PÁZMÁNY PÉTER
KATOLIKUS EGYETEM

Pázmány Péter Katolikus Egyetem Információbiztonsági Szabályzata (tervezet)

2018.

Tartalom

1. A SZABÁLYZAT CÉLJA

Az információbiztonsági szabályzat célja mindazon intézkedések és betartandó szabályok összefoglalása, melyek által a PPKE információbiztonsága (rendszerek adatok és információk rendelkezésre állása, sértetlensége és bizalmassága) fenntartható legyen.

2. HATÁLYA, ÉRVÉNYESSÉGE, MÓDOSÍTÁSA, FELÜLVIZSGÁLATA

Jelen szabályzat mindenkire nézve kötelező, aki használja a PPKE számítógép-hálózatát, annak berendezéseit (későbbiekben felhasználók). Az előbbieknek megfelelően a szabályzat személyi hatálya kiterjed a PPKE összes hallgatójára és dolgozójára, aki oktatási, kutatási, tudományos vagy az intézmény adminisztrációs feladataihoz a PPKE számítógép-hálózatát és eszközeit használja. Ha az intézmény harmadik félnek is lehetőséget biztosít hálózatának használatára, akkor harmadik félre nézve is kötelező a szabályzatban foglaltakat betartani.

A szabályzat alapszerkezete követi az ISO 27001:2013 szabvány „A" mellékletének („Szabályozási célok és kontrollok") szerkezetét. Ennek célja, hogy a PPKE hatékony és nemzetközi szabványon alapuló információbiztonsági irányítási rendszert alapozzon meg.

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

Jelen szabályzat a PPKE Egyetemi Tanács (továbbiakban ET) által történő elfogadásával lép hatályba. Mindaddig hatályos, amíg új verziót nem fogad el az ET vagy visszavonásra nem kerül. Jelen szabályzatot az ET módosíthatja.

A szabályzat mellékleteit, kapcsolódó dokumentumait, amennyiben más szabályozás nem érvényes a dokumentum változtatására vonatkozóan, az IT osztályvezetője (továbbiakban ITO) módosíthatja a Rektor hozzájárulásával.

Jelen szabályzat felülvizsgálatára az ITO irányításával évente egyszer kötelező jelleggel sor kerül.

3. KAPCSOLÓDÓ SZABÁLYZATOK, DOKUMENTUMOK

- PPKE Szervezeti és Működési Szabályzata (PPKE SZMSZ);
- PPKE IT Szervezeti és Működési Szabályzata (PPKE IT SZMSZ);
- PPKE Informatikai Szabályzata (PPKE IT-SZ);
- PPKE Informatikai Felhasználói Szabályzata (PPKE ITF-SZ);
- PPKE Adatvédelmi és Adatbiztonsági Szabályzata (PPKE AASZ);
- PPKE Információátadási Szabályzat (PPKE IASZ);
- PPKE IT munkaköri leírásai;
- Rektori Utasítás „A Pázmány Péter Katolikus Egyetem Központi Informatikai Szolgáltatási Csoport létrehozásáról" (Ikt. Szám: R-31/9/2009);
- A Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzata (20/2004. (VI.21.) IHM rendelet).
- PPKE alkalmazások (például Neptun, SAP, Nexon, ECM) üzemeltetési/felhasználói dokumentációi, gyártói licence és szolgáltatói megállapodások (például MS Campus szerződés), valamint az IT üzemeltetés-szabályozási utasításai (például IT folyamat szabályozások, jogosultság kezelés, DRP, mentési rend).
- Szolgáltatási szint vállalások (SLA – Service Level Agreement)
- PPKE IT stratégia

A kapcsolódó szabályzatok és dokumentumok az IT honlapján kerülnek elhelyezésre, PPKE munkatársak, hallgatók, IT munkatársak és bárki számára megtekinthető bontásban, amelyek megtekintése a vonatkozó jogosultság függvényében lehetséges.

4. ÁLTALÁNOS RENDELKEZÉSEK

4.1. A PPKE információbiztonsági felelőse

A PPKE információbiztonsági felelőse (továbbiakban IBF) az ITO.

Az IBF feladatait a PPKE IT SZMSZ határozza meg.

Az IBF (ITO) együttműködik a PPKE Adatvédelmi felelősével (DPO).

4.2. Feladat-, felelősség- és hatáskörök az információbiztonság területén

Az adatvédelmi incidensek esetében a DPO jár el az adatvédelmi incidenskezelési eljárás szerint.

Informatikai biztonsági incidensek esetében az ITO jár el az ebben a szabályzatban meghatározottak szerint.

4.3. Jogszabályi, törvényességi megfelelőség

Az információbiztonság területén megjelenő és érvényes jogszabályok betartásért és betartatásáért az IBF a felelős.

Adatszolgáltatást hatóságoknak (pl. NAIH megkeresések) a DPO teljesít.

Törvényes megkeresés alapján, a vonatkozó jogszabályi kereteknek megfelelve a PPKE minden, a bűncselekmény elkövetésének gyanúja alá eső felhasználó adatait, valamint naplózott adatokat a nyomozóhatóságnak kiszolgáltatja.

5. A PPKE INFORMÁCIÓBIZTONSÁGI POLITIKÁJA

A PPKE információbiztonsági politikájának célja, hogy a PPKE szervezeti egységei részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása és funkcionalitása biztosítása érdekében követendő irányelvekre.

Az irányelvek figyelembe vételével meghatározható az informatikai biztonsági szabályozás alapján minősített adatokat (pl. személyes adatok) kezelő informatikai rendszerek biztonsági osztályba sorolása; kidolgozhatók a konkrét, rendszer szintű informatikai biztonsági szabályozások, amelyek az informatikai rendszer teljes életciklusában meghatározzák a szabványos biztonsági funkciók tervezéséhez, megvalósításához, üzemeltetéséhez és megszüntetéséhez a szükséges alapelveket és követelményeket.

5.1. Információbiztonsági alapelvek

A PPKE szervezeti egységei által kezelt adatok védelmét bizalmasság, hitelesség, 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, a következők szerint:

1. A teljes körűségre vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén kell érvényesíteni úgymint:
    - az összes információbiztonsági rendszerelemre,
    - az informatikai rendszer infrastrukturális környezetére,
    - a hardver rendszerre,
    - az alap- és felhasználói szoftver rendszerre,
    - a kommunikációs és hálózati rendszerre,
    - az adathordozókra,
    - a dokumentumokra és feljegyzésekre,
    - a belső személyzetre és a külső partnerekre,

- az MSZ OSI 7498-1. szabványban meghatározott nyílt rendszerek architektúrája minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az informatikai alkalmazások szintjén,
- mind a központi, mind a végponti informatikai eszközökre és környezetükre.

2. A védelem zártsága akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni védelmi intézkedés megvalósul.
3. A védelem akkor kockázatarányos, ha az informatikai rendszerek által kezelt adatok védelmének erőssége és költségei a felmért kockázatokkal arányban állnak. Célkitűzés a minimális védelmi költséggel elért maximális védelmi képesség.
4. A védelem folytonossága úgy biztosítható, hogy az informatikai rendszerek fejlesztése és megvalósítása során kialakított védelmi képességeket a rendszerből történő kivonásig folytonosan biztosítani kell a rendszeres ellenőrzéssel és az ezt követő védelmi intézkedésekkel.
5. A zárt szabályozási ciklus úgy érvényesíthető, hogy az adminisztratív védelemmel biztosítani kell a szabályozás, érvényesítés, ellenőrzés és a védelmi intézkedések/szankcionálás zárt folyamatát.

További céljaink és elveink:

Igyekszünk a kockázatainkat minimalizálni, de minden vezetőben és munkatársban tudatosítjuk, hogy teljes körű védelem és biztonság nincsen, és ezzel összefüggésben a maradvány kockázatokat tudatosan vállaljuk.

A felelősségeket az információbiztonság területén hangsúlyozottan elhatároljuk és az egyes szervezeti szerepkörökhöz kötjük.

Hangsúlyozottan törekszünk a törvényi és jogszabályi megfelelőségre különös tekintettel a személyes adatok kiemelt védelmére (pl. GDPR előírások).

Megpróbáljuk kiegyensúlyozottan kezelni a mobilitás lehetősége és a biztonság közötti ellentmondást.

Elsődleges célunk a működőképesség fenntartása, ezért az olyan felhasználókat, akik magatartásukkal más felhasználók tömegeinek munkáját veszélyezteti, haladéktalanul kizárunk a szolgáltatásból mindaddig, amíg a veszélyt okozó tevékenységét nem szünteti meg.

A védelem mellett, de nem a biztonság rovására, biztosítjuk az oktatási és kutatási tevékenységhez szükséges szabad információáramlást.

A felhasználói jogosultságok természetes személyhez kötöttek és nem átruházhatók. Az információbiztonsági incidensek esetében a felelősség a jogosultsággal bíró személyhez kötődik. Rosszhiszemű felhasználásnak tekintjük, ha a felhasználó jogosultságát meghaladó műveleteket szándékosan kezdeményez, illetve jogosultságát megkísérli módosítani.

Elérendő cél, hogy a szolgáltató rendszerek üzemzavarait ne a felhasználók, hanem automatikus szolgáltatásmegfigyelő komponensek jelezzék.

5.2. Az információbiztonsági politika elfogadása és közzététele

Az információbiztonsági politikát az IBSZ részeként kezeljük, ezért elfogadása és közzététele az IBSZ-szel megegyező módon történik, azaz az Információbiztonsági politikát az IBSZ részeként az ITO előterjesztése alapján a PPKE Egyetemi Tanácsa fogadja el. Az Információbiztonsági Politika az IBSZ aktuális verziójának részeként az IT honlapján megtekinthető.

5.3. Az információbiztonsági politika rendszeres felülvizsgálata

Az információbiztonsági politika az IBSZ szerves része, és az IT-SZ-szel egy időben és azonos módon történik a felülvizsgálata:

- évente egy alkalommal (az esedékes következő felülvizsgálati időpontot a dokumentum lezárásakor kell kijelölni.)
- minden olyan esetben, amikor a politikában leírtakban jelentős változás(ok) történnek.

6. AZ INFORMÁCIÓBIZTONSÁG SZERVEZETI KÉRDÉSEI

Az információbiztonsággal kapcsolatos szervezeti kérdéseket az alábbiakban szabályozzuk:

Az információbiztonság belső szervezete

Az információbiztonsággal kapcsolatos felelősség megoszlik az IT, az egyes szervezetek és a felhasználók között. A felelősség-megosztás elveit az alábbiakban tárgyaljuk.

6.1.1. Vezetői elkötelezettség

Minden szervezeti egység vezetője személyesen felel az információbiztonság kultúrájának fenntartásáért.

A vezetők elkötelezettségüket személyes példamutatással (szabályozások betartása) és személyes felelősségvállalással demonstrálják.

A belső és külső szolgáltatói megállapodások (SLA-k) figyelése, figyelembe vétele és a bennük megfogalmazott paraméterek mérése a vezetői elkötelezettség kinyilvánítása. Az információbiztonsági intézkedések megvalósításához szükséges erőforrások biztosítása szintén a vezetői elkötelezettséggel összhangban zajlik.

Az intézmény informatikai rendszereinek IBSZ-nek való megfelelősége az ITO hatásköre.

6.1.2. Információbiztonsági koordináció (érintett felekkel egyeztetés)

Az informatikai rendszerek IBSZ megfelelőségi vizsgálatát, illetőleg az ezzel kapcsolatos tanácsadást az IT szolgáltatásmenedzsere végzi (a külső audit igények kivételével). Az IBSZ

megfelelőségi vizsgálatot az ITO vagy a rendszert üzemeltető szervezeti egység vezetője (üzemeltető osztály vezetője) kezdeményezheti.

A PPKE információbiztonsági vezetője az ITO, és ebben a minőségében az osztályértekezletek a döntések fórumai az egyes információbiztonsági védelmi intézkedésekkel kapcsolatban.

6.1.3. Az információbiztonsági felelősségek allokációja

Azon informatikai rendszerek esetében, amelyeknek nem volt sikeres az IBSZ megfelelőségi vizsgálata, minden negatív biztonsági esemény felelőssége az üzemeltető szervezeti egység vezetőjét terheli.

Azon rendszerek esetében, ahol az IBSZ vizsgálat sikeres volt (illetőleg a vizsgálat során készült és elfogadott hiánylistát az üzemeltető pótolta) a negatív biztonsági események felelőssége egyedi vizsgálat alapján állapítható meg. Az IBSZ (és annak a rendszerre vonatkozó mellékleteinek) betartása esetén az üzemeltető jóhiszeműnek minősül.

Az IT szolgáltatásmenedzserének felelőssége az információbiztonsági események, incidensek tanulságait és a pozitív példák megjelenítése az IT szokásos információs csatornáin.

6.1.4. Új információ-feldolgozó rendszerek elfogadási eljárása

Új informatikai szolgáltatás indítási kérelemhez az IT-SZ szerint csatolni kell a rendszer vázlatos leírását és a tervezett SLA-t. Ezen anyagok alapján az ITO a szolgáltatás engedélyezése előtt javaslatot kérhet a szolgáltatásmenedzsertől az IBSZ mellékletek aktualizálására, az új szolgáltatás IBSZ paramétereinek megállapítására. A szolgáltatás indítási kérelem automatikusan az IT-SZ és az IBSZ elfogadási szándéknyilatkozatának tekintendő.

6.1.5. Bizalmassági nyilatkozatok

Az információbiztonsági szabályok betartásával és betartatásával kapcsolatban az 1. számú mellékletben részletezett bizalmassági nyilatkozatot írnak alá az „A” és „B” osztályú rendszerek (lásd Informatikai Szabályzatban) üzemeltetői, illetve abban az esetben a felhasználók is, amennyiben erről az adott rendszer SLA-ja erről külön rendelkezik. Ugyanezt teszik a PPKE üzleti partnerei is a 2. számú mellékletben részletezett titoktartási nyilatkozat kitöltésével és aláírásával.

A rendszer üzemeltetői a rendszer üzemeltetése során különféle személyes, illetőleg bizalmas adatokhoz férnek hozzá. Ezen adatok védelméről gondoskodni kell.

A munkavégzés során a munkavégzők részére átadott, illetve tudomásukra jutott információkat védeni kell.

Minden bizalmassági kérdésben érintett szereplővel bizalmassági nyilatkozatot kell kitölteni, melynek aláírásával felvállalja, hogy a birtokában levő információval nem él vissza.

6.1.6. Kapcsolattartás hatóságokkal

A különböző törvényekben és rendeletekben előírt információbiztonsági adatszolgáltatási kötelezettség teljesítése az ITO felelőssége. A PPKE illetve az IT jogi képviseletet nem lát el az egyének jogvitáiban a hatóságokkal.

6.1.7. Kapcsolattartás különleges érdekközösségekkel, szakmai szervezetekkel

Az ITO felelős a kapcsolattartásért a különleges érdekközösségekkel (pl. ISACA Budapest Chapter, Hétpecsét Információbiztonsági Egyesület, más Egyetemek IT szervezetei, IT képzést végző középiskolák, egyéb szakmai képző- és vizsgahelyek stb.). Minden ilyen hivatalos IT jellegű tagsági és kapcsolattartási kérdésben a PPKE érdekeinek figyelembe vételével az ITO dönt.

A felhasználók egyéni tagságai (pl. ISACA, IVSZ stb.) az adott személy felelőssége. Egyéni tagként is köteles a kapcsolattartás során a PPKE érdekeit képviselni és az IBSZ vonatkoztatható előírásait betartani.

7. EMBERI ERŐFORRÁSSAL KAPCSOLATOS BIZTONSÁGI KÉRDÉSEK

Az emberi erőforrásokkal kapcsolatos elvárásokat a munkaviszony vagy hallgatói jogviszony vagy szerződéses viszony szakaszai szerint tárgyaljuk.

IT szolgáltatások igénybevétele előtti feladatok

Az informatikai rendszereket és eszközöket használó munkavállalók belépés előtti előzetes biztonsági megfelelési vizsgálatát a Humánerőforrás Gazdálkodási osztály végzi a saját eljárásrendje alapján. Ilyen jellegű vizsgálatot az IT már nem végez az informatikai jogosultságok és hozzáférések megadása előtt.

A titoktartással és a biztonsági intézkedések betartásával kapcsolatban a munkaszerződések rendelkeznek.

A hallgatói jogviszony létesítése előtt biztonsági megfelelőség vizsgálat nem történik, de a képzési szerződés aláírásával és a beiratkozással a hallgatók tudomásul veszik a vonatkozó szabályok betartási kötelezettségét.

A vendégekkel és a szerződéses viszonyban álló személyekkel és vállalkozásokkal kapcsolatos információbiztonsági kockázatokat a vendéglátó köteles mérlegelni mielőtt az érintettek jogosultságait és hozzáférési szintjét az IT-hez eljuttatná kérelmében. Az érintettektől szükséges írásos nyilatkozatok (pl. titoktartási nyilatkozat, stb.) beszerzése a vendéglátó feladata.

7.2. Tennivalók az alkalmazás (munkaviszony), a tanulmányok folytatása és a munkavégzés során

Minden munkatárs a belépési folyamat részeként tájékoztatást kap arról, hogy hol találja meg az információbiztonsággal kapcsolatos egyetemi szabályozásokat. A munkaszerződés részeként a munkavállaló nyilatkozik ezen szabályok tudomásul vételéről.

Hozzáférés, jogosultság csak a jogviszonyban meghatározott feladat elvégzéséhez szükséges és elégséges mértékben igényelhető, adható.

A hallgatók a hallgatói jogviszony létesítése során a képzési szerződés aláírásával elismerik ezen szabályzatok megismerését és betartását.

A vendég jogosultságot kapó személy esetében a vendégjogosultság igénylője felel a vendég informatikai rendszerek használatával kapcsolatos megfelelő szintű tájékoztatásáért.

Az ITO / DPO alkalomszerűen tájékoztatja az érintetteket a jogszabályi változásokról, illetve az információbiztonság tudatossági ismeretekről és elvárásokról.

Az ITO előírhatja szakmai minősítés, vizsga teljesítését valamely informatikai rendszer használatának előfeltételeként.

A szabályok megsértőivel szemben az Egyetem kezdeményezhet fegyelmi eljárást vagy polgári peres eljárást.

7.3. A munkaviszony megszüntetése, a tanulmányok befejezése és a szerződéses kapcsolat megszűnése és/vagy megváltoztatása esetén elvégzendő feladatok

A munkaviszony megszüntetésekor vagy a tanulmányok befejezésekor vagy a szerződéses kapcsolat megszűnése és/vagy megváltoztatása esetén az IT köteles megvonni a jogosultságokat és hozzáféréseket a HEGO értesítése és a munkahelyi vezető igénylése alapján (kilépő lap). A munkahelyi vezető kérheti a kilépő személy által kezelt intézményi adatok mentését, postafiókjának archiválását, és az ezekhez szükséges hozzáféréseket.

Hallgatók esetében a jogszabályokban előírtakon túl nem archiválja az adatokat az IT.

Szerződéses partnerek és vendégek (pl. vendégoktatók) esetében a vendéglátó vagy szerződéses PPKE kapcsolattartó igénylése alapján jár el az IT az archiválási és jogosultsági igények ügyében. A kilépő lapon vagy más dokumentált módon nem igényelt adatok archiválásáért, illetve indokolatlanul fennmaradó jogosultságokért a vendéglátó vagy a szerződéses PPKE kapcsolattartó a felelős.

A jogosultság kiadását kezdeményező annak megvonását kezdeményezheti rendkívüli eljárás keretében is, adott határidővel vagy azonnali hatállyal, telefonon és párhuzamosan dokumentált formában (ITSM rendszer bejelentés, e-mail, levél, SMS) az ITO-tól. A szolgáltatáshoz tartozó SLA tartalmazza az IT által vállalt határidőt a jogosultság megszüntetésére.

Amennyiben a jogosultság, hozzáférés tulajdonosa a jogosultságok és hozzáférések mennyiségében, minőségében eltérést tapasztal a neki célszerűen meghatározotthoz képest, vagy bármely gyanús eseményt tapasztal, azt haladéktalanuk jelenteni köteles a munkahelyi vezetője számára, aki köteles indokolt esetben az IT-hoz fordulni a problémával.

8. AZ INFORMÁCIÓVAGYON MENEDZSMENTJE

A PPKE információvagyonának védelmében az alábbi intézkedéseket, szabályokat hozza:

8.1. A vagyonelemekért viselt felelősség

A PPKE információvagyona kiterjed minden PPKE érdekkörébe tartozó, informatikai eszközön tárolt adatra, alkalmazásra, kódra, azok rendelkezésre állásához, használatához kapcsolódó dokumentációra, tudásra. Az információvagyon fenntartásához és használatához szükséges tudásanyag dokumentálása kötelező minden érintett részére.

A fentiekben meghatározott információvagyon a PPKE tulajdona. Kivételt képez az olyan eset, ahol a vonatkozó szerződés másként rendelkezik (pl. a kód nem a PPKE tulajdonát képezi).

Az információvagyon megőrzése, rendeltetésszerű használata minden PPKE alkalmazott, hallgató és PPKE-vel szerződésben álló fél kötelessége.

A DPO biztosítja az információvagyon kezeléséhez szükséges eljárásrendi feltételeket, az ITO pedig köteles biztosítani az információvagyon kezeléséhez szükséges technikai feltételeket. A DPO köteles vizsgálni és jelezni az információvagyon biztonsági kockázatait.

Az előírásokat minden felhasználó és üzemeltető köteles maradéktalanul betartani, kivétel saját felelősségre sem képezhető.

A PPKE tulajdonában álló információvagyon alkalmas formában való maradéktalan visszaszolgáltatása kötelessége minden azt kezelő, használó felhasználónak, üzemeltetőnek, vagy szerződött félnek, amennyiben azt a feladata tovább nem indokolja.

Az információvagyon felhasználása kizárólag a PPKE érdekeinek megfelelően történhet. Annak külső fél számára való elérhetővé tétele vagy hasznosítása csak a DPO és ITO együttes hozzájárulásával történhet, kivéve szerződéses és törvényi kötelezettségeket.

A szerződéses kötelezettségek vállalása az Egyetem vezetése vagy a DPO és ITO együttes és előzetes hozzájárulásával történhet.

8.2. Információosztályozás

Az információvagyon osztályozása az információbiztonság irányelvei szerint történik meg. Az osztályokba sorolást és nyilvántartást a DPO végzi a szakterületi vezetők bevonásával.

Az információosztályok az Egyetem esetében:

- Nyilvános információk osztálya: Az Egyetem által nyilvános módon működtetett felületeken (egyetemi, kari és tanszéki honlapok) megjelenített közérdekű információk
- Alapbiztonsági osztály: Személyes adatok, üzleti titok, pénzügy adatok
- Fokozott biztonsági osztály: Szolgálati titok, különleges személyes adatok, banktitok
- Kiemelt biztonsági adatok: Államtitok, nagy értékű üzleti titkok

Az egyes besorolási osztályok védelmét a törvényi előírásoknak megfelelő módon, mértékben köteles az Egyetem biztosítani.

8.3. Információhordozók kezelése

Az Egyetem információvagyonának elsődleges tárolási helye az Egyetemi IT infrastruktúra.

Magán eszközön vagy idegen tulajdonú tárolón az Egyetemi információvagyon tárolása tilos, kivételt képez ez alól a törvényi kötelezettség által előírt esetek, az Egyetem vezetése, vagy az ITO és a DPO közös, írásos hozzájárulásával elfogadott infrastruktúra vagy szerződött megoldás (pl. webes információtárolási szolgáltatások igénybevétele).

Az Egyetem tulajdonában lévő mobil eszközöket titkosítani szükséges. Az Egyetem területéről kizárólag titkosított formában vihető ki mobil eszközön információ.

A notebookok titkosítását az IT végzi el a felhasználó kérésére, személyes együttműködés keretében.

A mobiltelefonokhoz és tabletekhez („okos” eszközök) kapcsolódó információbiztonsági követelmények érvényesítése központi menedzsment program használatával történik. Külső adatkártyán PPKE adatot tárolni tilos.

A külső adathordozókon (pl. mobil HDD, pendrive, DVD) PPKE adatot tárolni csak titkosított formában engedélyezett. A titkosításhoz a technikai feltételeket az IT biztosítja.

Az Egyetem tulajdonában álló eszközöket megbízott félnek javításra csak az IT adhat át. Az eszközökön adat csak titkosított formában adható ki, de törekedni kell az adathordozó nélküli átadásra.
Amennyiben a javítás során az adathordozó átadása szükséges, nem titkosított adatokkal, a javítás csak az IT személyes részvételével lehetséges vagy az ITO és DPO együttes hozzájárulásával lehet eltekinteni a részvételtől.

Az eszközök beszerzésekor a helyszíni garancia vásárlása javasolt.

Az Egyetemről kikerülő eszközök (pl. értékesítés, selejtezés) adathordozóin található adatok a kor színvonalának megfelelő felülírással vagy az adathordozó eltávolításával vagy megsemmisítésével lehetséges. Az elszállítás, átadás előtt az IT munkatársa köteles írásos nyilatkozatban igazolni a törlést.

Adathordozó szállítása esetén a szállítást végző köteles kellő gondossággal eljárni az adathordozók és adatok biztonságának megőrzése érdekében. Az adatok eredeti forrása és mentése nem szállítható ugyanazon eszközzel.

Indokolt esetben az információ értékének megfelelő védelmi intézkedés, biztosítás szükséges. A szükségességről az ITO és a DPO közösen hoz döntést.

9. HOZZÁFÉRÉS SZABÁLYOZÁS

A hozzáférés szabályozás kapcsán a „lehető legkisebb jogosultság elvét" kívánjuk érvényesíteni, tehát minden érintett jogosultságát azokra az információkra korlátozzuk, melyek szükségesek a napi munkájuk végzéséhez.

Az Egyetem informatikai rendszereihez, erőforrásaihoz csak jogosultságengedélyezés után, és az IT által biztosított módon és mértékben lehetséges hozzáférni.

Hozzáférési jogosultság az IT HelpDesk-en keresztül a feladat elvégzéséhez szükséges mértékig igényelhető.

Hozzáférési jogosultság nem átruházható, az erőforrások megosztása tilos.

A jogosultságok, hozzáférések indokolatlan vagy szabályellenes felhasználása esetén az ITO kezdeményez eljárást a szabálysértővel szemben annak munkahelyi vezetőjénél.

Előzetesen nem engedélyezett jogosultság, hozzáférés megszerzésére tett kísérlet (megszerzéséhez szükséges technikai vagy egyéb információk gyűjtése, pl. hálózati forgalom megfigyelése, bármely típusú hacker tevékenység) súlyos biztonsági incidensnek minősül, amely azonnali kizárást az IT szolgáltatások igénybevételét illetően, valamint további munkaügyi, jogi eljárást vonhat maga után.

A hozzáférésekkel, jogosultságokkal való visszaélés (pl. adatbetekintés, saját célú vagy etikátlan, vagy törvénybe ütköző erőforrás használat) azonnali munkavégzés alóli felfüggesztést, eljárást vonhat maga után a Btk. 376. 424. és 425. §-ainak figyelembe vételével.

Hasonló elbírálás alá esik az a személy is, akinek tudtával vagy beleegyezésével vagy közreműködésével valósul meg a fenti cselekmény.

Az eljárásokat a DPO és/vagy az ITO kezdeményezi az Egyetem vezetésénél.

A felhasználó azonosítás címtárakban (AD, LDAP) történik. A felhasználó azonosítás során az egykapus és biztonságos azonosítási eljárások alkalmazására törekszünk a rendszerek elérhetőségének biztosítására. A Shibboleth megoldással támogatja az Egyetem a csatlakozó intézmények felhasználó azonosítás-biztonságát.

Az olyan bizalmas információkat tároló és kezelő rendszerek (pl. SAP, ECM, Nexon) elérhetősége csak belső egyetemi hálózatról engedélyezett a felhasználók számára.

Távolról történő rendszer-elérés felhasználók számára csak VPN (Virtual Private Network) alkalmazásával lehetséges.

Külső együttműködő, szolgáltató számára a rendszerekhez való hozzáférést az Egyetem VPN segítségével biztosít vagy egyedi megállapodás szerint, ideiglenes jelleggel (pl. SSH). A hozzáférések megadását az ITO engedélyezheti. A hozzáférés mértéke nem haladhatja meg a szerződött feladat elvégzéséhez szükséges és elégséges szintet.

Hozzáférési kulcs csak időkorlát alkalmazásával adható ki, annak időtartamát az ITO határozza meg.

Hozzáférési kulcs átadása felhasználónak csak személyesen történhet vagy indokolt esetben, titkosított formában lehetséges kiküldeni, amely feloldásához szükséges információt csak a kiküldési csatornától eltérő biztonságos csatornán (javasolt SMS-ben) lehetséges továbbítani az ITO hozzájárulásával.

Távoli rendszerüzemeltetés csak titkosított kommunikáció használatával lehetséges.

VPN hozzáférést kezdeményezni kizárólag egyetemi eszközről lehetséges.

Nem az egyetemi IT üzemeltetésében álló eszköz a belső hálózathoz nem csatlakoztatható.

Az IT jogosult minden IT üzemeltetésében álló eszköz esetében hozzáférést szabályzó, biztonságos működést, adatvédelmet célzó beállításokat, korlátozásokat alkalmazni.

A hozzáféréseket (belépéseket és kilépéseket) naplózza az IT és biztosítja, hogy ezek az adatok legalább 1 hónapra visszamenőleg és legfeljebb 1 évig visszakereshetők, lekérdezhetők legyenek.

Az Egyetem internetes hálózati kapcsolatait az ITO engedélyével lehetséges használni egyedi megállapodások alapján nem az egyetemi IT üzemeltetésében álló eszközökkel is, jellemzően kutatói tevékenység esetében, és a belső erőforrásoktól határvédelemmel elszigetelt módon. Az ilyen megoldás kialakítását megelőzően biztonsági kockázatelemzés szükséges az IT részéről. Az érintett eszközökkel az egyetemi belő hálózathoz csatlakozni tilos.

A nem az IT által üzemeltetett eszközökkel járó minden üzemeltetési, jogi, erkölcsi, gazdasági felelősség az üzemeltetést végző szervezeti egység vezetőjét terheli.

Az egyetemi IT erőforrásokat magán célú haszonszerzésre felhasználni tilos, ez a tiltás alól az egyetem Rektora vagy Gazdasági Főigazgatója adhat felmentést, az ITO tájékoztatásával. Az

egyetemi hálózati hozzáférés haszonszerzésre vonatkozó korlátait illetően az egyetemek közötti hálózati szolgáltatási szerződés (NIIFI, KIFÜ) az irányadó.

Az ITO hozzájárulása nélkül tilos IT szolgáltatást indítani, szolgáltatáshoz hozzáférést biztosítani az IT infrastruktúrán belül.

A PPKE érdekében az egyetemi IT infrastruktúráján kívül lévő szolgáltatást csak a Rektor vagy Gazdasági Főigazgató engedélyével, az ITO tájékoztatásával lehetséges indítani és üzemeltetni.

PPKE IT infrastruktúrán belül nem az IT által üzemeltetendő informatikai megoldásokat, szolgáltatásokat az ITO hozzájárulásával (ITO döntésétől függően a Rektor vagy Gazdasági Főigazgató engedélyével) lehetséges indítani és üzemeltetni az IT biztonsági és üzemeltetési irányelvek teljes mértékű figyelembe vételével és szabályainak betartásával. Az ilyen szolgáltatások üzemeltetői számára az ITO határozza meg az üzemeltetéshez szükséges hozzáférés módját és mértékét.

Az ITO bármely olyan IT üzemeltetésen kívüli szolgáltatást, amely az IT üzemeltetési tevékenységét, szolgáltatásainak működését, biztonságát kockáztatja, akadályozza, azonnali hatállyal az illetékes értesítése mellett leállíthatja, vagy annak leállítását kezdeményezheti.

Az IT üzemeltetésen kívüli szolgáltatások rendelkezésre állási feltételeit (pl. adat-visszaállítás mentésből), azokat szolgáltató eszközök fizikai elérhetőségének módját az ITO határozza meg a szolgáltatást nyújtóval konzultálva.

Az IT a hozzáféréseket, tevékenységeket az üzemeltetés biztonsága, adatok védelme, szolgáltatás javítása érdekében naplózhatja mind a felhasználókra, mint az üzemeltetőkre vonatkozóan.

Minden hozzáférés kizárólag személyes azonosításra alkalmas módon történhet IT rendszerhez. Nem nevesített felhasználóval üzemeltetési tevékenység sem végezhető. A hozzáférés birtokosa köteles gondoskodni a hozzáférés biztonságos kezeléséről. Az IT jogosult kötelező szabályokat meghatározni a hozzáférések kezelését illetően.

Az IT rendszerekkel kapcsolatos üzemeltetési szerződésekben a hozzáféréseket, a naplózás módját, és az üzemeltetői tevékenységgel kapcsolatos felelősségeket meg kell határozni és a megállapodásban foglaltakat érvényre kell juttatni, és a feltételek teljesülést az IT ellenőrizheti.

Az egyes rendszerekben történő üzemeltetési tevékenységek naplózása külső szolgáltató esetén a szerződésben szabályozott módon és mértékben, IT munkatársak esetében az üzemeltetői jogokkal való visszaélésekre alkalmat kínáló tevékenységek esetében kötelező. Az üzemeltetési tevékenység ésszerű határokon belüli, de az esetleges biztonsági incidensek, üzemeltetési események követhetőségét lehetővé tevő szinten való naplózására törekedni kell.

A tevékenységet és hozzáféréseket leíró napló- és rendszerfájlok védelmének biztosítása, az IT üzemeltetést végző munkatársaktól is, az üzemeltetést végző szakterületi vezetők munkaköri kötelessége.

10. TITKOSÍTÁS

Az „A” és „B” osztályú rendszerekbe történő, változtatási jogosultságot is lehetővé tevő bejelentkezés csak védett, titkosított kommunikációval (pl. SSH, VPN) engedélyezett a PPKE hálózatán kívülről.

10.1. Kriptográfiai kontrollok használatának szabályozása

Egyéb kriptográfiai szabályozásokat az adott szolgáltatásra kötött megállapodásban kezelik a felek.

10.2. Kriptográfiai kulcsok menedzsmentje

A hozzáférési jogosultságok elbírálását végző komponensek bármely rendszer esetében a felhasználói jelszavakat csak titkosítva tárolhatják.

11. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

Az IT kiszolgáló infrastruktúra kulcseleminek elhelyezése szerverszobában vagy hálózati eszközök esetében zárt szekrényekben kötelező.

A zárt infrastruktúrához hozzáférése csak az IT munkatársainak lehetséges, kivétel az üzemeltetés lezárt módon a Portán tárolt kulcsa különleges esemény kezelésére.

A szerverszobába csak naplózott módon lehetséges bejutni. A szerverszobában csak az IT személyzet tartózkodhat, egyéb személy csak IT munkatárs felügyelete alatt látogathatja a helyiséget. A szerverszobában biztonsági okok miatt maximum 8 fő tartózkodhat egyszerre.

A szerverszoba áram, szünetmentes, túlfeszültség védelmi és hűtés ellátását, videó és beléptetési és távközlési kapcsolati, tűz és vagyonvédelmi szolgáltatását az Egyetem üzemeltetésért felelős szervezeti egysége szolgáltatja. Az IT szolgáltatások rendelkezésre állást érintő, befolyásoló tevékenységekre vonatkozóan az IT tudomása és jóváhagyása nélkül változtatás, karbantartás, egyéb tevékenység nem végezhető.

Az üzemeltetés köteles gondoskodni a kiszolgáló szolgáltatások működés-folytonosságának garanciáiról.

A felhasználók leltári felelőssége alá tartozó eszközök fizikai biztonságáért a felhasználó felel. A felhasználó köteles kellő gondossággal eljárni, hogy a kezelésében álló vagyontárgyak, különös tekintettel az információvagyonra, az Egyetem tulajdonában, elvárható állapotban maradjanak, valamint képesek legyenek a feladatuk ellátására. (Pl. nem elfogadható gondosság a lezárt autóban felügyelet nélkül hagyott eszköz.)

Az IT eszközök tárolása a felhasználó távollétében használati szempontból zárolt állapotban, elzártan tartandó. Az oktatótermek esetében elzártnak akkor minősül az eszköz, ha annak leltári felelőssége követhető. Az eszköz használat szempontjából lezártnak minősül, ha tevékenység csak felhasználói bejelentkezést, azonosítást, jogosítást követően végezhető, illetve a tevékenységre utaló adat nem látható, nem visszaállítható. (Pl. kijelzőn adat, nyomtatóban lap.)

IT üzemeltetési vagy egyéb felhasználói információ, amely a rendszerbe történő illetéktelen behatolást, biztonsági incidens eredményezhet, használaton kívül is elzártan, arra alkalmas szekrényben, páncélszekrényben tárolandó.

Licence, telepítő média, amelynek elvesztése, illetéktelen kezekbe jutása anyagi, erkölcsi hátrányt, biztonsági incidenst eredményezhet, csak arra kijelölt, zárt szekrényben tárolható. A licenc dokumentumok, médiák központi technikai nyilvántartása, tárolása az IT feladata. Az IT leltári, gazdasági jellegű nyilvántartást nem vezet.

Adathordozóval szerelt berendezések (pl. HDD-vel szerelt multifunkciós eszközök) elzáratlan területen (pl. folyosó) csak abban az esetben elhelyezhetők, ha azokra 24 órás biztonsági megfigyelés garantálható (Pl. portaszolgálat kamera).

Az információtároló eszközök, helységek, szerverszobák megválasztása és kialakítása biztonsági szempontok teljes körű figyelembe vételével történhet.

Az informatikai eszközök, adathordozók elhelyezése, mozgatása (rakodás, raktározás) az egészségügyi, balesetvédelmi, adatbiztonsági és vagyonvédelmi kockázatok figyelembe vételével, szabályok betartása mellett lehetséges.

Az IT az informatikai eszközök tömeges mozgatását nem végzi, a szállításra előkészítés, majd az üzembe helyezés a feladata.

Az IT nagy tömegű eszközök (pl. nagyformátumú nyomtatók) mozgatását nem végzi, azok átvételét és beüzemelését az üzemeltetési helyszínen szükséges elvégezni.

Az IT az oktatástechnikai eszközök IT vonatkozású technikai működtetését támogatja. Azok biztonságos tárolása, sérülés elleni védelme, szállítása, telepítése (pl. mennyezeti projektor telepítés) nem feladata.

11.1. Területek védelme

Minden egyetemi campus porta szolgálattal védett. A fizikai belépés, beléptetés felügyelete a portaszolgálat feladata.

Az informatikai eszközök tároló helyiségeinek forgalmát, az eszközök fizikai védelmét (pl. közösségi területen elhelyezett rack szekrények) és az IT eszközök mozgását a portaszolgálat kiemelt figyelemmel kezeli.

Azon irodák, melyekben IT eszközök vannak elhelyezve, használaton, felügyeleten kívül kulcsra zárva tartandók.

Szállítási és rakodási területen IT eszköz felügyelet nélkül nem maradhat a rakodás idejére sem. A szállítási és rakodási területek kijelölése a Műszaki Igazgatóság feladata.

11.2. Berendezések

Az IT üzemeltetésében álló eszközök karbantartására az IT feladata. Az IT karbantartási felelőssége teljes körű a központi kiszolgálók, hálózati eszközök terén.

A felhasználók kezelésében álló eszközök fizikai karbantartása a felhasználó feladata (pl. notebook, monitor, telefon, billentyűzet portalanítás) az elvárható hozzáértés mértékéig. Amennyiben a felhasználó bizonytalan a karbantartási tevékenység megfelelőségét, biztonságos megvalósíthatóságát illetően, szakmai tanácsot kérhet az IT munkatársaitól. A felhasználó kizárólag a baleset-, egészség-, tűzvédelmi és vagyonvédelmi szabályok betartásával végezheti a karbantartást. A helytelen karbantartásra, rendellenes eszköz használattal, elhelyezéssel kapcsolatos károkra visszavezethető károk a felhasználót terhelik.

A felhasználói eszközök szoftveres karbantartása az IT feladata. A szoftveres karbantartási tevékenység (pl. frissítés, telepítés) támogatására központi menedzsment eszközök használat ajánlott.

Az IT központi, kötelezően alkalmazott kártékony kód elleni védelmi szolgáltatást biztosít felhasználói munkaállomásokra, amelyek frissítését az IT végzi, központi terjesztéssel. Az IT határvédelmi megoldással is támogatja a rosszindulatú tevékenységek elleni védelmet.

Felhasználó támogatási céllal távfelügyeleti megoldás (monitor és konzol átvétel) alkalmazása lehetséges, de kizárólag a felhasználó adott alkalomra vonatkozó hozzájárulásával.

Fizikai karbantartási tevékenység központi kiszolgálók esetében külső megbízott által csak az IT felügyelete alatt, annak engedélyével, személyes részvétel mellett, a szerződésben foglaltak szerint lehetséges.

Távfelügyelettel ellátott karbantartási tevékenység külső megbízott részéről a szerződésében foglaltak szerint lehetséges.

Takarítási tevékenység során az eszközök hálózati vagy áram ellátásának, ki-be kapcsolt állapotának változtatása tilos. Vonatkozó rendelkezésre-állás folytonossági biztonsági tájékoztatást a takarítást végző munkatársak számára a Műszaki Igazgatóság köteles biztosítani.

Az elektromos, telekommunikációs és hálózati összeköttetések biztonságos, védett elhelyezését, elvezetését a Műszaki Igazgatóság biztosítja rack szekrényig. A végződtetés helyét és minőségét az IT határozza meg. A szerverszobán belüli kábelezési kérdésekben az IT dönt és jár el.

Az IT eszközök elhelyezését balesetmentesen üzemeltethető formában kell megoldani. A szerverszobában egyedül csak bejelentés mellett lehetséges tartózkodni az IT munkatársainak is. A bejelentést a helyi portán, vagy a helyszíni IT munkatársaknak vagy az ITO-nak lehetséges megtenni.

A szerverszobában csomagolóanyag, használaton kívüli eszközök nem tárolhatók. A szerverszoba raktározásra nem használható.

Az IT eszközök raktározása a központi raktározási eljárásrend szerint történik, amely meg kell, hogy feleljen az adat és vagyonbiztonság arányos kockázatainak. Raktárban csak adat-tartalom nélküli eszköz tárolható.

Az eszközök beszerzést követő, raktárból történő kihelyezését, beüzemelését, visszavételét, az érintett szervezeti egységek együttműködését és adminisztrációs kötelezettségeit a vonatkozó belső utasítás tartalmazza.

IT eszközt selejtezési céllal elszállítani vagy harmadik fél számára elérhetővé tenni kizárólag az IT előzetes engedélyével lehetséges. Az IT köteles a kor színvonalának megfelelő szintű adatmegsemmisítésről gondoskodni minden kiadott adathordozó esetében, a selejtezésre elszállítás esetén az adathordozó fizikai használhatatlanná tétele kötelező. (pl. fizikai roncsolás fúróval).

A selejtezést végző és átadó munkatárs is köteles meggyőződni arról, hogy adathordozó vagy papír alapú dokumentum nem maradt az eszközben.

Az egyes munkahelyeken a „tiszta asztal és tiszta képernyő” elv megvalósítása kötelező.

12. AZ ÜZEMELÉS BIZTONSÁGA

Az üzemelés, üzemeltetés során figyelembe veendő eljárási szabályok:

12.1. Üzemeltetési eljárások és felelősségek

Az IT az üzemeltetési feladatait az ITIL irányelveinek figyelembe vételével végzi, azt az ésszerű erőforrások felhasználásához mérten köteles szabályozni és dokumentálni.

Kötelező dokumentumok, amelyeket változás esetén megújítani, éves gyakorisággal ellenőrizni szükséges:

1. Mentési eljárási rend
2. Kapacitás terv
3. Változás kezelési eljárási rend
4. Beszállítói szerződések nyilvántartása (főbb SLA paraméterek, kontakt személyek, stb.)

A szabályozás és dokumentum megfelelés felelőse az ITO.

Az IT munkatársainak tevékenység-ellenőrzésére az ITO külső szakértő bevonásával gondoskodik. Az ellenőrzés célja a visszaélések felderítése és megelőzése.

Az üzemeltetési tevékenység három logikailag elkülönült területen történik:

1. éles környezet,
2. fejlesztői környezet és
3. teszt környezet.

A három területen folyó üzemeltetés alapelveit a szakma általános gyakorlata alapján az IT köteles betartani és betartatni az ésszerű és lehetséges erőforrások korlátain belül.

Az IT éves gyakorisággal technikai javaslatot (éves fejlesztési terv) tesz a szükséges fejlesztések, kapacitás bővítések, pótlások végrehajtására az Egyetem vezetése és az önállóan beszerző szervezeti egységek számára.

A hosszútávó kitűzött célokat, fejlesztési elképzeléseket az IT stratégia dokumentum tartalmazza.

Az IT biztonsági mentést készít minden központi tárolón elhelyezett dokumentumról.

A felhasználói eszközökön, mobil adathordozókon tárolt adatok rendelkezésre állásáért nem válla az IT felelősséget. PPKE tulajdonú információ vagyon csak központi tárolón tárolható.

A mentések az éles rendszerek tárolási helyétől telephelyileg elkülönülő helyen kerülnek elhelyezésre.

Az IT biztosít Alfresco, ECM dokumentum kezelő szolgáltatást, valamint fájlmegosztó szolgáltatást. A dokumentumok használatára, tárolására adatbiztonsági (pl. zsarolóvírus) okokból az Alfresco, ECM megoldás javasolt, míg a fájlmegosztó megoldás célja az ideiglenes dokumentumok rugalmas átadásának támogatása.

12.2. Védelem a rosszindulatú szoftverek ellen

Minden olyan rendszer esetében, ahol kártékony kód fenyegetés fennáll és lehetséges installálni kártékony kód elleni rendszert, akkor azt az IT telepíti, és ennek a szoftvernek felhasználói megkerülése tilos.

Nem PPKE tulajdonú eszközök használatából eredő kártékony kód által okozott károkért a PPKE rendszereiben felhasználóként belépett személy a felelős (pl. vírusos USB kulcs).

12.3. Biztonsági mentés

A mentési eljárási rendnek tartalmaznia kell az alkalmazások és adatok mentési rendjét (a mentendő adatok körét, a mentés módját és gyakoriságát, és a mentésért felelős személyt, a mentés tárolási rendjét, mentés külső tárolásának rendje).

A mentési rendnek alkalmasnak kell lennie arra, hogy az üzemeltetési környezet visszaállítható legyen.

Minden „A” és „B” osztályú rendszer esetében mentés tesztelési környezetet kell létrehozni, és lehetősége szerint évente minimum egy alkalommal visszatöltési gyakorlatot (tesztelés) kell tartani, ami a mentések felhasználhatóságát ellenőrzi.

A PPKE adatmentési és archiválási gyakorlatát a Mentési eljárási rend szabályozza.

12.4.Naplózás és monitorozás

A PPKE IT 7/24 órában monitorozza az IT rendszerek működését. A monitorozás eredményeként megjelenő riasztások kezelése az IT munkaidejében történik.

A felhasználók nem férnek hozzá a naplófájlokhoz, az egyes rendszerek üzemeltetői betekintést nyerhetnek kérésre, melyet az IT teljesít.

A naplófájlok hitelességét óraszinkronizálással biztosítjuk.

12.5. Az operatív szoftverek kontrollja

Operatív szoftverek telepítésére az üzemeltetési rendszerekben kizárólag az IT-nek van joga. A hiteles licence nyilvántartás kidolgozása az IT feladata.

12.6. Műszaki sebezhetőségek menedzsmentje

Az adott alkalmazás üzemeltetője felelős az alkalmazások publikált technikai sérülékenységek elleni védekezés megvalósításáért. Az infrastruktúráért felelős üzemeltető kötelessége az infrastruktúra elemek védelmének sebezhetőség elleni biztosítása.
Alap rendszerek esetében (pl. operációs rendszerek, virtualizációs rendszerek, kártékony kódok elleni védekező rendszerek, stb.) törekedni kell a publikált sérülékenységek elleni védekező intézkedés (pl. patch-ek és fixek alkalmazása) mielőbbi végrehajtására, tekintettel a az adott rendszereket használó alkalmazások és az ésszerű erőforrás gazdálkodás korlátaira.
Alkalmazások esetében a gyártói ajánlás alapján, a szakma gyakorlata szerint kell eljárni.
Hardver elemekhez kapcsolódó frissítések végrehajtása esetében az alaprendszerek esetében meghatározott módon kell eljárni.
Azokban az esetekben, ahol az alkalmazás jelenti a naprakészség biztosítását, törekedni kell a rendszerek kiváltására, vagy kivonására, a biztosított szolgáltatások köréből.
Az ITO jogosult nem frissített rendszer/szolgáltatás azonnali kizárására az IT környezetből.

12.7.Az információs rendszerek felülvizsgálatával kapcsolatos megfontolások

Az információ biztonságot az ITO és a DPO minden évben köteles felülvizsgálni egy erre létrehozott projekt keretében.

Az IT köteles fejlesztési tervet készíteni (lásd 12.1 pont) az üzemeltetéshez kapcsolódó kockázatok, rendszerek sebezhetőségének csökkentése érdekében.

13. A KOMMUNIKÁCIÓ BIZTONSÁGA

A kommunikációs hálózatok (kivétel a szolgáltatók által biztosított rendszerelemek és szolgáltatások pl. távközlési hálózatok, mobil hálózat, idegen eszközök, alépítmények stb.) biztonságos üzemeltetését az alábbi irányelvek szerint köteles az IT biztosítani:

A hálózati eszközök kiválasztásánál a magas rendelkezésre állási minőségre, a központi menedzselhetőségre, a homogén (kapcsolható, ésszerűen tartalékolható, cserélhető) elemekből építkezésre, a hosszú távon gazdaságosan üzemeltethető megoldásokra (lehetőség szerint fix költség választására, rendszeres licence díjak kerülése) kell törekedni.

A passzív hálózat változtatása kizárólag az IT hozzájárulásával történhet. Aktív hálózati eszközt az Egyetemi tulajdonú eszközökön kívül csatlakoztatni a hálózathoz tilos. Az aktív eszközök beállítását és illesztését az IT végzi. A hálózati szolgáltatás megosztására alkalmas eszközt a hálózathoz illeszteni tilos az IT munkatársain kívül.

A hálózatokat fizikai és logikai megoldásokkal is szegmentálni szükséges. Az Internet oldali hálózatot és a belső hálózatot tűzfallal kell elválasztani. Internet irányba csak az erre alkalmas tűzfalakon lehet kilépni az Egyetem hálózatából.

A belső hálózatokat szegmentálni szükséges VLAN-ok kialakításával. A VLAN-ok szervezeti egységek és funkciók szerint kerülnek kialakításra.

Törekedni kell a MAC address alapú végpont azonosításra, port security korlátozások bevezetésére, ahol az biztonsági szempontból fokozottan indokolt.

A hálózati beállítások alapelve a „alapvetően minden tiltott és csak a munkavégzéshez szükséges kivétel engedélyezett (a szükséges legkisebb jogosultság elve)”.

Az alap hálózati infrastruktúra kialakítása magas rendelkezésre állással szükséges. Az alapinfrastruktúra kiterjed a magas rendelkezésre állású szolgáltatásokat (LDAP, AD, SAP, ECM, FileShare, Zimbra…) kiszolgáló hálózati eszközökre (switch, router), tűzfal szolgáltatást biztosító eszközökre és azokon futó szolgáltatásokra. A magas rendelkezésre állás biztosítása céljából az IT tartalékot köteles képezni az ésszerű erőforrás gazdálkodás irányelveinek betartásával.

A WAN hálózat szintjén redundáns optikai körgyűrű kialakítása szükséges a budapesti telephelyek összekötésére.

Törekedni kell a vidéki telephelyeken az optikai kapcsolat megszakadása esetére az alapvető működés biztosítására (lokális címtár kiszolgáló, Internet kapcsolat).

A vezetéknélküli hálózat elemeinek illeszkedni kell egy központilag menedzselt infrastruktúrába.
A központi menedzsmentet redundáns kialakítással szükséges megvalósítani. A WiFi controller és az AccessPoint-ok közötti forgalom titkosított. Az AccessPoint-ok jelszóval védettek, beállításuk a contoroller segítségével megváltoztatható a hálózatban.

A hálózati aktív eszközök eltulajdonítása esetén azokból nem nyerhető ki hálózati menedzsment információ, mert adatokat ezek az eszközök csak titkosítva tárolnak.

Hálózat menedzsmentje csak az IT által kijelölt személyek számára lehetséges. Hálózati menedzsment tevékenység csak hálózaton belülről, meghatározott IP címről kezdeményezhető. A kommunikáció titkosított módon lehetséges.

A hálózati forgalom lehallgatása, megfigyelése, szolgáltatások veszélyeztetése, vagy azokra utaló magatartás az IT rendszerekből történő azonnali kizárást és felelősségre vonást eredményez. A hálózati forgalom megfigyelésére, naplózására, elemzésére kizárólag az IT hálózati menedzsment feladatokat ellátó munkatársai jogosultak. A megfigyelés tárgya nem terjedhet ki a személyes felhasználói kommunikáció tartalmára (Pl. IT munkatárs nem olvashatja a hálózati forgalomból kinyerhető felhasználói üzenet tartalmát.) A megfigyelés tárgya kizárólag a hálózati szolgáltatás biztonságos, rendeltetetésszerű működésének biztosítását szolgálhatja.

A hálózati eszközök jelszó kezelése megegyezik az általános jelszókezelési szabályokkal.

A távközlési szolgáltatókkal kötött szolgáltatói szerződésekben a rendundáns megoldásokra kell törekedni. Külső szolgáltatóval a szolgáltatási felelősségi határokat úgy kell meghatározni, hogy azok egyértelműen számon kérhetők legyenek, valamint ne feltételezzenek átlapolódó menedzsment felelősségeket. A belső hálózatban külső szolgáltató nem kaphat lehetőséget felügyelet nélküli menedzsment tevékenységre, kizárólag az IT belső munkatársa közreműködésével járhat el.

13.1. A hálózati biztonság menedzsmentje

Az intézmény teljes területére kiterjedő alapinfrastruktúra (számítógépes és telefonhálózat) védelme egységes koncepció és megvalósítás mellett történik. Az irányelvek és módszerek meghatározását és a szükséges operatív beavatkozásokat a telekommunikációs hálózat üzemeltetésével megbízott IT szervezeti egység végzi. A kommunikációs hálózathoz való csatlakozás feltétele a (csatlakozás módjától és a csatlakoztatott rendszertől függő) biztonsági előírások maradéktalan betartása. Ezen előírások a csatlakozásnak, mint szolgáltatásnak az igénybevételi feltételei között tekinthetők meg.

A hálózat felépítését, az egyes zónákat a hálózati infrastruktúra dokumentáció tartalmazza. A dokumentáció naprakészségének biztosítása az IT vonatkozó szakterületének a feladata.

13.2. Információ átvitel

Az elektronikus információátadás szabályait az Egyetem vonatkozó elektronikus információátadási szabályzata tartalmazza.

A bizalmasságra, titoktartásra vonatkozó kötelezettségeket a munka és egyéb vállalkozási, hallgatói szerződések szabályozzák.

14. INFORMÁCIÓS RENDSZER BESZERZÉS, FEJLESZTÉS ÉS FENNTARTÁS

Információs rendszer, eszköz csak az IT-val egyeztetett módon, annak jóváhagyásával szerezhető be.

A rendszerek megválasztása során törekedni kell az egyéb rendszerekhez való műszaki illeszthetőségre, a hosszú távú gazdaságos (lehetőség szerint saját erőforrással történő) üzemeltethetőségre, kiszolgáló erőforrások rendelkezésre állására, biztonságra, szakértelem rendelkezésre állására, optimális ütemezésre, felhasználói elégedettségre.

Valamely feltétel hiánya, nem megfelelése esetén az IT jogosult a jóváhagyott rendszer beszerzését, vagy illesztését az IT infrastruktúrához megtagadni.

Az IT üzemeltetési szolgáltatást az előzetes megállapodásban rögzített mértékig köteles nyújtani.

Az felhasználók részére biztosított IT eszközök szabályozott módon, úgynevezett normatívák mentén szerint szerezhetők be.

A normatívák meghatározása beosztás és funkcionális megfelelés szerint történik. A felhasználói normatívák az egységes, biztonságosan üzemeltethető infrastruktúrát és költséghatékony gazdálkodást szolgálják. A normatívák meghatározásának műszaki vetületeiért az IT felelős. A normatívák szerinti beszerzés szabályozását a Beszerzési Osztály végzi.

A beszerzési igények meghatározása a Beszerzési Osztály koordinációjával történik. Az IT szakmai támogatást nyújt a tervezésben a szervezeti egységek számára, illetve a központi szolgáltatásokat, azokat biztosító IT eszközöket tervezi és szerzi be a rendelkezésére álló erőforrások mértékében.

Az IT az Egyetemi stratégia és az ésszerű gazdálkodás irányelveit köteles követni az erőforrások felhasználását illetően.

Alapelv a biztonság, adatok rendelkezésre állásának, sértetlenségének és bizalmasságának a biztosítása az üzleti igények kiszolgálásán túl.

14.1. Az információs rendszerek biztonsági követelményei

Új rendszerek megvalósítása során a biztonsági követelményeket előzetesen meg kell határozni, és a szolgáltatás indítási kérelemhez mellékelni kell.

A már működő rendszerek továbbfejlesztése, módosítása során a biztonsági követelmények nem változtathatók olyan irányba, hogy a rendszer biztonsági szintje csökkenjen (kivétel ez alól, ahol a kockázatelemzés eredménye ezt lehetővé teszi).

14.2. Biztonság a fejlesztési és a támogató folyamatokban

Minden alkalmazás fejlesztési tevékenységét a szolgáltató alkalmazás-példánytól és annak adatbázisától elkülönülten kell végezni. Amennyiben a fejlesztési tevékenységhez védett intézményi adatok is szükségesek, akkor a fejlesztői rendszer is „B” osztályú rendszernek minősül és a hozzáférési jogosultságok ennek megfelelően adhatók ki.

Intézményi fejlesztésű vagy vásárolt szolgáltató rendszer csak funkcionális teszt után vonható szolgáltató üzembe. A funkcionális tesztnek az SLA-ban rögzített minden paraméterre és funkcióra, valamint a tipikus felhasználási mintákra kell kiterjednie. A funkcionális tesztről írásos jegyzőkönyvnek kell készülnie, melynek az összes mért és ellenőrzött paramétert és funkciót tartalmaznia kell.

Minden, a szolgáltatási felületen vagy a funkciókészletben különbséget tartalmazó alkalmazás verzió esetén a tesztelési eljárást újra el kell végezni. A tesztelési kötelezettség az operációs

rendszerek, adatbázis kezelők és egyéb támogató alkalmazások (pl. web szerver) esetén is fennáll, de csak a használt funkciókra kell kiterjednie.

Szolgáltató üzemben működő alkalmazáson csak sikeres tesztelési jegyzőkönyv birtokában és az üzemeltető rendszergazda engedélyével végezhető változtatás (külső munkavégző cég esetében is). Ezen előírás alól csak a szolgáltatás helyreállítását célzó sürgős hibajavítás jelent kivételt, ami esetében a dokumentálást utólag kell elvégezni.

15. SZÁLLÍTÓI KAPCSOLATOK

A szállítóinkkal való kapcsolattartás szabályai:

- Személyes vagy intézményi adatok kiadása, csak a hatályos jogszabályoknak megfelelően történhet.
- Az átadott adatok védelméért a szerződő fél tartozik felelősséggel.
- Az egyetemi kapcsolattartó tanácsot kérhet, kétség esetén köteles kérni, a DPO-tól vagy az ITO-tól adatvédelmi és információbiztonsági kérdésekben.

15.1. Információbiztonság a szállítói kapcsolatokban

Minden szállítóval kötött megállapodás, szerződés esetében a megállapodásban vagy szerződésben rögzítendők az adatvédelmi és az információbiztonsági kérdések. Ennek felelőse mindig az adott egyetemi kapcsolattartó. Az egyetemi kapcsolattartó köteles bevonni a DPO-t vagy az ITO-t az adatvédelmi és információbiztonsági kérdések egyeztetésébe.

15.2. A szállítói szolgáltatások, teljesítés menedzselése

A szállítói IT (pl. Neptun, SAP fejlesztések) szolgáltatások ellenőrzésének felelőse az IT. Minden szállítói szolgáltatási megállapodás esetében az IT bevonása szükséges a szolgáltatási feltételek, ellenőrzés és együttműködés módjának egyeztetése és rögzítése céljából.

Szállítói megállapodásban mérhető, számonkérhető, a teljesítési elvárásokat jól tükröző teljesítménymutatókat kell meghatározni. A mért eredményeket folyamatosan vagy időszakosan, megállapodás és szolgáltatás jellegétől függően, jelenteni szükséges.

A szolgáltatási jelentéseket, riportokat a szolgáltatási szint egyeztetések keretében kell felhasználni a szolgáltatás minőségének javítására, szerződésben foglalt vállalások számonkérésére, szerződésben foglalt kötelezettségek érvényesítési alapjának szállítói egyeztetésére.

Törekedni kell a szállítóval való együttműködés során a saját ITSM rendszer használatára. Törekedni kell a szolgáltatások automatizmusokkal támogatott monitorozására, a proaktív szállítói tájékoztatásra, megelőző beavatkozások támogatására.

Az IT szerződés-nyilvántartást, eszkalációs kapcsolati listát kell vezessen kapcsolattartási és teljesítés értékelési céllal.

16. INFORMÁCIÓBIZTONSÁGI INCIDENSEK KEZELÉSE

Minden szolgáltató rendszer esetében a szolgáltatás üzemeltetője köteles incidens bejelentési lehetőséget biztosítani a felhasználóknak, és a bejelentés módját az SLA-ban közzétenni. A bejelentett incidenseket az üzemeltetők a szolgáltató rendszer integritásának és a kezelt adatoknak a védelmében kötelesek lehetőség szerint rövid reakcióidővel elbírálni és a szükséges lépéseket (pl. hozzáférés korlátozás, biztonsági komponensek beállításainak módosítása) megtenni. Az üzemeltető köteles a bejelentőt tájékoztatni a biztonsági esemény következményeiről és a megtett intézkedésekről. Tömeges érintettség esetén lehetőség van az IT központi tájékoztató csatornáinak használatára is.

Biztonsági esemény vagy gyengeség bejelentése esetén a bejelentő köteles csatolni mindazon adatokat, amik az esemény megítéléséhez legjobb tudása szerint szükségesek (pl. időpont, tapasztalt jelenség, log file részlet, stb.)

A szolgáltatások felhasználása közben tapasztalt biztonsági gyengeségek jelentése (a rendszer működőképességének fenntarthatósága érdekében) minden felhasználónak kötelessége. Ennek elmulasztása vagy a gyengeség kihasználása biztonsági eseménynek minősül.

Az információbiztonsági incidensek kezelésének részletes eljárási rendjét a vonatkozó utasítás tartalmazza.

17. A MŰKÖDÉSFOLYTONOSSÁG MENEDZSELÉSÉNEK INFORMÁCIÓBIZTONSÁGI ASPEKTUSAI

Az IT a működésfolytonossági igények szempontjából az alkalmazói rendszereket kategóriákba sorolja, és a kiemelt szolgáltatások biztosítása céljából legalább két, földrajzi értelemben különálló, elválasztott telephelyen szükséges az IT adatvagyon elhelyezése.

Az IT gondoskodik az éles rendszerek adatainak és mentéseinek elkülönült tárolásáról.

Támogatandó a gyors mentésből történő visszaállást, törekedni kell a tartalék infrastruktúra elemek és rendszerek kialakítására, és az ezirányú fejlesztési tervek megvalósítására.

Az IT évente felülvizsgálja és dokumentálja az infrastruktúra elemeit, meghatározza az aktuális fejlesztési prioritásokat.

A működésfolytonosság fokozása az üzleti igényeken alapuló, ésszerű erőforrás gazdálkodás elvein nyugszik.

A fejlesztési elképzelések az IT stratégia mentén az évenkénti költségvetés tervezésben meghatározott lépések szerint kerülnek végrehajtásra.

18. KÖVETELMÉNYEKNEK VALÓ MEGFELELŐSÉG

Az ITO felelőssége a mindenkori jogszabályi megfelelőség biztosítása a nyújtott szolgáltatások vonatkozásában.

Az ITO igazgatója értelemszerűen nem felel a felhasználók által elkövetett jogsértésekért (pl. jogosulatlan adatkezelés, szerzői jogokkal való visszaélés stb.), és hatósági megkeresés esetén a jogszabályban előírt adatokat az adott felhasználóval kapcsolatban kiadhatja.

Az információbiztonság független felülvizsgálata

Az IT-SZ-szel összhangban az ITO felelős azért, hogy az IT-rendszerek teljes körű belső biztonsági felülvizsgálata dokumentált módon (belső felülvizsgálati jelentés) legalább évente megtörténjen, és legalább háromévente sor kerüljön külső, harmadik fél általi felülvizsgálatra az „A” osztályú rendszerek esetében.

Súlyos biztonsági incidens esetén a DPO külön rendkívüli biztonsági ellenőrzést és felülvizsgálatot rendelhet el és minden esetben bevonja az ITO-t a vizsgálatba, illetve megosztja vele a tapasztalatokat.

A felülvizsgálatok eredményei alapján az ITO rendel el javító, helyesbítő és megelőző intézkedéseket, melyeket mindig a soron következő belső vagy külső, harmadik fél általi felülvizsgálat során kell dokumentált módon visszaellenőrizni.

Megfelelőség a biztonsági szabályzatoknak és standardoknak

Az ITO felelőssége a mindenkori biztonsági politikának, szabványoknak és műszaki előírásoknak való megfelelőség biztosítása a nyújtott szolgáltatások vonatkozásában.

19. ZÁRÓ RENDELKEZÉSEK

A Pázmány Péter Katolikus Egyetem Információbiztonsági Szabályzatát az Egyetemi Tanács 2018. xxxx. Yyy-én hozott xxx/2018 (IV…..) számú határozatával jóváhagyta.

Mellékletek

1. számú melléklet: Üzemeltetői (és felhasználói) bizalmassági nyilatkozat
2. számú melléklet: Titoktartási nyilatkozat üzleti partnerek részére