat szabályainak betartásával.
Bizalmasság, titkosság: Olyan tulajdonság, amely biztosítja, hogy az információt jogosulatlan egyének, entitások vagy folyamatok számára nem teszik hozzáférhetővé.
Biztonsági terület: olyan terület, ahol kritikus vagy érzékeny adatokat tárolnak. Ezeket az adatokat és az adatokat tároló informatikai eszközöket megfelelő védelemmel kell ellátni, különösen betörés, szándékos károkozás, elemi vagy egyéb kár bekövetkezésének elkerülése érdekében. Erre szolgáló eszközök például a riasztórendszer, biztonsági kamera vagy tűzjelző.
Business Continuity: működési vagy üzletfolytonosság.
Érzékeny adat: lásd: az Egyetem Adatvédelmi és Adattovábbítási Szabályzata és a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 2011. évi CXII.tv. .
Gépterem vagy rendszerfelügyeleti terem: Olyan egyetemi helység, ahonnan a szerverek, hálózati eszközök távoli felügyeletét látják el.
Harmadik fél vagy személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval (2011. évi CXII.tv. alapján).
Hozzáférési intézkedés politikája: felhasználók azonosítási jele (ID) és szükség szerint kódolt jelszavai, megengedett hozzáférési módok, az egyedi azonosítók ellenőrzése és használatának leírása, hozzáféréshez szükséges jogosultságok leírása, nyilatkozat a nem engedélyezett hozzáférések letiltásáról, folyamat leírása a hozzáférési jogok visszavonásáról vagy a felhasználók által használt informatikai rendszerek közötti kapcsolat megszakításáról.
Informatikai audit (Audit): az informatikai eszközhasználat, eljárásrendek, szabályzatok betartásának ellenőrzése. Más néven: informatikai rendszeraudit.
Informatikai audit kísérődokumentáció: Audit Trail, az informatikai ellenőrzés során előtérbe került és az aktuális üggyel kapcsolatos elektronikus és papír alapú dokumentációk összessége.
Informatikai vagyontárgy (vagyonelem): ISO/IEC 13335-1:2004 szabvány alapján, minden olyan informatikai eszköz, amely az Egyetem számára értéket jelent.
Informatikai biztonság fogalomköre: különösen az adatvédelem, az adatbiztonság, az információbiztonság, az információvédelem vagy a megbízható működés.

Információbiztonság: MSZ-ISO/IEC 17799:2006 szabvány alapján: „Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése…” Az információbiztonságba bevonható különösképpen „a hitelesség, a számon-kérhetőség, a letagadhatatlanság és a megbízhatóság”.
Információbiztonsági esemény: ISO/IEC TR 18044:2004 szabvány alapján: „…egy rendszer, szolgáltatás vagy hálózat állapotának azonosított előfordulása, amely mutatja az információbiztonsági politika esetleges megsértését vagy a biztonsági ellenintézkedések kudarcát vagy egy előzőleg ismeretlen helyzetet, amely lehet biztonság vonzatú.”
Információbiztonsági incidens: ISO/IEC TR 18044:2004 szabvány alapján: „Nem kívánt vagy nem várt egyedi vagy sorozatos információbiztonsági események, amelyek nagy valószínűséggel veszélyeztetik az üzleti tevékenységet és fenyegetik az információbiztonságot.”
Intézkedés: MSZ-ISO/IEC 17799:2006 szabvány alapján, kockázatkezelés eszköze, különösen szabályzatok, eljárások, irányelvek alkalmazása adminisztratív, műszaki, irányítási vagy jogi ügymenet esetén.
Közvetlen megismerési jogosultság: adott adatállomány informatikai alkalmazás igénybevételével kezelt adatainak megismeréséhez adott olyan jogkör, amely a jogosult számára lehetőséget biztosít arra, hogy az ott kezelt adatokhoz az általa megválasztott időpontban közvetlen lekérdezéssel hozzáférjen;
Közvetlen lekérdezés: adott adatállományban kezelt adatokban - az adatkezelő által előzetesen rendelkezésre bocsátott általános lekérdezési jogosultság felhasználásával - előre meghatározatlan időpontban és alkalommal, naplózott formában történő betekintés vagy az így megismerhetővé vált információ kinyomtatása.
Kritikus adat: különösen a kritikus informatikai rendszerben vagy papíron nyilvántartott, nem nyilvános jellegű adat.
Politika: Az Egyetem által hivatalosan is rögzített széles körű szándék és irányvonal.
Rendelkezésre állás: Olyan tulajdonság, amely lehetővé teszi, hogy az adott objektum – feljogosított entitás által támasztott igény alapján – hozzáférhető és igénybe vehető legyen.
Számítógépes labor: Oktatást vagy kutatást szolgáló nyilvános hallgatói PC terem.
Szerverszoba: Olyan egyetemi helység, ahol szervereket és hálózati eszközöket üzemeltetnek és a felügyeletet nem a helyszínen, hanem távoli eléréssel látják el.
Sértetlenség: A vagyontárgyak pontosságának és teljességének védelmét biztosító tulajdonság.
Számítógépes szerviz: Informatikai eszközök, különösen PC-k, nyomtatók, laptopok javítására szolgáló, szervízelési segédeszközökkel felszerelt egyetemi helység.
Szoftverzavar vagy hardverzavar: véletlen informatikai biztonsági esemény.

III. Informatikai biztonságpolitika

Az Informatikai biztonságpolitika (továbbiakban IBP) célja, hogy az Egyetem szervezeti egységei részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának biztosítása érdekében követendő irányelvekre. Az irányelvek figyelembevételével meghatározható az informatikai rendszerek biztonsági osztályba sorolása; kidolgozható a konkrét, rendszer szintű informatikai biztonsági szabályozás, amely meghatározza a szabványos biztonsági funkciók tervezéséhez, megvalósításához, üzemeltetéséhez és megszüntetéséhez a szükséges alapelveket és követelményeket.

Az Egyetem vezetősége az ITB elfogadásával támogatja az információbiztonság céljait és alapelveit a működési stratégiával és a célokkal összhangban.

Az informatikai rendszerek biztonsági, az Egyetem működéséhez igazított kategóriáit az Informatikai Szabályzat (továbbiakban ISZ) részletezi. A biztonságos használatra és üzemeltetésre vonatkozó felhasználói előírásokat az ISZ, az Egyetem központi rendszerüzemeltetői rendelkezéseket a Központi informatikai üzemeltetési és szolgáltatói minőségirányítási eljárás (továbbiakban IT Eljárás) tartalmazza.

1. Az IBP helye

Az Informatikai biztonságpolitika az ITB része, ezért elfogadása és közzététele az ITB-al együtt történik.

2. Az IBP alapelvei

Az Egyetem szervezeti egységei által kezelt adatok, információk védelmét bizalmasság, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából úgy kell megvalósítani, hogy az informatikai rendszernek és környezetének védelme folytonos, teljes körű, zárt és a kockázatokkal arányos legyen, valamint megvalósuljon a zárt szabályozási ciklus.

2.1 Általános irányelvek

a) a hitelesség biztosítása,
b) a bizalmasság biztosítása,
c) a sértetlenség biztosítása,
d) a rendelkezésre állás,
e) a biztonsági osztályba sorolás és
f) a működőképesség fenntartása.

2.2 Az általános irányelvek figyelembevételével az alábbi alapelvek alakíthatók ki

a) Teljes körűség. A védelmet fizikai, logikai és adminisztratív vonatkozásban egyaránt érvényesíteni kell.
b) Zártság. A védelem zártságát akkor lehet biztosítani, ha az összes valószínűsíthető fenyegetés elleni védelmi intézkedések megvalósulnak.
c) Kockázatarányosság. A védelem akkor kockázatarányos, ha az informatikai rendszerek által kezelt adatok védelmének erőssége és költségei a felmért kockázatokkal arányban állnak.
d) Folytonosság. Az informatikai rendszerek bevezetése és fejlesztése során kialakított védelmi konfigurációkat a rendszerből való kivonásig folyamatosan biztosítani kell: a rendszeres ellenőrzéssel és biztonsági intézkedésekkel.
e) Zárt szabályozási ciklus alapelve. A zárt szabályozási ciklus úgy érvényesíthető, hogy az adminisztratív védelemben biztosítani kell: a szabályozás-, érvényesítés-, ellenőrzés-, szankcionálás folyamatát és a ciklikus folyamatosságát.
f) Differenciált védelem. Az informatikai rendszerek védelmét az általuk kezelt adatok biztonsági osztályba sorolására kell alapozni.
g) Létfontosságú, hogy a fokozott biztonsági kategóriájú informatikai rendszereket olyan környezetben kell telepíteni és működtetni, amelyben az adatok és az adatfeldolgozás bizalmassága, sértetlensége, rendelkezésre állása és auditálhatósága egyaránt magas szinten garantált. Az ellenőrzésekről Audit Jegyzőkönyvet kell készíteni.
h) Kockázatelemzés. A kockázatokat minimalizálni kell. Minden felhasználóban tudatosítani kell, hogy teljes körű védelem és biztonság nincsen, és ezzel összefüggésben a maradvány kockázatot a Hálózati Iroda (továbbiakban HI) tudatosan vállalja, és elkészíti az Egyetem központi informatikai BCP elemzését. Az elemzés része a kockázatspecifikáció. A specifikáció tartalmazza a kockázatfelmérés módszertant, kockázatok azonosítását (a potenciális fenyegetettségek számbavételét), a katasztrófabekövetkezés valószínűségének, jellegének (hirtelen, fokozatos) és lefolyása időtartamának meghatározását.
Az elemzés során ki kell dolgozni az alábbi dokumentációkat:
- Vagyonleltár,
- Kockázat specifikáció,
- Veszélyforrások és azok bekövetkezési valószínűségei,
- Elfogadható kockázat,
- Kockázatkezelés, Kockázat-hatás elemzés alapjai.

i) Engedélyezés. Megfelelő felhasználói felhatalmazás, jogosítvány, engedély kibocsátás és jogosultság kibocsátás. A felhasználói jogosultságok természetes személyhez kötöttek és nem átruházhatóak. A visszaélés és a károkozás felelőssége a károkozás körülményétől függően a rendszerüzemeltetőt, a HI vezetőjét, a felhasználót és a szervezeti egységének vezetőjét terheli (ISZ vonatkozó fejezetei alapján). Rosszhiszemű felhasználásnak tekintendő, ha a felhasználó a jogosultságát meghaladó műveleteket szándékosan kezdeményez illetve jogosultságát megkísérli módosítani.

2.3 Az IBP alapelvei alapján elkészítendő vagy kapcsolódó dokumentációk

a) Adatvédelmi és Adattovábbítási Szabályzat,
b) Informatikai Üzletmenet Folytonossági Terv (BCP - Business Continuity Plan),
c) Központi informatikai üzemeltetési és szolgáltatói Eljárás,
d) Elektronikus dokumentumok biztonsági adatmentése, eljárás,
e) Intézményi Fejlesztési Terv.

Az előírásokat az illetékes szervezeti egység készíti el és az egységvezető gondozza, az informatikai szabályzatokat a HI készíti el és a HI vezetője terjeszti az Egyetem Szenátusa elé Informatikai Hálózatok és Fejlesztések Bizottság (továbbiakban IHéFB) ajánlása alapján.

2.4 Az informatikai vezetőség felelőssége

Az információbiztonsági politika gondozója a HI vezetője, akinek jóváhagyott vezetőségi felelőssége van a biztonsági politika fejlesztéséért, átvizsgálásáért és kiértékeléséért.

IV. Informatikai biztonság szervezete, az adatvagyon kezelése

1. Informatikai biztonsági infrastruktúra felépítése, az informatikai biztonság elemei és a biztonság kezelése

1.1 Egyetemi résztvevők

Az Egyetem célja az intézményi információbiztonság kialakítása, fenntartása, felügyelete és magasabb szintre való emelése. A létrehozandó irányítási keretrendszerrel kialakítható és szabályozható az információbiztonság bevezetése az intézményen belül. Az IBP alapján a HI vezetője kijelöli a központi biztonsági feladatköröket, amely koordinálja és vizsgálja az információbiztonság bevezetését az Egyetemen.

1.1.1 Informatikai biztonsági szakértő feladata

a) Informatikai szabályzatok, ajánlások és HI előírások kidolgozása és aktualizálása a HI vezetőjének irányításával.
b) Egyetemi és HI szintű informatikai rendszerauditokban való részvétel, felkérés alapján informatikai biztonsági kockázatok felderítése.
c) HI informatikai üzletmenet-folytonossági és katasztrófa-elhárítási tervének kidolgozása a HI vezetőjének irányításával.
d) Egyetemi és HI szintű IT biztonsági esetekben való aktív közreműködés, dokumentálás és az adott eset a HI informatikai katasztrófatervében rögzített módon való tájékoztatása.

1.1.2 Informatikai biztonsági szakértő joga és kötelezettsége

a) Az informatikai biztonsági szakértőnek joga van az előző pontban említett feladatok elvégzéséhez szükséges informatikai rendszerek áttekintésére és bizonyos jogosultságok használatára a munkaköri leírásában meghatározottak alapján.
b) Elvégzi a jelen fejezet 1.1.1 pontjában felsorolt feladatokat, figyelembe véve a felhasználói, fejlesztési, üzemeltetési és informatikai strukturális igényeket.
c) A szakértő figyelembe veszi a prioritásokat az egyetemi IT biztonsági események elhárításában részt venni és azt megfelelően dokumentálja, ezzel minél előbb biztosítva a zökkenőmentes és biztonságos működést. A fontosabb események a *hiba.uni-pannon.hu* honlapon naplózza, különösen a hacker tevékenységre utaló eseményeket.
d) Tájékoztatást ad a felhasználó által kért, a felhasználó feladatához tartozó informatikai biztonsági kérdésekben különösen a számítógép használatával, a szoftver beállítással és alkalmazással és a levelezőrendszer használatával kapcsolatos nehézségekben.
e) Az Egyetem rektora által elrendelt egyetemi szintű informatikai ellenőrzés alkalmával együttműködik.

1.2 Külső felek közreműködése

Az egyetemi informatikai eszközökhöz szerződésben rögzített feltételek mellett külső felek is hozzáférhetnek. A külső fél által használandó egyetemi informatikai eszközöket az üzemeltető szervezeti egységének az adott informatikai rendszer specifikációja szerint meghatározott védelemmel való ellátása javasolt. Ez által az Egyetem lehetővé teszi a külső felek által használható

- informatikai infrastruktúra megfelelő színvonalú biztonságát, amelyen az információ feldolgozása, közlése történik a külső felek felé vagy
- az infrastruktúra azon egységét, amelyet a külső felek kezelnek.

Az Egyetem informatikai infrastruktúrájának biztonsága nem csökkenthető a külső fél termékeinek vagy szolgáltatásainak bevezetésével. A szerződést az Egyetem SZMSZ-ében meghatározott előírások alapján kell megkötni.

Javasolt szabályozni az Egyetem összes informatikai eszközéhez belső szervezeten belül vagy külső fél általi hozzáférést, információ feldolgozást és különösen a külső fél számára való információ továbbítását. A szabályozást a központi informatikai eszközök esetében a HI egyéb esetben az üzemeltető szervezeti egység dolgozhatja ki és gondozza, az eljárást az üzemeltetett informatikai rendszer specifikációjának mellékleteként javasolt szerepeltetni. Az egyetemi informatikai infrastruktúrához való külső fél hozzáférése esetén kockázatfelmérést készítése ajánlott, amely meghatározza a biztonsági kihatásokat és az intézkedési követelményeket. A kockázatfelmérést az üzemeltető szervezeti egységvezető dolgozhatja ki.

A felmérés tartalmazza:

a) a külső fél hozzáféréséhez szükséges egyetemi informatikai eszközök listáját,
b) a hozzáférés típusát, különösen: a fizikai-, a logikai- és a hálózati hozzáférést és a hozzáférés helyszínét,
c) az érintett információ értékét, besorolását,
d) az egyetemi belső, érzékeny információk védelmének módját és a külső fél számára való titkosítási megoldását,
e) a külső fél által egyetemi információ kezelésébe bevont személyek adatait, feladatait, azonosítását és hozzáférési jogosultságát,
f) a külső fél által alkalmazott különböző berendezéseket és intézkedéseket, különösen az információ tárolására, a feldolgozására, a közlésére és a cserélésére vonatkozóan,
g) az információbiztonsági incidensek és lehetséges károsodások kezelésére szolgáló gyakorlatot és az eljárásokat, a feltételeket és a kikötéseket a külső fél hozzáférésének folytatására információbiztonsági incidens esetén,
h) a külső félre vonatkozó jogi és szabályozási követelményeket és más szerződési kötelezettségeket.

Külső feleknek az egyetemi információkhoz, informatikai infrastruktúrákhoz való hozzáférését nem javasolt addig biztosítani, amíg a megfelelő, a feladatelvégzéshez szükséges informatikai biztonsági intézkedéseket az Egyetemen be nem vezették, az Egyetemmel olyan szerződést alá nem írtak, amely meghatározza a feladatelvégzéshez szükséges egyetemi informatikai infrastruktúrához való csatlakozás vagy hozzáférés kikötéseit és feltételeit, konkrét informatikai feladat leírását.

1.3 Harmadik féllel kötött megállapodások

Harmadik féllel kötött szerződéseknek tartalmazza az alábbi biztonsági követelményeket:

a) Az Egyetem IBP alapelveit.
b) Az egyetemi informatikai infrastruktúrát érintő biztonsági intézkedéseket.
   Kiemelten kezelendő az egyetemi vagyontárgyak védelmére vonatkozó intézkedések:
   az egyetem tulajdonában lévő információ-, szoftver- és hardver védelme, bármely fizikai védelmi intézkedés és mechanizmus, rosszindulatú szoftver elleni védelem, információvesztés vagy - módosítás, szoftver- vagy hardvermódosítás, bizalmasság, sértetlenség, rendelkezésre állás, korlátozások az informatikai másolására vagy felfedésére és titoktartási megállapodások.
c) A hardver és szoftver telepítésének és karbantartásának felelősségét, az egyértelmű és előírt módosításkezelési folyamatokat.
d) A hozzáférés-ellenőrzési politikát, amelyet HI dolgoz ki és aktualizál.
e) Rendelkezéseket az információbiztonsági incidensek és biztonsági sértések jelentésére, bejegyzésére és kivizsgálására, ezen kívül a megállapodásban rögzített követelmények megsértésére.
f) A szolgáltatásra kerülő termék vagy szolgáltatás leírását, valamint a hozzáférhetővé teendő információ leírását a biztonsági osztályozás meghatározásával,
g) A szolgáltatás előirányzott szintjének és a szolgáltatás el nem fogadható szintjeinek meghatározását.
h) Igazolható teljesítési kritériumok meghatározását.
i) Jogosultságok meghatározását, különösen az Egyetem informatikai vagyontárgyaira vonatkozó bármely tevékenység figyelemmel kísérésére és megvonására. A külső szolgáltató bevonásával elvégzett audit során ajánlott rögzíteni az információbiztonsági auditorok jogait és kötelezettségeit.
j) Probléma-megoldási folyamatok kidolgozását vagy iránymutatását.
k) A szolgáltatás folytonossági követelményeit, különösen a rendelkezésre állásra, megbízhatóságra vonatkozó intézkedéseket.
l) A megállapodásban szereplő felek felelősségeit, jogi követelmények teljesítését, különösen az adatvédelmi jogszabályok figyelembe vételét.
m) A harmadik fél alvállalkozóinak alkalmazásának feltételeit.
n) Feladat teljesítésére vonatkozó feltételeket, megállapodásokat.

1.4 Hallgatók egyetemi informatikai infrastruktúrához való hozzáférése

Az illetékes szervezeti egységvezetőnek biztosítsa a hallgató részére a használandó rendszerek és alkalmazások specifikációjának elérhetőségét, amelyet az adott informatikai rendszert üzemeltető szervezeti egység készít el. A specifikáció tartalmazhatja az alábbi hozzáférési meghatározásokat, tehát

a) az egyetemi informatikai vagyontárgyak védelmének meghatározását és biztosítását,
b) a hallgató által használható informatikai terméket vagy szolgáltatást, az egyetem által nyújtandó szolgáltatás előirányzott szintjét,
c) a hallgató az egyetemi informatikai infrastruktúrához való hozzáférésének indokait, előnyeit és a hallgatótól elvárt követelményeket,

d) az információbiztonsági intézkedéseket, az incidensek és a biztonság sértések körét,
e) az Egyetem és a hallgató kötelezettségeit és jogait,
f) az adatvédelmi előírásokat,
g) az esetleges szellemi tulajdonjogok és szerzői jog meghatározását.

2. Informatikai biztonsági menedzsment és koordináció, felelősségek, együttműködés

Az informatikai biztonságot egyetemi szinten kell menedzselni. Ehhez javasolt az Informatikai Menedzselési rendszer létrehozása. A rendszernek tartalmazhatja az Egyetemen belüli informatikai biztonsági feladatokra vonatkozó kezdeményezéseket, kivitelezéseket és ellenőrizési lehetőségeket. Az ITB alapján az IHéFB a HI támogatásával az intézményen belül szervezi és összehangolja az informatikai biztonságot és kidolgozza az Informatikai menedzselési rendszert, amely kapcsolódik a jelen fejezet 1.1 pontban feltüntetett feladatokhoz.

A HI vezetője és a biztonsági szakértő figyelemmel követik az informatikai fejlesztések és változások trendjét és irányát, a szabványokat, az értékelési tényeket és a biztonsági események kezelésére alkalmas belső és külső informatikai kapcsolatrendszert biztosítanak az Egyetem részére. Az informatikai biztonság kialakításánál javasolt figyelembe venni a teljesíthetőségek szerteágazását, az egyetemi felhasználók együttműködését és a szakmai gyakorlatot a biztosítás és a kockázatkezelés területén.

Az információbiztonsággal kapcsolatos felelősség megoszlik a HI, a szervezeti egységek és a felhasználók között.

A HI gondoskodik az egyetemi hálózat, a központi szerverek és a felügyeletük alá tartozó hálózati eszközök folyamatos és biztonságos működéséről, meghibásodás esetén az illetékes szervezeti egységvezető tájékoztatásáról, a központi és a felkérés alapján, megbízott rendszerüzemeltetővel nem rendelkező szervezeti egységek számítógépeinek, nyomtatóinak és egyéb perifériás informatikai eszközeinek szervizeléséről.

A szervezeti egységvezető gondoskodik a szervezeti egysége által használt informatikai eszközök megfelelő biztonsági beállításáról, felelős a szervezeti egység felhasználói által használt informatikai eszközök biztonságos használatáért és az ISZ megfelelő tájékoztatásáért.

A felhasználó köteles az általa használt informatikai eszközöket rendeltetésszerűen alkalmazni, amennyiben előzetes informatikai biztonsági tájékoztatón vett részt és az adott eszközt nem megfelelően használta, felelős a rendellenes használatért az informatikai szabályzatok szankcionálásra vonatkozó rendelkezése alapján.

V. A humán erőforrás-ellátás informatikai biztonságának kialakítására vonatkozó ajánlás

1. A humán erőforrás ellátással kapcsolatos biztonsági célkitűzés

A humán erőforrás-ellátással kapcsolatos informatikai biztonsági javaslatok alkalmazásának célja az emberi hibák, lopás, csalás és visszaélés kockázatának csökkentése.

2. Közalkalmazotti jogviszony

2.1 Személyi alkalmazás előfeltétele, közalkalmazotti jogviszony létesítése

A biztonsági felelősségekről az alkalmazás előtt is tájékoztatni kell a felhasználót és a munkaköri leírásában rögzíteni kell az alkalmazás biztonsági feltételeit. A biztonságos munkavégzés informatikai feltételeit a HI és az IHéFB kidolgozása alapján az Egyetem Rektora adja ki. A munkaköri leírásban rögzített biztonsági előírások folyamatos aktualizálásáról gondoskodni kell. Kinevezés előtti személyi feltételek megvizsgálását az alkalmazandó szervezeti egység vezetője végzi el. Az informatikai eszközöket használó valamennyi egyetemi közalkalmazott felhasználót titoktartási megállapodás kötésére kell kötelezni a Humánpolitikai szabályzat alapján. A titoktartási megállapodásban az elektronikus információkra is ki kell térni.

2.2 Munkakör meghatározásának alapelvei

a) Feladatmegosztás

Informatikai rendszereket használó vagy üzemeltető személyek feladatköreit az illetékes szervezeti egységvezetőnek úgy kell meghatározni, hogy azzal minimalizálható legyen a mulasztások és szándékos visszaélések kockázata. Biztosítania kell a lehető legteljesebb körű helyettesítést vagy kiváltást. Ha az informatikai rendszer üzemeltetése megköveteli az üzemeltetési feladatok ellátására ügyeleti rendszert kell kialakítani. A feladatmegosztás kialakítása informatikai biztonsági feladat, ezért a szervezeti egységvezető kérheti a HI erre vonatkozó álláspontját.

b) Feladatelhatárolás

Az informatikai biztonság szempontjából összeférhetetlen munkaköröket szét kell választani a szükséges tudás elve alapján. A felelős vezető a felhasználó egyetemi kötelezettségének függvényében határozza meg a jogosultságokat különösen az adatkezelésre és az informatikai rendszerek használatára vonatkozóan. A feladatelhatárolások kialakítása informatikai biztonsági feladat, ezért a szervezeti egységvezető kérheti a HI erre vonatkozó álláspontját.

2.3 Személyi alkalmazás

Közalkalmazotti jogviszony létesítésekor a leendő közalkalmazott szervezeti egységének vezetője köteles az ISZ-ban meghatározott előírásokat betartani. A munkaköri leírás alapján rögzíteni kell a jogosultságokat és felelősségeket. Minden rendszerüzemeltető, fejlesztő vagy felhasználó csak a munkakörének ellátásához szükséges jogosultságokkal rendelkezhet. Az ISZ Fogalomtárában megfogalmazott kritikus és kiemelt rendszereket alkalmazó és üzemeltető felhasználókat az első használat vagy frissített változat alkalmazása előtt oktatásban vagy tájékoztatásban kell részesíteni, amiről a felhasználó szervezeti egységének vezetője gondoskodik. A tájékoztatás teljesítésével keletkezett többletköltség a felhasználó szervezeti egységét terheli. A hiányos tájékoztatás vagy a nem megfelelő oktatás miatt bekövetkezett informatikai infrastruktúrát érintő károkozás felelőssége a felhasználó szervezeti egységvezetőjét terheli.

2.4 Kilépés, elbocsátás vagy munkakör-változás

A felhasználó kilépésére vonatkozó előírásokat az ISZ VIII. fejezete valamint a Központi informatikai üzemeltetői és szolgáltatói eljárás rögzíti. Ezen felül javasolt a felhasználó kilépése vagy elbocsátása esetén minden rendszerüzemeltetői, fejlesztői és egyéb felhasználói jogosultságok valamint az Egyetem szerverein bármilyen tevékenységet lehetővé tevő belépési kódok azonnali visszavonása, amit a kilépő felhasználó és szervezeti egységének vezetője kezdeményez. Amennyiben a felhasználó közalkalmazotti jogviszonya megszűnik, de feladatait más jogviszony keretén belül látja el, a régi jogosultságokra vonatkozókat vissza kell vonni és új felhasználó jogosultságot kell létrehozni.

3. Biztonság és munkaköri felelősség

Az informatikai biztonság olyan felelősség, amelyet az Egyetem vezetői és munkatársai egyaránt viselnek.

Kiemelt felelősségek az informatikai biztonság területén:

a) HI vezetője,
b) Üzemeltetési és biztonságszervezési igazgató,
c) Informatikai biztonsági szakértő,
d) Adatvédelmi felelős.

3.1 Vezetői felelősség

Minden szervezeti egység vezetője személyesen felel az információbiztonság kultúrájának kialakításáért és fenntartásáért. A vezetők az elkötelezettségüket személyes példamutatással és személyes felelősségvállalással szemléltessék. A belső és külső informatikai szolgáltatói megállapodások (SLA) figyelése, nyomon követése és az ehhez

kapcsolódó tények elemzése informatikai vezetői feladat. Az információbiztonsági intézkedések megvalósításához biztosítani kell a szükséges informatikai és emberi erőforrásokat. Az Egyetem informatikai rendszereit, az informatikai rendszerüzemeltetési specifikációt és az informatikai üzemeltetői munkaköri leírásokat az üzemeltető szervezeti egységvezetőnek lehetőleg úgy kell kialakítania, hogy megfeleljen az ITB előírásainak. Az Egyetem Központi Igazgatás felügyelete alá tartozó központi informatikai rendszerek ITB-el való megfelelése a HI vezetőjének hatásköre és felelőssége.

3.2 Felhasználói felelősség

A felhasználó az egyetemi informatikai eszközök használatára vonatkozó kötelességeit és felelősségét az ISZ vonatkozó fejezete rögzíti. A felhasználó köteles a szervezeti egység vezetője által megfogalmazott és elvárt biztonsági előírásokat betartani különösen a kritikus és a kiemelt informatikai rendszerek használata esetén.

3.3 Rendszerüzemeltetői felelősség

A központi rendszerüzemeltető az egyetemi informatikai eszközök használatára vonatkozó kötelességeit és felelősségét az Központi informatikai üzemeltetői és szolgáltatói eljárás rögzíti. A központi rendszerüzemeltető köteles a szervezeti egység vezetője által megfogalmazott és elvárt biztonsági előírásokat betartani különösen a kritikus és a kiemelt informatikai rendszerek üzemeltetése és használata esetén.

4. Az informatikai biztonság oktatására és képzésére vonatkozó ajánlások

4.1 Informatikai tájékoztatás és oktatás

Az ITB személyi hatályába tartozó személyeket – a titoktartási nyilatkozat aláírását követően – az informatikai rendszerekben való munkavégzést megelőzően tájékoztatni kell és biztosítani kell számukra az informatikai szabályzatok elérhetőségét. A felhasználó szervezeti egység vezetőjének gondoskodnia kell arról, hogy a felhasználó a dokumentumot megkapja vagy belső egyetemi hálózaton elérhesse.

Az érintett szervezeti egységvezetőnek szükség esetén a betöltött munkakörtől függő rendszer-specifikus informatikai oktatást kell biztosítania a munkavégzést megelőzően. Az informatikai oktatást új rendszer bevezetése vagy meglévő rendszer frissítése esetén is meg kell tartani. Lehetőséget kell adni arra, hogy a jelenlévők felhasználói, gyakorlati problémáikra is választ kapjanak. Ebben az esetben az oktatáson való részvétel kötelező a rendszert használó összes felhasználó számára. Az oktatásról vagy tájékoztatásról az érintett felhasználó szervezeti egység vezetője gondoskodik és a rendszer üzemeltetőjének kötelező a részvétel. Az oktatásról emlékeztetőt és jelenléti ívet kell felvenni. Az oktatásnak tartalmaznia kell az érintett rendszerhez kapcsolódó informatikai biztonsági ismereteket és követelményeket is. Az adott rendszerhez tartozó követelményeket a rendszert üzemeltető szervezeti egységnek kell kiadni.

4.2 Informatikai képzések

Az informatikai szakembereknek a betöltött munkakörtől függő, belső vagy külső informatikai képzéseket célszerű biztosítani. A képzés úgy kell kiválasztani, hogy igazodjon az Egyetemen lévő és az adott felhasználó által használt vagy üzemeltetett rendszerekhez és teljesítse az Egyetem **Minőségirányítási Kézikönyvében** foglaltakat. Az informatikai képzések tervezéséhez a Minőségirányítási Kézikönyv **PE-MK-02** és a belső képzésekhez a Minőségirányítási Kézikönyv **PE-MK-03** számú mellékletét kell használni. Külső képzés kiválasztása esetén az üzemeltetéshez magas színvonalú, felsőfokú képzéseket kell előnybe részesíteni. A kiválasztott képzésnek informatikai biztonsági tartalommal kell rendelkeznie. A képzések ajánlását a HI végzi el, amelynek segítségével kiválasztható az adott felhasználóra és az alkalmazott rendszerhez igazodó megfelelő színvonalú képzés.

5. Biztonsági események, zavarok

Az Egyetem HI-a vagy az üzemeltető szervezeti egység gondoskodik arról, hogy az általa üzemeltetett informatikai rendszerekben a biztonsági rések és zavarok által keletkezett kár minimális legyen. A felderített károkat az üzemeltető szervezeti egység rendszerüzemeltetőinek elemezni kell és ez alapján ki kell alakítani a DRP-t és növelni kell a biztonságtechnikai alkalmazásokat.

Potenciális fenyegetettségek

Fenyegetettség típusa	**A bekövetkezés**		
	esélye	**jellege**	**lefolyás időtartama**
Áramkimaradás	közepes	hirtelen	rövid
Informatikai rendszer leállása	alacsony	hirtelen	változó
Elektronikus adatok sérülése,	alacsony	hirtelen	változó
Elektronikus adatok eltulajdonítása	közepes	fokozatos	változó
Vírusfertőzés, kártékony alkalmazások	közepes	fokozatos/ hirtelen	mértéktől függő
Interneten keresztül történő támadás (szerver, kliens szg.)	magas	fokozatos/ hirtelen	mértéktől függő
Betörés	közepes	hirtelen	mértéktől függő
Szándékos rongálás	alacsony	fokozatos/ hirtelen	mértéktől függő

5.1 A biztonság gyenge pontjai

Az Egyetem illetékes polgárait tájékoztatni kell a biztonság gyenge pontjaival kapcsolatos kötelezettségeikről. A felhasználó által észlelt informatikai infrastruktúrához

kapcsolódó biztonsági gyengeséget, fenyegetettséget vagy ezek gyanúját jelezni kell az adott szervezeti egységvezetőnek és a HI vezetőjének. A HI az értesítés alapján megvizsgálja az érintett informatikai rendszert vagy szolgáltatást és megteszi a szükséges lépéseket.

A felhasználóknak tilos kezelni a feltételezett biztonsági gyengeséget vagy fenyegetettséget, mert ez a rendszerrel kapcsolatos visszaélésnek minősülhet. A biztonsági gyengeség vagy fenyegetettség jelzéshez egyetemi szinten előre definiált, elektronikus dokumentum (*hiba.uni-pannon.hu*) alkalmazása ajánlott, amelyet a HI aktualizál.

A bejelentésnek tartalmaznia kell:

- a gyengeség vagy a fenyegetettség rövid leírását,
- az észlelő nevét, szervezetét és elérhetőségeit,
- az észlelés időpontját és helyét,
- az értesített személyek nevét, szervezetét,
- az eset esetleges részletes leírását,
- egyéb megjegyzéseket.

A HI a gyengeségről vagy a fenyegetettségről szóló jelentés kézhezvételét követően visszajelez a jelentés készítőjének. A visszajelzésnek tartalmaznia kell az intézkedés menetét és aktuális állapotát. A HI tájékoztatja a gyengeség vagy fenyegetettség által érintett teljes felhasználói kört a kivizsgálás végeredményéről, esetleges elhárítás módjáról, bekövetkezés okairól, a jövőben alkalmazandó elvárható óvintézkedésekről, valamint a felhasználóktól elvárt feladatokról. Amennyiben az informatikai eset megkívánja, a menedzseléséről az informatikai rendszerek üzemeltetéséért felelős szakemberek, rendszerüzemeltetők gondoskodnak. A feladat elvégzésének módját a HI informatikai BCP-je határozza meg.

5.2 Szoftverzavarok

A szoftverzavarok biztonsági kezelésénél rögzíteni kell azt, hogy melyek azok a kiemelt szoftverzavarok, amelyek esetében a felhasználó köteles minden egyéb tevékenységet azonnal beszüntetni és a hiba elhárításáig nem folytathatja a munkavégzést az érintett számítógépen. A szoftverzavarok típusát tartalmazó dokumentációt az informatikai rendszert üzemeltető szervezeti egység vezetője vagy a HI készíti el és rendszeresen aktualizálja. A tapasztalt szoftverzavarokat az illetékes rendszerüzemeltető hárítja el. A központi rendszereket érintő rendellenes szoftverműködést a HI kezeli.

Felhasználónak nem ajánlott kezelni vagy elhárítani a feltételezett szoftverzavart és a hibás szoftvert vagy állományt eltávolítani. Amennyiben a biztonsági eset megkívánja, a rendszerbiztonsági felelősöknek a szoftverzavar által érintett teljes felhasználói kört tájékoztatniuk kell a biztonsági esemény megszüntetéséről, a kivizsgálás végeredményéről, esetleges elhárítás módjáról, bekövetkezés okairól, a jövőben alkalmazandó elvárható óvintézkedésekről, valamint a felhasználóktól elvárt feladatokról.

A szoftverzavar menedzseléséről az érintett informatikai rendszerek üzemeltetéséért felelős szakemberek (rendszerüzemeltetők) gondoskodnak.

Kiemelt szoftverzavarok

A kiemelt szoftverzavarokat az adott rendszert üzemeltető szervezeti egységvezetője specifikálja.

A kiemelt szoftverzavarok észlelése esetén értesíteni kell a HI munkatársait vagy a rendszerüzemeltetőt. A rendszer üzemeltetője vagy a HI az IHéFB bevonásával

késlekedés nélkül megkezdi az üggyel kapcsolatos kivizsgálást. A HI részére át kell adni a szoftverzavarral kapcsolatos informatikai biztonsági állományok, érintett rendszerek, elektronikus dokumentációk másolatát. A HI részére átadott dokumentumok, informatikai bizonyítékok, biztonsági másolatok központilag megőrzésre kerülnek. A szoftverzavar által érintett számítógépeket le kell kapcsolni az Egyetem hálózatáról és használatát a teljes helyreállításig lehetőleg fel kell függeszteni. A szoftverzavar által érintett számítógépekről tilos az állományok áthelyezése más gépekre. A szoftverzavarról értesítettek kötelesek a tájékoztatás kézhezvételét követően késlekedés nélkül intézkedni.

5.3 Hardverzavarok

Az esetleges hardverzavarok dokumentációját, hardverzavarok elhárítására vonatkozó eljárást az adott informatikai rendszert üzemeltető szervezeti egység dolgozza ki. Az elhárítást a dokumentáció alapján kell lefolytatni.

5.4 Esettanulmányok

A biztonsági események elemzését éves szinten az IHéFB a HI segítségével végzi el. Az elemzéshez az Egyetem összes karának hozzá kell járulnia ahhoz, hogy valósághű elemzés készülhessen. Ezért ajánlott a biztonsági események megfelelő rögzítése az egyetemi *hiba.uni-pannon.hu* honlapon. Az elemzéskor összegzésre kerülnek a biztonsági események okai, a menedzselés folyamatok értékelése, a tanulságok, a szükséges fejlesztések. Elektronikus rögzítés hiányában az Egyetem karainak a HI által meghatározott formátumban kell a tanulmányhoz szükséges adatokat megadni.

VI. Fizikai és környezeti biztonságra vonatkozó ajánlás

1. Általános óvintézkedések és alapelvek

Az Egyetem a biztonságos informatikai infrastruktúra kialakításának érdekében javaslatot tesz a fizikai és a környezet biztonságának kiépítésére, így a biztonságos munkaterületek kialakítására és az egyetemi informatikai eszközök védelmére. Meg kell akadályozni a jogosulatlan fizikai hozzáférést, károsodást és az információáramlás megzavarását.

A kritikus vagy érzékeny egyetemi adatokat feldolgozó informatikai eszközöket javasolt a meghatározott biztonsági területeken elhelyezni. Az Egyetem javaslatot tesz a biztonsági területet és a fizikai hozzáférést szabályozására. Amely szerint

- a kritikus adatokat tároló területet meghatározott biztonsági határzónába kell sorolni és megfelelő biztonsági korlátokkal és belépési ellenőrzéssel kell védeni.
- Az Egyetem tulajdonában lévő informatikai eszközök elveszését, károsodását, ellopását, veszélyeztetését és az Egyetem tevékenységének megszakítását meg kell akadályozni.
- Az egyetemi informatikai infrastruktúrát védeni kell a fizikai és környezeti ártalmaktól.
- Az illetékes szervezet felel a biztonságos informatikai munkakörnyezet kialakításáért és a biztonsági előírások betartásáért.

2. Biztonságos környezet

2.1 Irodák, helyiségek és az informatikai eszközök biztonsága

Az irodák, helyiségek és az informatikai eszközök használatára vonatkozó további biztonsági előírásokat az Egyetem SZMSZ vonatkozó szabályzatai tartalmazzák, különösen a

- Tűzvédelmi Szabályzat,
- Rendészeti és Vagyonvédelmi Szabályzat.

Az Egyetemen használt szerverek közül a fokozott és kiemelt biztonsági osztályba tartozó rendszerek hardvereszközeit megfelelően kell védeni, ezért javasolt azok szerverszobában való elhelyezése.

2.2 A szerverszobák kialakítására vonatkozó ajánlások

a) A padló és a berendezések lehetőleg antisztatikus kivitelezésűek legyenek.

b) Szerverszobák falai nem készülhetnek könnyűszerkezetes technológiával, nem lehetnek üvegből, gipszkartonból vagy más könnyen áttörhető anyagból.

c) Ajtók megerősített kivitelezésűek legyenek, több ponton záródjanak, az ablakok fixen beépítettek, a zárt ablakok betörésvédő fóliázással vagy fém ráccsal és árnyékoló (sötétítő) fóliázással ellátva legyenek. Ablak nélküli helyiségek is megfelelőek.

d) A szerverszobákat klímaberendezéssel kell ellátni és olyan teljesítményűeknek kell lenniük, hogy a szerverszoba maximális teljesítményénél és 35 C° külső hőmérséklet esetén is 20 C° környezeti hőmérséklet biztosítható legyen. A klímaberendezés duplikált vagy redundáns legyen, mert az esetleges meghibásodás esetén maximum 27 C°-ra emelkedhet a szerverszoba hőmérséklete. A relatív páratartalomnak szabályozhatónak kell lennie (50-80% között). Klímaberendezéseket porszűrővel kell ellátni és enyhe túlnyomást kell létrehozni a helyiségben a nagy értékű berendezések porszennyeződésének elkerülésére. A klímaberendezésnek az automata tűzoltó rendszerrel összhangban kell működnie.

e) A szerverszobákat el kell látni automatikus tűzérzékelő, riasztó és oltó berendezéssel, a riasztójelzésnek a biztonsági szolgálathoz kell befutnia. A szerverszobákba megfelelő számú mozgás- és nyitásérzékelőket kell felszerelni.

f) Álpadló esetén: az álpadlóban megfelelő számú nedvességérzékelőt kell elhelyezni. Az érzékelőknek az épület vagy a telephely biztonsági rendszerébe kell becsatlakozniuk.

g) Önálló riasztó- és beléptető rendszert kell kiépíteni, hogy a helyiségbe belépőket utólag is bármikor azonosítani lehessen. A szerverszoba biztonsági rendszerének az épület meglevő rendszerével összhangban kell működnie.

h) Az elektromos hálózat legalább a szerver és a szükségvilágítás vonatkozásában 30 perces áthidalási idejű megszakításmentes átkapcsolással rendelkező szünetmentes tápegységgel legyen ellátva. A tápegység akkumulátorai a maximális igénybevételt követő töltés hatására teljes kapacitásukat 24 órán belül nyerjék vissza. Szerverszobákban a szünetmentes tápláláson kívül szükséges kiépíteni nem szünetmenetes energia elérési lehetőséget is (pl. külső generátor).

i) Szerverszobák elhelyezkedésére utaló jelzéseket az Egyetem épületeiben nem szabad elhelyezni.

j) A szerverszoba ajtaja munkaidőn kívül vagy ha nem tartózkodik egyetlen ott dolgozó munkatárs sem ne maradjon nyitható állapotban.

k) A szerverszobákba a belépés szigorúan szabályozott, a mozgásokat a szerverszoba naplóban kell rögzíteni. Meg kell határozni és a bejáratnál ki kell akasztani a belépésre jogosultak névsorát. A listán nem szereplő személyek csak felügyelet mellett léphetnek be a helyiségbe. Idegenek a szerverszobákban kizárólag a rendszerüzemeltető szervezeti egység engedélyével, felügyelet mellett tartózkodhatnak. A szerverszobákban tartózkodni kizárólag indokolt esetben (más helyszínen el nem végezhető munkavégzés esetén) szabad.

l) Szerverszobába ételt, italt bevinni, étkezni vagy ott dohányozni tilos. Nyílt láng vagy egyéb nagyteljesítményű hőforrás használata ugyancsak tilos.

m) A szerverszobákban nem tárolhatók idegen berendezések, alkatrészek és anyagok különösen dokumentációk, festékpatronok, összerakásra váró számítógépek.

n) A szerverszobák takarításának, épület-karbantartásnak valamint az esetlegesen felmerülő rovar, és rágcsálóirtásnak felügyelet mellett kell megtörténnie. A takarítás során a géptermekben elhelyezett berendezésekbe nedvesség nem juthat. A takarításhoz a szünetmentes áramforrásokat nem szabad használni.

o) Rendszeresen biztosítani kell a szerverszobában elhelyezett berendezések (szerverek, hálózati eszközök) tisztítását, pormentesítését, illetve a gyártó által előírt tervszerű karbantartást.

p) A szerverszobában fénykép, videó- vagy más felvétel készítése tilos, kivéve, ha az a szerverekhez kapcsolódó munkavégzéshez szükséges vagy a biztonságtechnikai intézkedés előírja.

q) A központi, kiemelt szerverszobáknak redundáns betáplálással kell rendelkezniük, tápáramellátását szünetmentes áramforrásokon keresztül kell biztosítani.

r) Az áram– és vízszolgáltatás, csatornázás fűtés és légkondícionálást a szerverszobában üzemeltetett informatikai rendszerek követelményéhez kell igazítani, figyelembe véve az SZMSZ erre vonatkozó előírásait. Vízbetáplálást kell biztosítani a légkondicionáló berendezéshez úgy, hogy a vízbetáplálás rendszere és a légkondicionáló berendezés meghibásodása esetén a szerverszobában elhelyezett informatikai eszközöket ne károsítsa. Vizesblokkot sem a szerverszobában sem pedig a szomszédos (felette és mellette) helyiségben nem lehet kialakítani, a meglévőt meg kell szüntetni. Csatorna vagy gázvezeték a szerverszobában vagy a szerverszoba falában nem húzódhat.

s) További javaslat: a szerverszobára vonatkozó eljárás szervezeti egység szintű kidolgozása, gondozása és betartása.

2.3 Munkavégzés és tanulás biztonságos környezetben

Az egyetemi polgárok munkavégzésének és tanulásának biztonságos informatikai környezetét biztosítani kell. A HI feladata, hogy a főbb, központi informatikai területekről, különösen információs szolgáltatásokról, számítógépes laborokról, szerverszobákról és szervizszobákról környezeti helyzetfelmérést és ergonómiai dokumentációt készítsen és azt aktualizálja. A HI-n kívüli egyetemi szervezetek által felügyelt informatikai rendszerek esetében ezt a feladatot az illetékes szervezeti egység végzi el.

3. Informatikai eszközök biztonsága

Az informatikai berendezéseket fizikailag védeni kell a biztonsági fenyegetésektől és a környezeti veszélyektől. A megfelelően kialakított védelemmel (VII. fejezet) csökkenthető különösen az illetéktelen adathozzáférés, az adatvesztés és adatsérülés kockázata. Kiépítés és felújítás során a kivitelezőnek vagy rendszerüzemeltetőnek figyelembe kell venni a berendezések elhelyezését és a velük kapcsolatos rendelkezést (VI/2. /2.1, 3.1-3.4). Különleges óvintézkedésekhez hozzá tartozik a támogató eszközök, különösen a villamosenergia-ellátás vagy a kábelezési infrastruktúra eszközeinek megóvása.

3.1 Az informatikai berendezések védelmének irányelvei

a) Az informatikai berendezéseket úgy kell elhelyezni, hogy a szükségtelen hozzáférés a munkaterülethez a legkisebb legyen.

b) Az érzékeny adatokat kezelő, tároló, megjelenítő informatikai eszközöket, különösen a perifériákat úgy kell elhelyezni, hogy használatuk alatt a jogosulatlan személyek az érzékeny információkat ne láthassák és azokhoz hozzá ne férhessenek.

c) Kockázatelemzéssel, katasztrófa-elhárítási és cselekvési (akció) terv segítségével a lehető legkisebbre kell szorítani a lehetséges fizikai fenyegetések kockázatát, különösen a lopás, a tűz, a robbanás, a víz vagy a vízszolgáltatás meghibásodás esetére, a por, a vegyi hatások által okozott zavarra, villamos szolgáltatás zavarára, a kommunikációs zavarra, a elektromágneses sugárzás és értelmetlen rombolás okozta zavarra vonatkozóan.

d) Az informatikai rendszerek közelében tilos az étkezés, az ivás és a dohányzás.

e) Az informatikai berendezéseket óvni kell a negatív környezeti hatásoktól, különösen a hőmérséklet és légnedvesség által okozott meghibásodásoktól. Érzékeny információkat tároló, kezelő informatikai eszközöket csatlakoztatott szünetmentes tápegységgel kell ellátni. Az ilyen informatikai eszközök helységében légkondicionálót kell elhelyezni és üzemeltetni.

3.2 Tápáram-ellátás

a) A kritikus és kiemelt informatikai rendszerek tápáramellátását szünetmentes áramforrásokon keresztül kell biztosítani.

b) Megfelelő szoftverek telepítésével biztosítani kell a külső áramforrások és a gépek közötti biztonságos kommunikációs kapcsolatot.

c) A szünetmentes és a tartalék áramforrások karbantartását és tesztelését rendszeresen el kell végezni, a feladat elvégzését naplózni kell (*hiba.uni-pannon.hu* honlapon). A tartalék áramforrás működtetését folyamatosan biztosítani kell.

3.3 Kábelezés

a) Az energetikai és informatikai kábelezést úgy kell kialakítani, hogy a mechanikai sérülésektől és az elektromágneses zavaroktól megfelelőképen védettek legyenek. A zavarok hatásának minimalizálása érdekében az erősáramú és az informatikai kábeleket elkülönítetten kell vezetni, az optikai kábelek kivételével.

b) El kell kerülni az illetéktelen rácsatlakozást, ennek érdekében a kábelezés végpontjait és a rácsatlakozást lehetővé tevő pontokat zárható helyiségben vagy illetéktelennek hozzá nem férhető helyen, zárható rendezőszekrényben kell elhelyezni.

c) A kritikus rendszerek kábelezését lehetőség szerint redundáns módon kell kialakítani. Ebben az esetben a kábelezéseket elkülönült nyomvonalon kell

bevezetni, különösen az áramellátást más rendszerektől elkülönült áramkörökről kell megoldani.

d) A villamos kapcsolószekrényekben a fenti áramkörökhöz tartozó kismegszakítókat, biztosítókat egyértelműen kell megjelölni. Ezeket védeni kell a véletlen kikapcsolás ellen (pl.: zárható szekrény).

3.4 Karbantartás

Az informatikai berendezéseket és eszközöket a gyártójuk által megadott eljárásnak és időszaknak megfelelően kell karbantartani. A karbantartást és javítást csak az arra feljogosított személy végezheti el. A feltételezett vagy a tényleges meghibásodásokról és a karbantartásokról feljegyzést kell készíteni. A hibajegyet rögzíteni kell a *hiba.uni-pannon.hu* egyetemi honlapon az ISZ vonatkozó fejezetének előírása szerint.

VII. Informatikai rendszerek biztonsága

Az üzemeltető egyetemi szervezetegységnek az egyetemi informatikai rendszerek biztonságának kialakításakor helyzetfelmérést, védelmi lehetőségvizsgálatot javasolt készíteni, amely alapján az aktuális és az elvárt védelmi szint meghatározató, a magasabb védelmi szint előirányozható és kivitelezhető. Az egyetemi informatikai rendszereket üzemeltető, illetékes informatikai szervezeti egységnek a feladata az ISZ alapján az informatikai védelmi rendszer kiépítése és dokumentálása, amelyet elősegít a szervezeti egység szintű Üzemeltetői eljárás kidolgozása és életbelépése. Az egyetemi központi informatikai védelmi rendszer előírásait a HI dolgozza ki, különösen a hozzáférésre, behatolás elleni védelmére, mentésre, helyreállításra és vírusvédelemre. Az egyetemi szervezetek hálózati, védelmi rendszereit szinkronizálni kell a gerinchálózat védelmi rendszerével. A HI vezetőjének és az üzemeltető szervezeti egységvezetőnek a felelőssége a megfelelő szinkronizálás végrehajtása.

VIII. Az egyetemi üzletmenet biztonsági kérdései

1. Üzletmenet szempontjából kritikus adatok

Az egyetemi üzletmenet szempontjából kategorizálása javasolt, amelybe az Egyetem informatikai rendszereiben nyilvántartott adatai besorolhatóak. Az így nyilvántartott adatok kezeléséről és védelméről informatikai adatvédelmi és adatbiztonsági szabályozást ajánlott készíteni, amelyben rögzíteni lehet különösen az informatikai adatok érzékenysége alapján kialakított kategóriákat, azok kezelését és a védelmi szinteket. A szabályozásban kiemelendő a kritikus rendszerekben nyilvántartott valamint a kritikus adatok kezelése.

2. Üzletmenet (működés) folytonosság

2.1 Az egyetemi működésfolytonosság

Az egyetemi működésfolytonosság biztosításának célja az egyetemi működési tevékenységek megszakításának megelőzése és elhárítása, különösen a kritikus működési folyamatok védelme és az egyetemi működésfolytonosság informatikai támogatása, a szükséges informatikai rendszerek folyamatos biztosítása. Az egyetemi működésfolytonosság biztosítására működésfolytonossági irányítási folyamatot lehet bevezetni, aminek a részeként javasolt az informatikai működésfolytonosság kialakítása.

A cél tehát, hogy a lehető legkisebbre lehessen csökkenteni az intézményre gyakorolt káros események hatását. A folyamatok definiálásával a megelőző és a helyreállító intézkedések kombinálásával elhárítható legyen az egyetemi információs vagyontárgyak elvesztése különösen természeti katasztrófa, baleset, berendezések meghibásodása és szándékos beavatkozás esetén.

Az általános működésfolytonosság dokumentáció (továbbiakban egyetemi BCP) kialakításának szempontjai:

a) Javasolt az egyetemi szervezeteknek azonosítani és specifikálni az informatikai folyamatokat különösen a kritikus működési folyamatokat. Ehhez kapcsolódik az eseménykezelési dokumentáció.
b) Fenyegető tényező felmérése, amelyek az Egyetem működési folyamatainak tekintetében mérvadónak tekinthetők. A kockázat-felmérési dokumentációban lehet szerepeltetni a fenyegető tényezők előfordulási valószínűségét.
c) Rögzíthető, hogy a fenyegető tényezők bekövetkezésekor milyen kárkövetkezményekre lehet számítani.
d) Működési hatáselemzésnek kell alávetni különösen az üzemzavarok, a biztonsági meghibásodások, a szolgáltatás elvesztés és a szolgáltatás rendelkezésre-állás követelményeit.
e) Kiesések bekövetkezésekor milyen időtartam alatt valósulhat meg a folyamat helyreállítása.
f) Az olyan bekövetkezett vagy lehetséges váratlan eseményeket vizsgálata, amelyek az Egyetem folyamatos működését veszélyeztetik. Megoldások kidolgozása.

2.2 Az informatikai működésfolytonosság

Az informatikai működésfolytonosságnak igazodnia kell az egyetemi működésfolytonossághoz. A központi informatikai üzletmenet vagy működés folytonossági tervet (informatikai BCP) a HI dolgozza ki és az alábbiakat tartalmazza:

a) Központi informatikai rendszerek működési folyamatainak dokumentálása.
b) Helyzetelemzés.
c) Krízis-vészhelyzeti eljárás vagy katasztrófa-elhárítási terv.
   A katasztrófaterv magába foglalja:
   - a támogató szolgáltatók, a közhivatali kapcsolatok jegyzékét,
   - az érintett erőforrások felmérését,
   - a tárgyi feltételek vizsgálatát,
   - optimalizálást, különösen a káresetek bekövetkezésének valószínűségét,
   - a katasztrófa bekövetkezése esetén a helyettesítő megoldásokra való áttérés eljárásait, a cselekvési (akció) tervet,
   - az újrakezdés vagy a folytatás eljárásait,
   - a tesztelési és a felülvizsgálati rendet.
d) Tudatosítás és az oktatás megvalósítását.
e) Az egyéni és az érintettek felelősségét.
f) A BCP tulajdonosának megjelölését.

Az egyetemi kritikus informatikai rendszerek esetében javasolt a BCP kidolgozása, amely az informatikai rendszert üzemeltető szervezeti egység feladata.

IX. Záró rendelkezések

1. Érvényesség

1.1 Az ITB személyi hatálya

Jelen Ajánlás kiterjed minden Egyetemi Polgárra.

1.2 Az ITB tárgyi hatálya

Jelen ITB tárgyi hatálya kiterjed az Egyetem minden használatban lévő informatikai eszközére, vagyontárgyára és az ezekben a rendszerekben tárolt adatokra, információkra, különös tekintettel:

a) összes szoftverre, adatbázisra,
b) összes hardverre,
c) informatikai rendszerekhez kapcsolódó infrastrukturális elemekre, hálózati eszközökre,
d) informatikai rendszerekben rögzített, nyilvántartott illetve továbbított elektronikus vagy papír alapú adatokra, dokumentumokra.

2. Az ITB felülvizsgálata

a) Áttekintés és esetleges módosítás kétévente egy alkalommal, az ajánlás lezárásakor meghatározott időpontban vagy
b) minden olyan esetben, amikor az ajánlásban leírtakban vagy az ajánlást is érintő szervezeti egység struktúrában és működésben jelentős változás(ok) vagy nagyobb fejlesztések történnek.

3. A Pannon Egyetem biztonsági besorolása

A Pannon Egyetem alapbiztonsági fokozatba tartozik.

4. Az ITB jóváhagyása

A jelen ajánlást az Egyetem Szenátusa 2012. május 31-i ülésén megtárgyalta és a 230/2011-2012. (V. 31.) Szenátus sz. határozatával elfogadta. Az ajánlás (ITB) 2012. június 15-én lép hatályba, egyidejűleg a 2010. december 8-án Rektori Tanács által megtárgyalt és elfogadott Pannon Egyetem Informatikai Biztonsági Ajánlása hatályát veszti.

Veszprém, 2012. május 31.

Dr. Friedler Ferenc sk.
rektor