PÁZMÁNY

1635

Pázmány Péter Katolikus Egyetem Informatikai Szabályzata

PÁZMÁNY
Pázmány Péter Katolikus Egyetem
1635

2023.

Változások, felülvizsgálatok jegyzéke:

Verzió	Dátum	Rövid összefoglaló
1.0	2022.06.08.	Eredeti változat
1.1	2022.07.11.	Módosítások egyeztetése
1.2	2022.08.17.	Szabályozások meghatározása

Dokumentum felülvizsgálata:

Következő tervezett felülvizsgálat dátuma:	Felelős

Jóváhagyta:

Dátum:	Felelős	Aláírás
2022.xx.xx		

PÁZMÁNY
Pázmány Péter Katolikus Egyetem
1635

Dokumentum elektronikus adatai:

Elektronikus tárolás:	Érvényes
PPKE_Informatikai_Szabályzat	2023
Elektronikus verzió tárolási helye:	

Tartalomjegyzék

1. Az Informatikai szabályzat célja

Az informatikai szabályozás elsődleges célja, hogy megteremtse, biztosítsa és garantálja a **Pázmány Péter Katolikus Egyetem** (Továbbiakban: **PPKE**) működése számára a kiemelten magas színvonalú, egységes, biztonságos, stabil, fejlődőképes informatikai működési és szabályozási környezetét. Az informatikai eszközök egyre szélesebb körű használatára azonban új, eddig nem tapasztalt, változó és mindig megújuló kockázatot jelent a PPKE számára, ezért jelen szabályzat célja egységes keret szabályokat, értelmezéseket, iránymutatást adni az adatgazdák, az informatikai eszközök üzemeltetői, fejlesztői, felhasználói számára, rögzítve azokat a szabályokat, amelyeket a munkakörükhöz rendelt adatok kezelése során követniük kell.

A jelen Informatikai Szabályzat (IT-SZ) szabályzat célja:

- Egységes szemléletben meghatározni a felhasználók és az információtechnológiai rendszerek viszonyát az informatikai rendszerek által kezelt **adatokat, információk bizalmasságának, sértetlenségének, rendelkezésre állásának megőrzése** érdekében;
- Azon alapvető biztonsági normák, ajánlások és működési keretek meghatározása, amelyek érvényesítésével a PPKE az elfogadható minimumra csökkentheti az adatkezelés és adatfeldolgozás kockázatait, beleértve a hatályos jogszabályi feltételek betartását is;
- A PPKE-hez bekerülő, illetve ott keletkező adatok, információk informatikai rendszere(ke)n történő adatfeldolgozásával szemben támasztott biztonsági követelmények rögzítése;
- Az adatbiztonsággal kapcsolatos szerepek, felelősségi és jogkörök rögzítése;
- Az informatikai berendezések, hálózati eszközök (hardver) és alkalmazási rendszerek (szoftver) biztonságának elősegítése;
- Egyértelműen meghatározni a PPKE-n igénybe vehető informatikai szolgáltatásokat, ezen szolgáltatások határait és a hozzá kapcsolódó felelősségeket;
- Hatékonyan karbantartható és naprakész keretet biztosítson a szabályozásoknak.

2. Az Informatikai szabályzat hatálya

Az IT-SZ hatálya kiterjed a PPKE minden információkezeléssel és -feldolgozással kapcsolatos folyamatára és tevékenységére vagy támogatásukban résztvevő informatikai eszközökre, illetve azok elhelyezésére szolgáló létesítményekre.

Egyaránt vonatkozik a PPKE tulajdonában vagy használatában lévő informatikai rendszerekben előforduló adatokra, információkra, a PPKE Informatikai rendszereinek teljes életciklusára, beleértve (tervezés, fejlesztés, beszerzés, bevezetés, üzemeltetés, kivezetés).

2.1. Az Informatikai szabályzat személyi hatálya

Az IT-SZ szabályzat személyi hatálya kiterjed:

- A PPKE valamennyi Informatikát alkalmazó vagy az informatikai környezetében működő szervezeti egységre (Intézmények-re).
- A PPKE valamennyi munkavállalójára és felhasználójára (oktatók, óradók, kutatók, hallgatók, adminisztratív dolgozók, üzemeltetők, stb.)
- A PPKE informatikai rendszerével, szolgáltatásaival kapcsolatban a PPKE szerződéses jogviszonyban álló természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban: külső személy), a velük kötött szerződésben, illetve a titoktartási nyilatkozatban rögzített mértékben.
- A PPKE-vel felhasználói jogviszonyban lévő regisztrált, informatikát használó felhasználójára.
- A PPKE Informatikai Osztály (továbbiakban IT) biztosítja az informatikai infrastruktúrát és támogatja a PPKE-en folyó informatikai oktatást, kutatást, innovációt a jelen szabályzat keretei között.

2.2. Az Informatikai szabályzat tárgyi hatálya

Az IT-SZ szabályzat tárgyi hatálya kiterjed a PPKE:

- Adataira,
- Adathordozóira,
- Alkalmazásaira,
- Folyamataira,
- Alap szoftvereire,
- Az IT rendszerre, és az infrastrukturális környezetre,
- A környezeti infrastruktúra elemeire, objektumaira,
- Az Informatikai eszközökre (notebook, desktop, stb.)
- A jogszabályoknak és a külső követelményeknek való megfelelésre.

2.3. Az informatikai szabályzat területi hatálya

Az IT-SZ szabályzat területi hatálya kiterjed az informatikai erőforrások üzemelési helyszíneire:

- A PPKE intézményeire és telephelyeire,
- A külső szolgáltatók által, a PPKE-nek nyújtott szolgáltatásaiban érintett helyszíneire.

2.4. Az Informatikai szabályzat időbeli hatálya

Jelen IT-SZ szabályzat a PPKE Egyetemi Tanács (továbbiakban: ET) által történő elfogadásával lép hatályba, a dokumentumban foglalt feladatok, folyamatok és szabályok ezen időponttól alkalmazandóak. Mindaddig hatályos, amíg új verziót nem fogad el az ET vagy visszavonásra nem kerül. Jelen IT-SZ szabályzatot az ET módosíthatja.

Jelen IT-SZ szabályzat felülvizsgálatára az Informatikai Osztályvezető (Továbbiakban: ITO) irányításával évente egyszer kötelező jelleggel sor kerül. Minden évben felül kell vizsgálni, annak betarthatósága és aktualizálása szempontjából és értékelni kell, hogy megőrizte-e azon biztonsági fokozatát, amelyet előirányozott. Jelen szabályzatot módosítani kell, ha a felülvizsgálat eredménye, annak betarthatatlanságát vagy aktualizálatlanságát állapította meg, illetve a vizsgálaton kívül olyan

külső vagy belső környezeti változás történt, amely szükségessé teszi azt. Ezek a változások ugyancsak vizsgálatot vonhatnak maguk után, amennyiben nem egyértelmű a kivitelezendő változtatás az IT-SZ-re vonatkozó hatása. A szabályzat aktualizálásáért az ITO a felelős. Az IT-SZ-ben bekövetkezett módosításokról a hatályba lépést követő 2 héten belül minden szabályzat hatálya alá tartozó személyt értesíteni kell.

3. Kapcsolódó dokumentumok

Kapcsolódó szabályzatok, dokumentumok:

- PPKE Szervezeti és Működési Szabályzata (PPKE SZMSZ);
- PPKE Információbiztonsági Szabályzata (PPKE IBSZ);
- PPKE Informatikai Felhasználói Szabályzata (PPKE ITF-SZ);
- PPKE Adatvédelmi és Adatbiztonsági Szabályzata (PPKE AVBSZ);
- PPKE Információátadási Szabályzata (PPKE IASZ);
- PPKE Incidenskezelési Szabályzata (PPKE ITINC);
- PPKE Változáskezelési Szabályzata (PPKE ITVA);
- PPKE IT munkaköri leírásai;
- PPKE Információbiztonsági Politika
- PPKE Jelszókezelési szabályzat
- A Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzata (20/2004. (VI.21). IHM rendelet).
- PPKE szolgáltatás katalógus (pl. Neptun, SAP, Nexon, ECM).
- Üzemeltetési / felhasználói dokumentációk.
- Valamint az IT üzemeltetés – szabályozási utasításait (pl. IT folyamat szabályozások, jogosultság kezelés, DRP, mentési rend, BCP)
- Szolgáltatási szint vállalások (SLA – Service Level Agreement)
- PPKE IT stratégia
- PPKE IT stratégia
- Szervezeti Diagram

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

4. Általános rendelkezések

4.1. PPKE Informatikai szervezete és feladatai

Az IT-nak a PPKE szervezetében betöltött szerepét, felügyeletét a PPKE SZMSZ határozza meg. Az IT feladatait az Informatikai és Információbiztonsági Szabályzat tartalmazza.

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

Minden üzemeltetett rendszer esetében az informatikai szabályzatnak való megfelelés, folyamatok és szabályozások betartatása, az adott rendszert üzemeltető szervezeti egység vezetőjének felelőssége.

Az IT által biztosított szolgáltatások színvonalának felügyeletét, biztonságát és a szabályozások betartását az ITO mellett működő szolgáltatásmenedzser látja el.

A szolgáltatásmenedzser felelős a szolgáltató és a szolgáltatást igénybe vevője között a szolgáltatás tartalmának és egyéb rendelkezéseinek, paramétereinek egyeztetéséért, és a megállapodás betartásának ellenőrzéséért.

A szolgáltatásmenedzseri teendőket a szolgáltatás menedzser kinevezéséig az ITO látja el.

A nem IT üzemeltetésben álló IT rendszerek szakmai felügyeletét (pl. elkülönített kutatói szakrendszerek, egyedileg kialakított rendszerek) az azt üzemeltető szervezeti egység vezetője látja el.

Az ITO jogosult az egyes szolgáltatások, informatikai rendszerek IT szabályzatoknak való megfelelőség és betartás-ellenőrzésére.

4.3. Jogszabályi, törvényességi megfelelőség

A PPKE-n informatikai szolgáltatásainak igénybevétele során az elkövetett bűncselekményekért, illetve egyéb jogsértésekért (pl. az informatikai rendszerbe történő betörésből fakadó károkozás,

informatikai szabályozástok nem betartása, stb.) a szolgáltatást igénybe vevő büntetőjogi felelősséggel tartozik.

Az informatikai szolgáltatás üzemeltetője a jogszabályokban meghatározott dokumentumokat, nyilvántartásokat köteles vezetni, azok rendelkezésre állását köteles biztosítani.

Törvényes megkeresés alapján, a vonatkozó jogszabályi kereteknek megfelelve a PPKE minden, a bűncselekmény elkövetésének gyanúja alá eső felhasználó adatait, valamint a naplózott adatokat, az adatvédelmi tisztségviselő (továbbiakban: DPO) bevonásával a nyomozóhatóságnak kiszolgáltatja.

DPO elérhetősége: dpo@ppke.hu – címen keresztül közvetlenül elérhető, az incidensek és események bejelentésére vonatkozóan. A DPO-hoz tartoznak az adatvédelmi és adatkezelési szabályozások és ezzel kapcsolatos incidensek kezelésének lebonyolítása és tájékoztatása.

A szolgáltatások igénybe vevőit a jelen Informatikai Szabályzatban leírtak megsértése esetén az alábbi szankciókkal sújthatja:

- Szolgáltatás megtagadás (kizárás a szolgáltatásból)
- Az okozott anyagi kár megtérítése
- Polgári vagy büntető jogi feljelentések megtétele

A szolgáltatásokat igénybe vevők bármilyen szankcionálása csak akkor történhet meg, ha a szolgáltatás üzemeltetője dokumentálta a szankció elrendelését kiváltó eseményt, incidenst.

Ennek felelőse a szolgáltatást nyújtó szervezeti egység vezetője.

5. IT rendszerek biztonsági osztályai és besorolása

A PPKE IT által nyújtott szolgáltatások külön a PPKE_IT_Szolgáltatásai (szolgáltatás katalógus) című mellékletben találhatóak meg, ezen felül a szervezet számára fontos informatikai rendszerek, és a hozzá tartozó eszközparkok a következő besorolási szinteket határozza meg. Ebből a kiemelten a

legfontosabbak a kritikus rendszerek, melyek a szervezet működéséhez elengedhetetlenek. Erre vonatkozóan az incidenskezelés és változáskezelési szabályzatban megfogalmazott előírások a betartandók, amennyiben valamilyen nem várt esemény bekövetkezik a szervezetnél.

5.1. Kritikus rendszerek (A szintű besorolás)

A PPKE intézmény infrastruktúrája és informatikai alapszolgáltatások szempontjából kritikus rendszerek, melyek az üzlet folytonossági szabályzatban is meghatározásra kerülnek, azok a rendszerek, melyek a működés szempontjából nélkülözhetetlenek. Ezen rendszerek jelentik a legnagyobb kihívást a PPKE IT üzemeltetése számára, mert ezen rendszernek a mai kornak megfelelő biztonsági szempontból is naprakészen kell tartani. Melyhez különböző monitorozó és rendszerfelügyeleti megoldások is alkalmazásra kerülnek.

- Authentikációs rendszerek (LDAP – Lightweight Directory Access Protocol, AD – Active Directory) ezen rendszerek a tartomány számára a felhasználók bejelentkezését, nyilvántartását, és hozzáférhetőségét tartalmazzák, mely a működés szempontjából a legkritikusabb rendszer besorolást kapja.
- Határvédelmi (DMZ – Demilitarized Zone, Edge rendszerek) és a hálózati (network) forgalmat szolgáltató rendszerek (BSD, Távközlési szolgáltatók rendszerei – Internet, Telefonközpont, Bérelt vonal)
- Virtualizációs rendszerek, melyek a fizikai szerverekre épült réteget biztosítanak. A PPKE-nél két megoldás jellemző Microsoft alapú Hyper-V és a Linux-os rendszerekre vonatkozóan a KVM technológia.

Ezen rendszerek a PPKE infrastrukturális működését hivatottak biztosítani, melyek folyamatos rendszerfelügyeletet is igényelnek, mert ezen rendszerek rendelkezésre állása 7/24-es.

A PPKE intézmény működése szempontjából kritikus, a PPKE intézmény egészére kiterjedő rendszerek, melyek szenzitív, illetve (különleges) személyes adatokat tartalmaznak. Ezen információk és adatok a GDPR hatókörébe tartoznak, melyek bármilyen incidens bekövetkezése

esetén, kivizsgálásra kerülnek, adatveszteség és adatszivárgás szempontjából is. Ezen intézkedéseket a PPKE incidenskezelési szabályzata tartalmazza, melyeben az alkalmazandó folyamatok is rögzítve vannak. Ezen rendszerek így adatvédelmi szempontból kiemelt védelmet igényelnek (mind fizikai és mind szoftveres, biztonsági szempontból is). Ennek következménye, hogy ezen rendszerek monitorozása is elsődleges feladat a PPKE IT számára.

A PPKE intézményi szoftverek, melyek kritikus besorolással rendelkeznek:

- Bér – és Munkaügyi rendszer (NEXON – Nexon Kft.)
- Gazdasági, ügyviteli rendszer (SAP – SAP Hungary Kft.)
- Iktatási rendszer (Poszeidon – SDA DMS Zrt.)
- ECM / Alfresco dokumentumkezelő rendszer
- Tanulmányi rendszer (NEPTUN)
- Központi levelező kiszolgálók (Linux – Zimbra, Microsoft 365)
- Központi és tárhely-kiszolgálók (Szerverek, Storage-ek, NAS, CORE hálózati eszközök)

5.2. Kiemelt rendszerek (B szintű besorolás)

A PPKE intézmény működése szempontjából kritikus rendszerek, amelyek elsősorban technikai jellegűek, feladatokra, folyamatokra és szolgáltatásokra vonatkozóan. Ezen rendszereken tárolt adatok nem személyes jellegűek.

- Telekommunikációs hálózat (Internet, Intranet)
- Technológiai rendszerek
- Kiszolgáló rendszerek (Microsoft és Linux alapokon)
- Szerverszoba és géptermi rendszerek (pl. Hűtés, UPS, aggregátor, tartalék megoldások, backup, stb.)
- Kommunikációs rendszerek (Telefonközpontok, VoIP alapú rendszerek)
- Honlap szolgáltató rendszerek

5.3. Normál rendszerek (C szintű besorolás)

A PPKE intézmény azon rendszerei, melyek nem tartoznak az „A" vagy „B" kategóriába sorolt rendszerei közé, a teljes intézmény működése szempontjából nem kritikus, illetve az intézmény csak egyes bizonyos részeire (pl. PPKE intézmény karai-ra) kiterjedő olyan rendszerek, amelyek indítása / üzemeltetése / karbantartása során központi felülvizsgálat történik. Ezen rendszerekről és ezen használatáról, működéséről teljes körű dokumentáció készül:

- Interaktív kiszolgáló szerverek
- Kutató rendszerek alap és kiszolgáló infrastruktúrája
- Szuperszámítástechnikai (HPC – High Performance Computing) alap és kiszolgáló infrastruktúrája

5.4. Egyéb rendszerek (D szintű besorolás)

A PPEK intézmény azon rendszerei, melyek az előző három kategóriába nem sorolt rendszerek, és megjelölésük egyéb (D) jelzéssel ellátottak az IT szolgáltatásokra vonatkozóan. Ezen rendszerek működése az üzletfolytonosság szempontjából nem relevánsak.

6. Az Informatikai biztonsági követelmények a PPKE IT rendszerek szállítási szerződéseiben (BESZÁLLÍTÓK)

A PPKE-nél a szolgáltatásért felelős szervezeti egység vezetője felel azért, hogy a PPKE IT rendszereihez történő beszállítások során a szállítói szerződések minimálisan tartalmazzák az alábbi részeket:

- Hatályos jogszabályoknak teljeskörű megfelelés
- Átadás / átvételi jegyzőkönyv (szerződés melléklete)
- Kapcsolattartó neve és elérhetősége (Telefonszám, e-mail)
- Műszaki feltételek megléte
- Támogatási / garanciális feltételek

- A beszállítás (másnéven: projekt) menedzsmentje
- Jogi nyilatkozatok (Tulajdonjog, Szoftver használati jog, stb.)
- Biztonsági előírások
- Felelősségi körök elhatárolása
- Titoktartási nyilatkozat

A PPKE intézmény egyes, IT szolgáltatásaihoz kötődő szerződéseket a PPKE Pénzügyi és Számviteli Osztálya tartja nyilván, és kezeli ezeket. A PPKE IT Osztályának betekintési joga van ezekbe a szerződésekbe és tájékoztatási kötelezettsége van bármilyen PPKE IT területről érkező, kezdeményezett, szerződést érintő változás esetében.

6.1. A PPKE beszállítóival összefüggő információbiztonsági kockázatok azonosítása

A PPKE beszállítója és vagy külső partnere lehet:

- Kiszervezett (outsourcing) tevékenységet ellátó szervezet,
- Informatikai tanácsadó szervezet
- Egyéb szerződéses beszállító, illetve partner

A PPKE számára beszállítói tevékenységet végzővel szemben támasztott informatikai biztonsági követelmények nem lehetnek enyhébbek, mint a PPKE hatályos szabályzataiban meghatározott, illetve a PPKE-vel szemben támasztott jogszabályi követelmények. A beszállítói szerződésnek tartalmaznia kell a PPKE biztonsági és / vagy védelmi szabályzatában megfogalmazott általános elemeket. A szerződés megkötését párhuzamosan kísérnie kell egy intézkedési tervnek, amelyben az adatkezelés, az adatfeldolgozás vagy az adattárolás folyamatosságának biztosításához szükséges személyi, tárgyi és biztonsági követelmények érvényesülésére tett feladatokat kell megjeleníteni a PPKE üzletmenet folytonosságának biztosítása érdekében.

A PPKE beszállítóival kötött szerződéseit – az informatikai biztonsági követelmények szempontjából minden esetben az IBF – Információ Biztonsági Felelős (vagy ITO)-nek kell felülvizsgálnia, továbbá az észrevételeket meg kell vitatni az érintett szakterület és vagy szervezeti egység vezetőivel.

6.2. Az információbiztonság kezelése a beszállítókkal való kapcsolat során

A PPKE többféle módon biztosítja a kapcsolattartást a beszállítóival (személyes út, postai levelezés, e-mail, internet, stb.). A PPKE (személyes) adatainak jogszabályokban meghatározott, megfelelő kezelését minden esetben biztosítania kell. Ugyanígy gondoskodni kell az interneten érkező, és vagy továbbított, beszállítók által küldött és / vagy számukra küldött üzenetek megfelelő védelméről. Az adatokat illetéktelen személyektől elrejtve (titkosított csatornán) keresztül kell küldeni, illetve szállítani.

6.3. A biztonság kérdésének kezelése harmadik féllel kötött megállapodásokban

A harmadik felekkel kötött megállapodásokat, beleértve a PPKE információihoz, illetve információ-feldolgozó eszközeihez való hozzáférést, azok feldolgozását, kommunikálását, illetve kezelését, valamint termékeknek, illetve szolgáltatásoknak az információ-feldolgozó eszközökhöz való hozzáadását, valamennyi a PPKE által meghatározott biztonsági követelményt tartalmazniuk kell.

Harmadik fél részére az informatikai rendszeren történő munkavégzéshez hozzáférést csak a szerződésben rögzített munkához feltétlenül szükséges, és elégséges jogosultságokkal kell biztosítani, a megállapodás hatálya alatt.

A PPKE szerződéseiben rögzíteni kell azokat a feltételeket, amelyek alapján a szerződő beszállító, illetve partner magára nézve kötelezőnek ismeri el a PPKE-ra vonatkozó jogszabályi követelményrendszert, további a PPKE Információbiztonsági szabályzat előírtakat, beleértve a jelen PPK Informatikai szabályzatot is.

7. Az IT-rendszerek biztonsági ellenőrzése

Az ITO (Informatikai Osztály vezető) felelős azért, hogy az (A) szintű kritikus besorolású IT-rendszereket, teljeskörűen, naprakészen tartása a belső biztonsági vizsgálata dokumentált módon (belső felülvizsgálati jelentés) legalább háromévente – teljeskörűen – megtörténjen, figyelembe véve a mai kor által támasztott biztosági követelmények, és ajánlások betartását. Amennyiben szükséges, abban az esetben amennyiben érdemi változás történik mind a rendszerben, mind az átalános szabályzásokban, előírásokban és módszertanokban, abban az esetben kerüljön sor, külső, harmadik fél általi felülvizsgálatra. Ezen ponton a külső partner rendelkezzen a megfelelő és naprakész minősítésekkel, melynek köszönhetően a naprakészséget alá tudja támasztani. A felülvizsgálatok eredményei alapján az ITO rendel el teljeskörű és / vagy részleges javító, helyesbítő, továbbfejlesztő vagy éppen megelőző intézkedéseket, melyeket mindig az éppen soron következő belső és / vagy külső, harmadik fél általi felülvizsgálat során kell dokumentált módon visszaellenőrizni, és szükség esetén a méréseket elvégezni.

A nem az IT által üzemeltetett informatikai és kiszolgáló rendszerek esetében a tevékenység és/vagy szolgáltatás felelőse, vagy az adott szervezeti egység vezetője.

8. Szolgáltatásszint menedzsment

8.1. A szolgáltatásszint menedzsment folyamata

Bármilyen biztonsági kategóriába sorolt rendszer csak az ITO által vagy engedélyével üzemeltethető a PPKE-n belül. A szolgáltatás tartalmára a szolgáltatási megállapodásban az üzemeltető szervezeti egység vezetője tesz javaslatot, a szolgáltatás indíthatóságáról a megállapodási javaslat alapján az ITO dönt. Figyelembe véve a PPKE-n hatályba levő informatikai, információs és biztonsági szabályozásokat. Elutasító döntés esetén a javaslattevő 15 napon belül felszólalással élhet a Rektornál közvetlenül. Ilyen esetekben a végleges döntést az Egyetem Rektora határozza meg.

A PPKE-n központilag jóváhagyott szolgáltatásokat a PPKE IT a honlapján közzéteszi. Ezek a szolgáltatások („A", „B", „C" kategória szintű besorolása) ezek a PPKE hivatalosan auditált szolgáltatásinak tekintendőek. (Továbbiakban a IT szolgáltatás katalógusa, későbbiekben külön mellékletként található).

8.2. A szolgáltatási megállapodások (SLA – Service Level Agreement) tartalma

A PPKE IT által központilag nyújtott szolgáltatásokra szolgáltatási szint megállapodások készülnek (SLA – Service Level Agreement). A szolgáltatások nyújtása a megállapodások alapján történik. A hasonló paraméterekkel vállalt szolgáltatások esetében az egyes szolgáltatási szintek összevonthatóak. A központi egységes szint megállapított általános tartalma a következőkből áll:

- Szolgáltatás neve (Egyedi megnevezés)
- SLA pontos verziószáma
- Lezárás dátuma (Az SLA pontos lezárásának dátuma)
- Igénybe vevő és / vagy szolgáltató, beszállító, partner, jóváhagyó (A szolgáltatás igénybe vevője, vagy ezen szolgáltatások képviselője, beszállító illetve szolgáltató, illetve képviselője mellett a PPKE IT részéről a jóváhagyó megnevezése)

- Rövid lényegre törő szolgáltatás leírása, illetve összegzés (Pár mondatban meghatározott, röviden összefoglalva a szolgáltatás pontos célját és tartalmát.)
- Érvényességi idő / megszűnés dátuma, illetve oka (Ezen szolgáltatások érvényességének évenkénti felülvizsgálata, igény esetén a szolgáltatás meghosszabbítása)
- Aláírások (Név, Szervezeten belül betöltött pozíció, Dátum)
- Szolgáltatás leírása (Részletes megfogalmazás, Technikai leírás)
    - Kulcsfontosságú pontok azonosítása és definiálása
    - Felhasználók számára szükséges technikai paraméterek, és leírások
    - Szolgáltatás megfelelő priorizálása (A Kritikus besorolásútól a D egyéb besorolású szolgáltatási szintig – Jelen szabályzat 5.1 – 5.4. -es pontja alapján – kerül meghatározásra.
- Pontos szolgáltatási időszak meghatározása (pl. 24/7-es folyamatos mindennap elérhető szolgáltatás, illetve a munkaidőben meghatározott szolgáltatási időtartam, mely munkanapokon 8-16 között, illetve további egyedi meghatározások alapján kialakított időpontokban.)
- Szolgáltatás használatba vételének módja
    - Szolgáltatás igénybe vevők körének meghatározása és azonosítása
    - Szolgáltatás helyszínének pontos meghatározása (mely a szabályzat területi hatálya alá esik)
    - Szolgáltatás kapcsolattartója (Szolgáltatásgazda, szolgáltatás menedzser, szervezeti egység vezető, pontos elérhetősége (telefon, e-mail) – Kapcsolattartás módjának meghatározása és szolgáltatási reagálási idők meghatározása
    - Szolgáltatás igénylés módja
    - Szolgáltatás biztosítás átfutási időtartama (meghatározott időn belül)
    - Szolgáltatás feltételei (adott munkakör, adott tanszéki igény, szervezeti egység, képzettség, tanúsítvány, stb.)
    - Szolgáltatással kapcsolatos tájékoztatás módja (szóban, írásban, elektronikus, személyesen, postai úton)

- Szolgáltatás karbantartási időszakok (éves, és havi szinten meghatározva, előre tervezhető módon, pl. minden hónap első péntekén este 9 – től este 11 -ig.) A szolgáltatás karbantartása szabályozás szintjén a Változáskezelési szabályzatban érhető el.)
- Szolgáltatás rendelkezésre állása (% -os meghatározásban)
    - Szolgáltatásra vonatkozó mérés módjának meghatározása (Ticket, Monitoring mérések alapján)
- Szolgáltatás támogatása
    - Szolgáltatás tartalma, melyben meghatározásra kerülnek, a hozzáférési szintek is.
    - Szolgáltatás elérhetősége (elektronikus módon)
    - Rendelkezésre állás (SLA és A-D besorolási osztályozások alapján, illetve figyelembevételével)
- Incidenskezelés (Részletesen a PPKE IT Incidenskezelési szabályzatban kerül meghatározásra, mint melléklet.)
    - Incidensek bejelentésének módja, lehetősége és formai követelményei, elektronikus felületeken és szolgáltatásokon keresztül.
    - Incidenseknek feldolgozása mennyi időn belül kezdődik meg, elsődleges érintettségi szint meghatározása és biztonsági besorolás megfelelő azonosítás.
    - Incidens bekövetkezésének karbantartására, javítása fenn álló időablak rendelkezésre áll vagy sem, érintett-e kritikus A biztonsági besorolású rendszer, illetve érintett-e személyes adatt, ebben az eset a folyamat szempontjából a DPO értesítése és megfelelő eszkalációs folyamat végrehajtása, érintettek pontos és megfelelő értesítése, elektronikus, illetve az adatvédelmi szabályzatban meghatározott módon.
- Szolgáltatás teljesítménye és minőségének mérése (osztályozása, minőségi szintek meghatározása)
- Szolgáltatás optimális teljesítményadatok figyelembevétele és feldolgozása (pl. elérési idő, válasz idő, megoldási időkeret, hatékonyság, illetve ami értelmezhető az adott szolgáltatás esetében, stb.)

- Változáskezelési eljárások (Részletesen a PPKE IT Változáskezelési szabályzatban kerül meghatározására, mint melléklet.)
- IT és üzletmente folytonosság (Részletesen a PPKE IT BCP – Business Continuity Plan -ben kerül meghatározása.)
    - Kritikus rendszerek, besorolás alapján
    - Alapvető és CORE szolgáltatások működésének biztosítása
- IT és szolgáltatások katasztrófa és helyreállítási terve (Részletesen a PPKE IT DRP – Data Recovery Plan -ben kerül meghatározásra.)
    - Kritikus rendszerek mentésének és helyreállításának meghatározása
    - Helyreállítási tervek és mérési eredményeik
    - Off-site és Offline backup – mentési megoldások, tárolása és hozzáférhetősége
    - Helyreállítási idő és terv mérésének eredményének és tesztjének dokumentálása.
- Informatikai biztonság (Részletesen a PPKE IBSZ – Információbiztonsági szabályzatban kerülnek meghatározása – külön álló szabályzatként.)
- Szolgáltatások kötelező felülvizsgálatának ideje / időszaka / helye és érintettségi köre. (Az SLA felülvizsgálatára, módosítására, illetve a PPKE számára / általa nyújtott szolgáltatások nyújtásának alapvető, vagy biztonsági feltételeiben bekövetkezett érdemi változás esetében szükséges.)
- Szójegyzék (Részletesen a PPKE Információbiztosági szabályzatban kerülnek meghatározásra) – Azok a technikai, speciális kifejezések, amelyek szerepelnek az egyes szolgáltatásokban, SLA-ban, és pontos magyarázatra szorulnak az értelmezhetőség szempontjából.) – Eltérő gyártói (Microsoft, Cisco, Mikrotik, stb.) elnevezések használatából adódó különbségek kiküszöbölése.

A szolgáltatási szint megállapodás tartalma közös megegyezéssel változtatható, tekintettel a szolgáltatás jellegére, és írásos formában való dokumentálása a változtatásoknak.

Az egyedi, illetve speciális szolgáltatási igényekre vonatkozóan a szolgáltatást igénybe vevő és a PPKE IT külön megállapodást köthet, melyet írásban rögzítenek, a hatályban lévő szabályozásokat betartásának alkalmazásával és figyelembevételével.

8.3. SLA megfigyelés (monitoring), jelenés készítés és áttekintés (felülvizsgálat)

Az előre meghatározott és ütemezett (úgynevezett: tervezett) IT szolgáltatás-kieséseket, illetve a várható kieséseket, valamint a meghibásodás miatti kieséseket, - ide értve az incidenseket is – az SLA-ban meghatározott módon publikálni kell (elektronikus, írásos, szóban, stb.) módon, az események (incidens, tervezett karbantartás, változáskezelésnek megfelelő módosítás, rendkívüli „0-day"-es sérülékenységek azonnali biztonsági frissítései) a felhasználók – ide értve a PPKE intézmény hallgatóit és alkalmazottakat, és külsős személyeket is, megfelelő irányú kommunikáció az ITO feladata és felelőssége. Személyes adatok érintettsége esetén a DPO közreműködése is szükséges, a megfelelő felhasználói tájékoztatás érdekében.

Az SLA-kban megadott szolgáltatások kulcsparamétereinek monitorozásáért, és esetleges incidens észlelése vagy bekövetkezése során az adott szolgáltatást nyújtó szervezeti egység vezetője a felelős.

Az SLA-k tartalmazzák az adott szolgáltatás pontos monitorozási feltételeit és előfeltételeit. Az SLA-kban történt és rögzített méréseket a szolgáltatásért felelős szakmai vezetők tekintik át – egyes esetekben, az ITO közreműködését kérhetik. A monitorozás eredménye a szolgáltatás minőségének fejlesztését szolgálja, mely minőségbiztosítási eredmények alátámasztásához felhasználható, viszont az SLA jelentések nem szükségszerű része, viszont erősen ajánlott.

9. Incidenskezelés / Ügyfélszolgálat

A PPKE IT rendszerekre vonatkozó incidenskezelést bővebben a PPKE Incidenskezelési szabályzatban meghatározottak az irányadóak. Jelen szabályzat az Ügyfélszolgálati – Támogatás (support) szolgáltatásra tér ki, globális folyamatok meghatározását jelen szabályzat nem tartalmazza.

A PPKE IT Ügyfélszolgálata a TOPDESK szoftvert használja a felhasználói események nyilvántartására és kezelésére, ennek működése, használata és szabályozása a PPKE Incidenskezelési szabályzat részét képezi.

9.1. Incidens naplózása és incidensek kezelése

A PPKE számára támogatás (Support): Az adott szolgáltatás SLA-ban meghatározottak alapján nyújtja a szolgáltató, melyeben a szolgáltatások hatálya – mind a területi, tárgyi, személyi és időbeli hatályt figyelembe véve -meghatározásra került.

Az incidens-kezelés, naplózás: Az incidens kezelés és naplózás technikai támogató rendszere az IT szolgáltatás menedzsment rendszere (Továbbiakban: ITSM rendszer), ettől bármilyen mértékben való eltérés az SLA-ban foglaltak szerint lehetséges.

Az incidensek kezelését az ITSM rendszerben kialakított keretek között végzi a PPKE IT. Amennyiben az incidens elhárítással kapcsolatos információkat a PPKE IT ITSM rendszerétől eltérő rendszer (más szolgáltató, illetve beszállító által biztosított megoldás) tárolja, kezeli, alapvető elvárás a rendszerrel szemben az SLA alapján történő elszámoláshoz szükséges, a hiteles riport előállításának képessége. Az incidens kezelés adminisztrációs feladataiba az IT rendszerétől eltérő rendszer / megoldás csak az ITO jóváhagyásával lehetséges. Amennyiben a szolgáltató, illetve beszállító nem rendelkezik az ITO által elfogadott adminisztrációval, riport képességgel, a szolgáltatási szint paramétereire vonatkozóan, a szolgáltatás elfogadását az ITO megtagadhatja. (Részletesen a PPKE Incidenskezelési szabályzat hatályába tartozik.)

9.2. PPKE IT Ügyfélszolgálat (Service Desk) opciók és eljárások

A PPKE IT Ügyfélszolgálatán az incidensek, szolgáltatás igénylések bejelentése, tájékoztatás kérés, jogosultság igénylés – csak dokumentált módon -, az ITSM rendszerében történhet, az ott meghatározott tartalommal, egyéb esetben a kérés megoldását az ITO megtagadhatja, mert a hatályos szabályzat formai és technikai követelményei nem teljesülnek. – Természetesen nagyobb érintettségi incidens észlelése esetén, a megfelelő – gyors – proaktív megoldásra való törekvés az elsődleges.

A PPKE IT Ügyfélszolgálatának minden bejelentést egyedi azonosítóval ellátott módon, számon kell tartania. A bejelentő számára az ITSM rendszerben tájékoztatást kell biztosítani a bejelentés

életútjáról, folyamatáról és állapotáról. A bejelentések megőrzése és rendelkezésre állásának biztosítása a PPKE IT feladata, és legalább 5 éves időtartamra visszamenőleg elérhető és kereshető legyen.

A PPKE IT Ügyfélszolgálata – csak az IT hatáskörébe tartozó rendszerekkel összefüggő – műszaki problémákat old meg, a biztonsági besorolások alapján történő priorizálás után. Nem vesz részt harmadik féllel felmerült vitás kérdések rendezésében, nem lát el jogi képviseletet sem felperesi, sem alperesi oldalon. Ezen események nem tartoznak a PPKE IT hatáskörébe.

9.3. Incidensek osztályozása és prioritás hozzárendelés

A bejelentett események, illetve incidensek kezelésére a rendszer besorolásától („A – D") prioritási szinten (1. szint, 2. szint, 3. szint) kerül sor. A priorizálás az IT Ügyfélszolgálat feladata és felelőssége.

Több incidens bekövetkezése esetén, a magasabb szintű és magasabb biztonsági besorolású incidens elsőbbséget élvez, amit – egyes esetben az IT több személyét is bevonhatja, a hatékony incidens megoldásba és eszkalálásba.

10. Problémakezelés

10.1. Incidens, probléma és az ismert hiba kezelése

Az incidens- és problémakezeléssel megbízott PPKE IT szervezeti egység és / vagy munkacsoport és / vagy beszállító / szolgáltató automatikus incidens és / vagy probléma felderítő rendszereket üzemeltethet, és ennek megfelelő szankciókkal élhet, (mely szankciók a PPKE Incidenskezelési szabályzatban találhatók).

A szolgáltatási incidenseket, eseményeket és problémákat az üzemeltető személyzet, a felhasználók jelezhetik, illetve ahol erre lehetőség van és kiépített felderítő rendszer üzemel, ott automatikus jelzés is történhet.

A monitorozó és hálózatfigyelő (SIEM) rendszerek jelzéseit először a PPKE IT Üzemeltetés értékeli és minősíti. Amennyiben a jelzés, illetve esemény incidensnek minősíthető, akkor a PPKE IT Üzemeltetés elvégzi a bejelentés adminisztrációját az ITSM (TopDesk) rendszerben.

A visszatérő, több incidens kiváltó okaként megjelenő, és azonosítható problémákat, a probléma adatbázisba való felvétele történhet manuálisan – speciális esetben automatikusan, amit az üzemeltető személyzet vagy az IT Ügyfélszolgálat végez el. Az ismert visszatérő hibák kiszűrése, a hibafelvétel során történik meg.

Az adott szolgáltatáshoz tartozó és meghatározott időn túl fennálló ismert hibákat a PPKE IT a hivatalos információs csatornáin (levelezési lista, Weboldal, Portál, Intranet, ITSM rendszer, címlista) publikálja, amennyiben személyes adat is érintett, abban az esetben a DPO bevonása, és tájékoztatási is megtörténik. Ennek következtében a belső folyamatszabályozások kerülnek végrehajtásra, mely folyamatok a PPKE Incidenskezelési szabályzatban rögzítettek.

10.2. Trend – azonosítás és elemzés

Az SLA-kban előírt teljesítmény – mutatók (mérési eredmények) figyelése során a PPKE IT megfelelő csoportjainál statisztikai értelemben vett idősorok jönnek létre, melyek elemzése az adott

szolgáltatást nyújtó szervezeti egység vezetőjének feladata. Az ilyen mérési eredmények alapján képződő adatokat az ITO felhasználja, és szükség esetén fejlesztési, módosítási, tervezési irányokat határoz meg, az egyes projektek kijelölésekor.

10.3. Probléma megelőzése

Az egyes szolgáltatások üzemeltetőinek nem csak reaktív, hanem preventív és proaktív intézkedéseket is végezniük kell a szolgáltatások zavartalan működésének érdekében.

Ezek lehetnek általános, tervezett, javasolt és az adott szolgáltatásra jellemző feladatok:

- Igény szerinti újraindítás (szolgáltatásokba beragadó események feladatok, kinullázása, esetekben egy szolgáltatás újra indítása, objektumok törlése végett – másnéven reset, restart eljárás meghívása.)
- Szerver, illetve alkalmazásokra vonatkozó, javító csomagok (Service Pack), javítások (Patch), biztonsági frissítés (Security Update), Hotfix, Update, Konfigurációs frissítése, verzióváltás, szerepköri bővítések, funkciók és szolgáltatások hozzáadása.
- A jelszavak kezelése és hozzáférési azonosítók kódok megfelelő komplexitással, rendszeres idő közönként cseréje. (Részletesebben a PPKE Jelszókezelési szabályzatban kerül kifejtésre.)
- A naplóállományok (logok, dump, stb.) rendszeres kiértékelése.
- Személyzet és felhasználók, alkalmazottak oktatása, és képzése.

Egy esemény, incidens, kockázat vagy saját hatáskörben elvégzett védelmi – biztonsági – intézkedés bejelentésének elmulasztásából, illetve a saját – nem megfelelő – használatból következő károk (káresemények, incidensek, rendszerleállások, szolgáltatási kiesések) az adott szervezet egység felelősségi körében tartoznak.

11. Konfigurációkezelés

Minden a PPKE-n elérhető szolgáltatás és szolgáltató rendszer esetében az üzemeltetőknek rendelkeznie kell a szolgáltatáshoz szükséges információval, hardver, szoftver komponensekről, kiegészítőkről (csomagok, driverek, egyedi fejlesztési alkalmazás csomagok), valamint azok konfigurációjáról (röviden: üzemeltető dokumentáció).

A szolgáltatásért felelős szervezeti egység vezető feladata dokumentálni a gyártó (vendor) által javasolt, valamint a rendelkezésre álló infrastruktúra paramétereit, előfeltételeit és gondoskodni kell ezek összhangjáról, működéséről. A szükséges változtatásokról szóló javaslat a tervezés részét kell, hogy képezze.

Bizonyos szolgáltatáscsoportok azonos alapinfrastruktúrán valósulnak meg, ezért az egyes szolgáltatásokhoz csak speciális, hozzá tartozó infrastruktúra elemeket szükséges dokumentálni, a közös infrastruktúra egyszeri dokumentálásán túl.

A nem már nem szükséges és továbbiakban megszűnő szolgáltatási igényekről a PPKE IT Ügyfélszolgálatát haladéktalanul tájékoztatni kell, mert ezen szolgáltatások korlátozására vonatkozó és kivezetésre alkalmazandó folyamatokat kell elvégezniük.

11.1. A konfigurációkezelés (CMDB)

Az adott rendszer üzemeltetőjének minden szolgáltatás és szolgáltató rendszer esetében időrendben vezetnie kell a szolgáltatásban érintett komponenseket (konfigurációs elem, CI) leíró adatbázist. Ezen konfigurációs adatbázis elkészítése és naprakészen tartása külön részét képezi a szabályzatoknak, mely működésének és vezetésének szabályozása külön mellékletként érhető el.

Minden változás esetén az alábbiakat kell megadni:

- A változó komponensek egyértelmű azonosítását lehetővé tevő adatok (azonosítók)
- A változás szükségességének indokai (biztonsági, funkció fejlesztés)
- A tesztelésre vonatkozó adatok, bele értve az infrastrukturális környezetet is

- Az aktuális visszaállítási teendőket, forgatókönyveket, tartalmazó információkat / hivatkozást is tartalmaznia kell a konfiguráció bejegyzésnek (whitepaper)

12. Változáskezelés

A PPKE IT-n található változáskezelést részletesen, a PPKE Változáskezelési szabályzat tartalmazza, melyből jelen szabályzat kivonati elemeket tartalmaz.

12.1. Központosított változás kezelés és felügyelet

Az Informatikai rendszerekre vonatkozó változás kezelés és felügyeletet a PPKE IT látja el, melynek kibővített és részletes folyamatát a PPKE Változáskezelési szabályzat tartalmazza.

12.2. Változáskezelési folyamatok

A központi változás kezelés felügyelete és folyamata:

Amennyiben nem a PPKE IT Üzemeltetésében, de a PPKE szervezeti egység üzemeltetésében álló rendszerek esetében az adott szolgáltatás üzemeltetője a változtatás (Change Management) megkezdése előtt köteles konzultálni a rendszerek kialakítása és jelentős változtatás esetében az ITO-val (előzetes megállapodás szerint az IT szakterület vezetőjével), melynek köszönhetően elkerülhető a „CORE" rendszert érintő esetleges érintettség.

Jelentős változtatás alatt értjük azokat a változásokat, változtatásokat, amelyek a rendszerek és kapcsolódó IT infrastruktúrák és szolgáltatások biztonságára, konzisztens állapotára (rendelkezés állásra, üzletfolytonosságra, bizalmasságra és sérthetetlenségére, integritására), adatvédelmi és adatbiztonsági előírásoknak való megfelelésére, erőforrás igényére, üzemeltetési feltételeire kihatással bírnak.

A PPKE IT-vel való konzultáció a tervezési fázisban, a bevezetési fázisban és annak lezárásakor is kötelező a PPKE-n működő IT Infrastruktúra integrált fejlesztéseinek fenntartása céljából.

Külső szolgálató és / vagy beszállító nem végezhet változtatást semmilyen éles rendszerben, kivéve ez alól amikor a PPKE változás jóváhagyására meghatalmazott, előzetesen megállapodott kapcsolattartója ezt engedélyezi, illetve a változáskezelés szabályzatban megfogalmazott előírások, folyamatok betartását is alkalmazza.

A PPKE által üzemeltetett fejlesztői és teszt rendszerben a változtatások a szakterületi vezető iránymutatásai szerint, megállapodott célok és irányelvek menték történhetnek külső szolgáltató, illetve beszállító részéről is.

A rendszeres, üzemeltetési gyakorlat tevékenységébe tartozó változások végrehajtása a szakterületi vezető, illetve a szervezeti egység vezető jóváhagyásával történhet meg, amely lehet vagy egyszeri, vagy az adott feladatra vonatkozó folyamatos érvényű jóváhagyás.

Amennyiben a nem rendszeres üzemeltetési gyakorlat részét képező változások (különös tekintettel a szolgáltatás rendelkezésre állására jelentős kockázattal bíró változtatásokra), csak az ITO jóváhagyásával történhetnek meg.

Az „A" és „B" biztonsági besorolású üzleti rendszerek esetében az éles, teszt és fejlesztői környezet kialakítása kötelező. Biztosítani kell a mentési megoldások működését, és ezen mentési megoldásokból történő visszaállítások sikerességének állapotát. Éles – produktív – rendszerben csak tesztelés után végezhető el változás. Kivételes esetben az ITO engedélyével történhet az éles rendszerben változtatás, ennek a folyamatát dokumentálni kell, esetleges nem várt esemény bekövetkezése estén a gyors reagálás végett.

Az engedélyezett változtatásokat (hardver, szoftver, adatbázis, stb.) a szolgáltatás üzemeltetője az üzemeltetési leírásban foglaltak alapján hajtja végre, sikeres végrehajtás esetén a rendszer leírásában azt megfelelően dokumentálja.

12.3. Szerepkörök és felelősségek

Amennyiben nem a PPKE IT biztosította szolgáltatások esetében a változások felelőse a szolgáltatás üzemeltetője.

A PPKE IT biztosított szolgáltatások esetében a változás és változtatás felelőse a szolgáltatási szakterületi vezetője, illetve a szervezeti egység vezetője. Az ITO változás és változtatás, illetve szolgáltatás kérés esetén a tervezésbe és jóváhagyásba történő bevonása a szakterületi vezető, illetve szervezeti egység vezető felelőssége. Az ITO bevonásával történő változások és változtatások felelőse az ITO.

Külső szolgáltató és / vagy beszállító üzemeltetésben (vagy közreműködő üzemeltetésben) álló szolgáltatások esetében a felelősségi határokat és a felelősségek meghatározását az erre vonatkozó SLA megállapodás kell, hogy tartalmazza.

A változást végrehajtó felelős minden olyan beavatkozásért, amely nem a jóváhagyott gyakorlat vagy folyamat mentén, nem a jóváhagyott módon történt, és azoknak a változásoknak, illetve változtatásoknak az esetében, amelyek során a rendszer-üzemeltetési leírása nem lett betartva.

13. Kiadáskezelés (Új szolgáltatás indítása – RELEASE)

A rendszer megvalósítását és dokumentálását, valamint a szolgáltatás tesztelését az IT szolgáltatás-menedzsere ellenőrzi – egyesesetekben az ITO. A sikeres tesztüzem után a szolgáltatás üzembe állítását az ITO engedélyezi.

A „A" és „B" besorolású kategóriába tartozó rendszerek esetében a szolgáltatás elindításának feltétele, hogy az ITO jóváhagyja az SLA-t, az üzemeltetési dokumentációt, a rendszerkonfigurációt (CMDB) és a változáskezelés folyamatot (Change Mangement – Részletesen a PPKE Változáskezelési szabályzatban).

13.1. Terítés és implementáció

Minden a PPKE IT által működtetett szolgáltatás esetén az ITSM rendszer felülete nyújt tájékoztatást, valamint az IT e-mailben juttatja el a fontosabb információkat az érintetteknek, azon hardver és

szoftver elemek (kliensek) listájáról és elérhetőségéről, amelyek a szolgáltatás igénybevételéhez szükségesek.

A PPKE IT központosított szoftver disztribúciós és üzemeltetési céllal felügyeleti szolgáltatást és védelmi megoldásokat is nyújt a felhasználók számára.

13.2. A hiteles szoftver tár és licence kezelés

A PPKE IT feladata a szoftverek ésszerű beszerzésének és felhasználásának biztosítása. Jelen szabályzatban szoftvernek tekintendő a licence igazolás, és az úgynevezett egyéb szoftver használati megállapodás, és a gyártói (vendor) támogatói megállapodás is.

Amennyiben nem a Központi PPKE IT által üzemeltetett szoftvert üzemeltetője köteles a PPKE IT részére az általa üzemeltetetett és / vagy használt szoftverekről tájékoztatást adni. A tájékoztatás pontosan meghatározott tartalommal történik. A tájékoztatást a PPKE IT igényelheti. Amennyiben olyan kutatási célhardver részét képező szoftver, amely kizárólagosan az eszközhöz köthető, és egyéb területi felhasználása nem lehetséges, abban az esetben nem jár tájékoztatási kötelezettség.

A szoftverek rendelkezésre állásának, nyilvántartásának és jogszerű használatának biztosítása az üzemeltető szervezeti egység vezetőjének felelőssége.

Minden új szoftver beszerzést a PPKE IT-nak véleményezni szükséges, függetlenül a beszerzés forrásától, módjától. Szoftver leltári nyilvántartásba vétele, raktári kiadás, üzembe helyezése csak a PPKE IT tudomásával és jóváhagyásával történhet.

A központi beszerzésű szoftverek esetében az egyes szakágak, illetve szervezeti egységek vezetői központilag hozzáférhető módon tárolják és karbantartják a központilag beszerzett szoftverek eredeti példányait, licence és telepítő csomagjait.

A szakterületi vezető, illetve a szervezeti egység vezető felelőssége:

- Legfrissebb verziók letöltése, a csomagok és telepítők frissítése
- Patchek, hotfixek, javítások, biztonsági javítások és frissítések letöltése és közzététele

- Csomagokon, telepítőn, frissítéseken, megfelelő mai kornak megfelelő kártékonykód-ellenőrzés végrehajtása, - esemény esetén jelentés és tájékoztatás a PPKE IT Ügyfélszolgálata felé
- Hozzáférési jogosultságok kezelése (Szükség esetén: PPKE Jogosultságkezelési szabályzatban foglaltak alapján)

14. IT Szolgáltatásfolytonosság biztosítása (BPC -Business Continuity Plan)

A PPKE-n az IT szolgáltatásfolytonosság biztosítsa, részeletesen a PPKE IT BCP terven kerül meghatározásra, mely tartalmazza a „core" szolgáltatások működésbiztosításának a folyamatát.

14.1. Kockázatkezelés

A PPKE IT-n elérhető „core" szolgáltatásokra vonatkozó kockázatelemzés részletessége nem része jelen szabályzatnak, bővebb információ a PPKE IT Kockázatelemzés – ben található, a kritikus rendszerek azonosításával együtt.

Minden „A" és „B" besorolású kategóriába eső rendszer esetében, melyek kiemelt kockázati besorolásúak, rendelkezni kell olyan kockázatelemzéssel, ami a rendszer által nyújtott szolgáltatások részleges vagy teljes kimaradásának a PPKE intézmény működőképességére tett hatásait tartalmazza.

Külön kell kezelni a szolgáltatás elérhetetlenségéből, illetőleg az adatbázis sérüléséből származó hatásokat, mert külön érintettségi hatáskörrel rendelkeznek.

A Kockázatelemzési dokumentum előállítása és karbantartása az üzleti terület felelőssége, az ITO és az Adatvédelmi tisztségviselő (DPO – Data Protection Officer) közreműködésével történik.

14.2. Üzleti (működési – folytonossági) hatáselemzés

Minden „A" és „B" besorolású kategóriába eső rendszer esetében, melyek kiemelt kockázati besorolásúak, rendelkezni kell olyan kockázatelemzéssel, ami a rendszer által nyújtott szolgáltatások részleges vagy teljes kimaradásának a PPKE intézmény működőképességére tett hatásait tartalmazza. – Ezen dokumentum a hatásokra tér ki a rendszer érintettségét figyelembe véve.

A kockázatelemzési dokumentum előállítása és karbantartása az üzleti terület képviselőinek felelőssége, a PPKE IT és a DPO közreműködésével készül.

14.3. Vészhelyzeti forgatókönyvek (DRP – Data Recovery Plan) és az IT szolgáltatásfolytonossági terv (BCP)

A PPKE-n az IT Vészhelyzeti forgatókönyve biztosítja a helyreállítási terveket, mely részletesen a PPKE IT DRP tervben kerül meghatározásra.

A szolgáltató és kiszolgáló rendszerek üzemeltetési leírásának tartalmaznia kell az alábbi teendőket és folyamatokat (másnéven a BCP – Üzletfolytonossági terv):

- Milyen helyettesítési lehetőségek állnak rendelkezésre (műszaki, technológiai és szervezeti megoldások) vagy az adott szolgáltatás kiesése esetén (Vészhelyzet – Katasztrófa)
- Milyen intézkedéseket kell megtenni, ennek pontos naprakész tesztelt és ellenőrzött folyamatnak kell lennie az üzletmenet folytonosság / működési folytonosság fenntartása érdekében
- Kik azok a személyek, akik intézkedésre jogosultak, milyen feladatok és folyamatok vonatkoznak rájuk a megfelelő működés biztosításához
- Kik azok a személyek, akiket értesíteni kell (értesítési lánc) – Besorolástól, állapottól, eseménytől, és hatástól függően.

A BCP – Üzletfolytonossági terv elkészítésének és karbantartásának felelőse az ITO.

15. Rendelkezésre-állás biztosítása (Későbbiekben: Magasrendelkezésre állás)

15.1. Rendelkezésre-állás, megbízhatóság, szervizelhetőség szintjei

A PPKE működése szempontjából kritikus szolgáltatások az („A") és („B") kategóriába besorolt rendszerek, ezek esetében az ITO határozza meg a rendelkezésre állási idő intervallumot, amiben a szolgáltatásnak elérhetőnek kell lennie, és ez az üzleti területtel egyeztetve kerül meghatározásra.

15.2. Karbantarthatóság, biztonsági szintek

Az adott szolgáltatás üzemeltetőinek a szolgáltatás aktuális rendszertervében (PPKE IT Szolgáltatási jegyzék)-ben, fel kell tüntetni azon műszaki megoldásokat, amelyek a szolgáltatás meghatározott elérési paramétereit hivatottak biztosítani (pl. Redundancia, Failover Cluster, HA megoldásokat biztosító rendszerek és szolgáltatások). A PPKE IT-nek a szolgáltatás következő éves fejlesztési tervében rögzíteniük kell az elavult, nem szervizelhető, fejleszthető komponenseket, és azok cseréjére vonatkozó javaslatokat.

15.3. Magas rendelkezésre állású rendszer tervezése

Az ITO a felelős a különböző kritikussági osztály besorolású alkalmazások és azok műszaki és megfelelő működésének tervezéséért.

A műszaki tervezéseket és javaslatokat (költségbecsléssel kiegészítve) a Gazdasági Főigazgatónak nyújtja be a szolgáltatás által érintett szervezeti egység / osztály / kar / személyek támogatásával.

16. Pénzügyi irányítás

Az ITO felelősségi körébe eső szolgáltatások esetében a pénzügyi tervezés és irányítás éves ciklusa az évben aktuális, tervezésre vonatkozó Gazdasági Főigazgatói utasításában foglaltak szerint történik.

Átalános gyakorlata:

- Technikai és műszaki tervezés: (a pénzügyi évet megelőző szeptember – október, PPKE IT szakterületi vezetők)
- Belső költségvetés és éves projektterv összeállítása: (október – november, érintett végrehajtó személy: ITO)
- Költségvetés és projekttervek véglegesítése: (a pénzügyi évet megelőző december, érintett végrehajtó személy: ITO)
- Egyetemi szintű költségvetési fordulók: (tárgyév januárjában, érintett végrehajtó személy: ITO)

16.1. Költségvetés

A PPKE IT a tervezési időszakban beterjeszti azon tételeket összegekkel ellátva, amelyek a központi szolgáltatások fenntartásához szükségesek. A költségvetési terv tartalmazza a fix üzemeltetési költségeket (pl. távközlési költségek, a szoftver támogatási és licence költségek).

A PPKE IT a tervezési időszakban beterjeszti a tervezett új szolgáltatásokat, fejlesztéseket, projekt jellegű beruházások tételeit és forrásigényét.

Ezek a tételek összegezve adják a PPKE IT következő éves költségvetését.

16.2. Informatikai számvitel

Az egyes PPKE központi IT fejlesztési projektek projekt alapú gazdálkodásáért az ITO a felelős. Más szervezeti egységek által indított és felügyelt projektek a PPKE IT vonatkozású költséggazdálkodásáért az adott szervezeti egység vezetője felel.

Az ITO készíti a PPKE központi IT projekt költségvetést, a költségvetés kidolgozásáért felelős szervezeti egységek támogatásával, iránymutatása mentén. Az időszaki forrás-felhasználási jelentéseket, nyilvántartásokat a PPKE IT az illetékes szervezeti egységtől kérheti.

A PPKE IT a PPKE pénzügyi szervezeteivel együttműködve látja el feladatát, de alapvetően az IT műszaki és technológiai tevékenységet lát el. A PPKE IT a szolgáltatásaiban érintett eszközüket az IT Üzemeltetési szempontjai szerint, műszaki paraméterek alapján tartja nyilván és kezeli.

A PPKE IT az egyes beszerzések felett szakmai felügyeletet gyakorol. Az IT a mindenkori beszerzési szabályzat szerint jár el.

16.3. Költségterhelési opciók

Az ITO véleményezési joggal bír az IT típusú beszerzések felett. A pénzügyi terhelés és kontrolling besorolás a pénzügyi szabályzat szerint történik. A PPKE IT által nem elfogadott vagy nem ismert beszerzések minden költségvonzata a beszerzőt terhelik.

17. Kapacitáskezelés

Az ITO a felelős azért, hogy a felhasználóktól beérkező igények, a szolgáltatói környezet változása, a technikai fejlődés figyelembevételével tervezze, és az elfogadott PPKE egyetemi költségvetés szerint biztosítsa a PPKE működéséhez szükséges IT-kapacitásokat.

17.1. Kapacitástervezés

A szolgáltatást biztosító rendszer és infrastruktúra várható terhelését az üzemeltető szervezeti egység vagy a PPKE IT szakterület az eddigi használati trendek alapján évente előre jelzi a következő éves időtartamra. A beérkező információk, alapján a PPKE központi IT kapacitások tervezését az IT hajtaja végre és végzi el.

Amennyiben nem a PPKE központi IT által tervezett informatikai kiszolgáló beruházások esetében az üzemeltetéshez szükséges kapacitásokat az Üzemeltetési osztály biztosítja (pl. Szerverszobai szünetmentes, áramellátás, hűtés és légkondicionáló használata, stb.) A várható kapacitás igényt, tervezett fejlesztéseket az Üzemeltetési osztálynak és a beruházónak egyeztetnie kell az ITO-val vagy a kijelölt szervezeti egység / szakterületi vezetővel.

17.2. A kapacitásterv

Az elkészített következő évi terhelés előrejelzés alapján az üzemeltetők kapacitástervet készítenek, aminek tartalmaznia kell az összes olyan rendszerkomponens listáját, amit a szolgáltatás zavartalan biztosítása érdekében a várható terhelést figyelembe véve módosítani vagy bővíteni kell.

17.3. A kapacitáskezelés

A PPKE IT által üzemeltetett szolgáltatások esetében az üzemeltető szervezeti egység / szakág / csoport vezetője az adott szolgáltatás kapacitásterve alapján fejlesztési tervet készít, melyeket a következő évi költségvetés tervezésével együtt benyújtja az ITO-nak.

A kapacitástervek és a fejlesztési tervek elfogadásáról az ITO szolgáltatásonként külön, nyilvános döntést hoz.

18. Általános felhasználói szabályok

Az általános felhasználói szabályokat részletese, a külön PPKE IT Felhasználói szabályzat tartalmazza.

A kliensoldali informatikai infrastruktúra működésének és használatának rendje:

1. A PPKE kliens oldali informatikai eszközeinek beszerzését a PPKE IT konzultatív, véleményező, koordináló feladatot lát el a mindenkori beszerzési szabályzat szerint.
2. Műszaki, szakmai és technológiai szempontból alkalmatlan eszközöknek a PPKE Informatikai infrastruktúrájához való illesztését a PPKE IT megtagadhatja.
3. Tömeges (kari vagy egyetemi szintű) kliens oldali hardver, szoftver vagy szolgáltatás beszerzése esetén a beszerzés műszaki vonatkozásait a PPKE IT irányítja. A gazdálkodó szervezeti egységek egyedi beszerzéseiket maguk kezdeményezik és bonyolítják.
4. A beszerzett eszközök első üzembe helyezését, a PPKE Informatikai infrastruktúrába való illesztését és üzemeltetését a PPKE IT szakemberei végzik, egyéb szerződésben foglalt feltételek hiányában (pl. SAP)
5. Meghibásodás, rendellenes használat, és működés esetén a PPKE IT szakembereit kell értesíteni, akik intézkednek a hibaelhárításról. A jogosulatlan hibaelhárításból eredő következményekért, károkért a jogosulatlan hibaelhárítást végző személy kártérítési felelősséggel tartozik.
6. A személyi számítógépekre a felhasználó által telepített szoftverek működéséért, annak következményeiért és jogtisztaságáért a felhasználó a felelős.
7. A szolgáltatásokkal kapcsolatos hiba bejelentésekekel, támogatás igénybevételével vagy információ kérési céllal a PPKE IT Ügyfélszolgálati (HelpDesk) munkatársai kereshetőek, az alábbi elérhetőségen: https://helpdesk.ppke.hu
8. PPKE IT szolgáltatással kapcsolatos panasz kezelése céljából az ITO-hoz vagy a feletteséhez a Gazdasági Főigazgatóhoz lehet fordulni.
9. A PPKE IT szolgáltatásokhoz kapcsolódó folyamatait, mint pl. igény vagy hiba bejelentés kezelése, a vonatkozó IT Szabályzat és leírás tartalmazza.
10. A hozzáférés igénylés részleteit a Jogosultságkezelési szabályzat tartalmazza.

19. Általános üzemeltetői szabályok

A PPKE IT a tevékenységét a szakma legnagyobb gyakorlatainak iránymutatásával és módszertanainak betartásával végzi. Többek között (ITIL, COBIT, ISO 27001)

Az üzemeltetési vállalások alapját a szolgáltatási szint megállapodások képezik. Az SLA-k a szolgáltatást igénybe vevő szervezetek és a PPKE IT között köttetnek.

A működés szabályozását a PPKE IT vonatkozó belső szabályzatai, folyamat leírások, működési utasítások tartalmazzák. Az IT belső szabályozás az IT vezető (ITO) feladata és hatásköre. Az SLA alapú működés-fejlesztés részleteit az IT fejlesztési terv tartalmazza.

20. A PPKE Információ biztonsági politikája

A PPKE információbiztonsági politikáját a PPKE Informatikai Biztonsági Szabályzat (PPKE IBSZ) tartalmazza.

21. A PPKE IT által nyújtott informatikai szolgáltatások

A PPKE IT által nyújtott szolgáltatásokat a PPKE Szolgáltatás katalógus tartalmazza.

A PPKE Szolgáltatási katalógus bizonyos elemei automatikusan rendelkezésre állnak a felhasználóknak, a jogviszony létrejöttét követően, míg más szolgáltatások elérése igénylés útján érhetőek csak el.

22. Záró rendelkezések

1. A Pázmány Péter Katolikus Egyetem Informatikai Szabályzatát az Egyetemi Tanács 45/2023. (VI.15.) számú határozatával jóváhagyta.
2. A jelen szabályzat a kihirdetését követő napon lép hatályba.

Budapest, 2023. június 29.

Dr. Kuminetz Géza György
rektor
Pázmány Péter Katolikus Egyetem