PÁZMÁNY

1635

PÁZMÁNY PÉTER KATOLIKUS EGYETEM LEVELEZÉSBIZTONSÁGI SZABÁLYZAT

Hatályos: 2026. május 11. napjától

Tartalomjegyzék

1. Bevezetés

A digitalizáció rohamos fejlődése és az online kommunikáció mindennapjaink szerves részévé válása mellett az egyetemek számára kiemelt fontosságú egy modern, biztonságos és megbízható levelezési rendszer alkalmazása. A Microsoft 365 platformja nemcsak az oktatási és adminisztratív tevékenységek támogatására alkalmas, hanem a kutatási, kommunikációs és együttműködési folyamatok hatékony kezelésére is. Az egyetem által használt Microsoft 365 levelezési rendszer az oktatók, hallgatók és adminisztratív dolgozók számára egységes keretet biztosít a napi feladataik elvégzéséhez, az információk biztonságos tárolásához és megosztásához, valamint a globális kommunikáció fenntartásához.

Ez a szabályzat átfogóan szabályozza a levelezési rendszer használatának módját, a biztonsági és adatvédelmi előírásokat, valamint az egyetemi ügyintézését hatékonyságát és biztonságát elősegítő felhasználói kötelezettségeket. Egyaránt érinti a hallgatók, alkalmazottak és vendégfelhasználók levelezési tevékenységét, és biztosítja, a rendszer jogszabályi megfelelőségét, különös tekintettel az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló rendeletnek (a továbbiakban: általános adatvédelmi rendelet) való megfelelőséget.

A szabályzat céljai a következők:

1. **Hatékony működés biztosítása:**

   Az egyetem által nyújtott levelezési szolgáltatások célja, hogy elősegítse az oktatási, kutatási és adminisztratív feladatok gördülékeny lebonyolítását. A Microsoft 365 modern technológiai megoldásainak segítségével a felhasználók gyorsan és egyszerűen kezelhetik e-mailjeiket, megoszthatják dokumentumaikat, és részt vehetnek virtuális megbeszéléseken.

2. **Adatbiztonság garantálása:**

   A digitális kommunikáció biztonsága napjaink egyik legnagyobb kihívása. A szabályzat célja, hogy biztosítsa a felhasználók adatainak védelmét, minimalizálja a kiberbiztonsági

kockázatokat, és garantálja a személyes és érzékeny információk titkosságát. Az egyetemi ügyrend biztonságos és hatékony működése érdekében, a PPKE által biztosított e-mail fiókkal rendelkező személyek kötelesek munkájuk és egyéb egyetemen belüli ügyintézésük során egyetemi e-mail címüket használni. Egyéb, nem @ppke.hu, @kar.ppke.hu vagy @it.ppke.hu e-mail cím használata nem megengedett.

3. **Jogszabályi megfeleltetés:**

A PPKE elkötelezett a releváns jogszabályoknak, különösen az általános adatvédelmi rendeletnek való megfelelőség biztosításában. A szabályzat részletesen kitér az adatkezelésre és -tárolásra vonatkozó előírásokra, biztosítva a jogszabályokkal való teljes összhangot.

4. **Felhasználói felelősség meghatározása:**

A szabályzat egyértelműen rögzíti a felhasználók jogait és kötelezettségeit, beleértve a rendszer biztonságos és etikus használatát, ez segít megelőzni az esetleges visszaéléseket és szabálytalanságokat.

5. **Tudatosítás és oktatás:**

A PPKE fontosnak tartja, hogy a felhasználók megértsék a levelezési rendszer működését, valamint a szabályokat, amelyek segítik őket az eszközök helyes és biztonságos használatában. Ennek érdekében a szabályzat részletes képzési és tudatosítási programokat is tartalmaz. A felhasználók segítése érdekében, a PPKE Levelezésbiztonsági Szabályzatából kivonat készül, mely jelen szabályzat 1. sz. mellékletét képezi.

Hatálya és alkalmazási kör:

A szabályzat minden felhasználóra vonatkozik, aki az egyetem Microsoft 365 levelezési rendszerét használja, beleértve:

- **Hallgatók:** Az aktív hallgatók e-mail fiókjai az egyetemi tanulmányok idejére állnak rendelkezésre, bizonyos esetekben korlátozott ideig a végzés után is hozzáférhetők.
- **Oktatók és adminisztratív dolgozók:** Az alkalmazottak fiókjai a munkaviszony idejére elérhetők, és a távozás után meghatározott ideig archiválásra kerülnek. Az archiválás a

munkaviszony megszűnése esetén, a munkaviszony megszűnésétől számított egy év. Ettől a volt munkavállaló közvetlen felettesének, valamint az adatvédelmi tisztviselő véleményének figyelembevételével, az Informatikai Osztály vezetője eltérhet. A volt munkavállaló munkaviszonyának megszűnését követően, az Informatikai Osztály vezetője, az adatvédelmi tisztviselő, valamint a volt munkavállaló közvetlen felettesének véleményét figyelembe véve határoz arról, hogy indokolt-e a volt munkavállaló levelezésének átirányítása.

- **Vendégfelhasználók:** Meghívott kutatók, vendégelőadók és partnerek korlátozott hozzáférést kapnak a levelezési rendszerhez, az egyetem által meghatározott időtartamra. A hozzáférés mértékét, valamint a hozzáférés időtartamának hosszát a vendégfelhasználó közvetlen felettesének, valamint az adatvédelmi tisztviselő véleményének figyelembevételével, az Informatikai Osztály vezetője határozza meg.

A szabályzat a PPKE levelezési rendszer teljes működési spektrumát lefedi, beleérve a következőket:

- A levelezési rendszer használati szabályai és jogosultságai.
- Biztonsági előírások, beleértve az adatvédelem és a hozzáférés védelmének biztosítását.
- Az automatikus és manuális archiválás, adatmegőrzés, valamint fióktörlési eljárások részletei.
- Speciális szabályok a külső címekre történő e-mailek továbbításának korlátozására.
- Migrációs szabályok a korábbi levelezési rendszerekből történő adatmigrációhoz.
- Felhasználói oktatási és támogatási programok, amelyek elősegítik a rendszer biztonságos és hatékony használatát.

A levelezésbiztonsági Szabályzat szerepe a PPKE digitális infrastruktúrájában:

A PPKE Microsoft 365 alapú levelezési rendszere nem csupán egy technológiai eszköz, hanem a hatékony működés egyik alappillére. A szabályzat biztosítja, hogy minden érintett fél számára egyértelműek legyenek a jogok és kötelezettségek, valamint a rendszer biztonságos működésének alapfeltételei.

A szabályzat nemcsak a napi operatív tevékenységeket támogatja, hanem hosszú távú stratégiát is meghatároz a digitális infrastruktúra fenntartható és biztonságos fejlesztésére, melyet a PPKE

Informatikai Stratégia is tartalmaz. A PPKE elkötelezett amellett, hogy a hallgatók, oktatók és adminisztratív személyzet számára modern, megbízható és felhasználóbarát digitális szolgáltatásokat biztosítson, amelyeket a jogszabályoknak megfelelően és etikus módon használnak.

2. Levelezési rendszer használata

A levelezési rendszer hatékony, biztonságos és szabályos működése érdekében az egyetem Microsoft 365 platformján alapuló szolgáltatásokat szigorúan szabályozott keretek között lehet használni. Ez a rész pontos iránymutatásokat nyújt a felhasználók számára a rendszer használatáról, a jogosultságokról és a tiltott tevékenységekről.

2.1. Általános használati szabályok

- **Használati cél:** A levelezési rendszer kizárólag oktatási, kutatási és adminisztratív célokra használható. Magáncélú használat nem megengedett. Jelen rendelkezés megsértése esetén, a munkavállaló tudomásul veszi, hogy munkaviszonyának megszűnése esetén a PPKE a jelen rendelkezés megsértésének következtében levelezési rendszerben tárolt adatait megismerheti.

  A levelezőrendszer használata nem akadályozhatja az egyetemi tevékenységeket és nem sértheti a szabályzat előírásait.
- **Fiókbiztonság:** Minden felhasználónak kötelessége biztosítani, hogy fiókjához illetéktelenek ne férhessenek hozzá. Ennek érdekében kötelező az erős jelszó használata és a kétfaktoros hitelesítés (MFA) bekapcsolása.
- **Tiltott tevékenységek:** Tilos a rendszer használata sértő, etikátlan, valamint jogellenes tartalmak továbbítására. Nem megengedett a rendszer terhelése tömeges, nem engedélyezett üzenetküldéssel.
- **Harmadik fél hozzáférése:** A felhasználók nem adhatják át fiókjuk jelszavát vagy egyéb hozzáférési adataikat más személyeknek.

2.2. Külső címekre történő automatikus továbbítás tilalma

- **Továbbítási korlátozások:** Biztonsági és adatvédelmi okokból **szigorúan tilos** az egyetemi e-mail fiókokba érkező levelek automatikus továbbítása külső e-mail címekre. Ez magában foglalja a privát e-mail címekre (pl. Gmail, Yahoo) történő másolást vagy átirányítást is.

- **Rendszerellenőrzés:** Az IT-rendszer automatikusan figyeli és blokkolja a külső címekre irányuló automatikus továbbítási kísérleteket.
- **Szabálysértések következményei:** A továbbítási tilalom megsértése fegyelmi eljárást vonhat maga után, amelynek során a felhasználó fiókját ideiglenesen vagy véglegesen letilthatják.

2.3. Felhasználói csoportok és jogosultságok

A levelezési rendszer különböző felhasználói csoportok számára eltérő szabályokkal és kvótákkal működik:

- **Hallgatók:**
  - **E-mail cím formátuma:** vezeteknev.keresztnev@hallgato.ppke.hu
  - **Kvóta:** 100 GB tárhely. Amikor a tárhely kihasználtsága eléri a 90%-ot, figyelmeztetést kapnak.
  - **Archívum:** Automatikus archívumkezelés 1 év után (50 GB archívum tárhely).
  - **Továbbítás:** Külső címre irányuló automatikus továbbítás nem engedélyezett.
  - **Napi limit:** Külső címekre napi 100 címzett üzenet küldhető.
- **Alkalmazottak (oktatók és adminisztratív dolgozók):**
  - **E-mail cím formátuma:** vezeteknev.keresztnev@kar.ppke.hu, vezeteknev.keresztnev@ppke.hu
  - **Kvóta: 100 GB tárhely.** Amikor a tárhely kihasználtsága eléri a 90%-ot a felhasználók figyelmeztetést kapnak.
  - **Archívum:** Automatikus archívumkezelés 2 év után (50 GB archívum tárhely).
  - **Továbbítás:** Külső címre irányuló automatikus továbbítás nem engedélyezett.
  - **Napi limit:** Külső címekre napi 500 címzett üzenet küldhető.
- **Vendégfelhasználók:**
  - **E-mail cím formátuma**: Ideiglenes e-mail címek a rendszer generálásával.
  - **Kvóta:** 50 GB tárhely.

- [1] Jogosulti kör: Az Egyetemmel hallgatói jogviszonyban, munkaviszonyban vagy egyéb munkavégzésre irányuló jogviszonyban nem álló személyek jogosultak az egyetemi levelezőrendszer használatára, valamint saját felhasználású, @ppke.hu, @itk.ppke.hu, @jak.ppke.hu vagy @btk.ppke.hu végződésű e-mail-cím igénylésére.
- [2] Saját felhasználású e-mail-cím igénylésére kizárólag abban az esetben van lehetőség, ha ez az Egyetem érdekeinek érvényesítése érdekében szükséges, továbbá, ha az igénylő és az Egyetem közötti jogviszony vagy együttműködés jellege ezt indokolttá teszi.
- [3] A saját felhasználású, vendégfelhasználók számára biztosított e-mail-cím létrehozása @itk.ppke.hu, @jak.ppke.hu vagy @btk.ppke.hu végződés esetén az illetékes dékán, @ppke.hu végződésű e-mail-cím esetén pedig a gazdasági főigazgató jóváhagyásával lehetséges.

- **Hozzáférés időtartama:** A hozzáférés időtartamának hosszát a vendégfelhasználó közvetlen felettesének, valamint az adatvédelmi tisztviselő véleményének figyelembevételével, az Informatikai Osztály vezetője határozza meg, külön engedélyeztetést követően az IT ITSM rendszerben.
  - **Archívum:** Nem elérhető.

2.4. Szűrők és automatizált szabályok

A rendszer automatikusan szűri az üzeneteket az alábbi kategóriák szerint:

- **Spam és adathalászat:** A levelek automatikusan elkülönítésre kerülnek, ha veszélyes vagy kéretlen tartalom található bennük.

[1,2,3] Beiktatta az Egyetemi Tanács 51/2026. (V.7.) számú határozata. Hatályos 2026. május 11. napjától.

- **Veszélyes csatolmányok:** Az adathalász támadásokkal összefüggésbe hozható fájlokat a rendszer blokkolja.
- **Jogellenes vagy sértő tartalom:** Az ilyen tartalmak automatikusan karanténba kerülnek, és erről értesítést kap az IT csapat.
- **Tömeges üzenetküldés:** Az egyetemi rendszer nem engedélyezi nem jóváhagyott tömeges üzenetek küldését.

2.5. Megőrzési időszak és törlési értesítések

- **Automatikus archiválás:**
  - Hallgatói e-mailek automatikusan archívumba kerülnek 1 év után.
  - Alkalmazotti e-mailek esetén az automatikus archiválás 2 év után történik meg.
- **Adattörlési értesítés:** A felhasználók fiókjainak törlése előtt az IT-rendszer automatikusan értesítést küld az érintetteknek legalább 2 héttel a törlés előtt. Az értesítés tartalmazza:
  - A törlés pontos dátumát.
  - Az adatmentési lehetőségeket.
  - Az IT-támogatás elérhetőségeit.

3. Biztonsági szabályok

A Microsoft 365 alapú levelezési rendszer biztonságának megőrzése alapvető fontosságú a PPKE adatvédelmi és információbiztonsági céljainak elérése érdekében. A levelezési rendszer biztonsági szabályai biztosítják a felhasználói adatok titkosságát, integritását és elérhetőségét, minimalizálva a kibertámadások, adatvédelmi incidensek és illetéktelen hozzáférések kockázatát.

3.1. Hozzáférésvédelem

1. **Erős jelszavak használata:**
   - Minden felhasználónak olyan jelszót kell választania, amely legalább 12 karakter hosszú, és tartalmaz nagybetűt, kisbetűt, számot, valamint speciális karaktert.
2. **Kétfaktoros hitelesítés (MFA):**
   - A rendszerbe történő bejelentkezéshez kötelező a kétfaktoros hitelesítés (pl. jelszó + mobilalkalmazás értesítése).
   - Az MFA engedélyezése minden új felhasználó számára alapértelmezett.
3. **Automatikus kijelentkezés:**
   - Inaktivitás esetén a felhasználók automatikusan kijelentkeztetésre kerülnek 45 perc elteltével a webes felületekről, a kijelentkeztetés nem érinti a kliens programokat pl: outlook, thunderbird, stb.
   - Ez a szabály különösen fontos nyilvános helyekről vagy megosztott eszközökről történő bejelentkezések esetén.
4. **IP-alapú korlátozások:**
   - A PPKE rendszergazdái bizonyos IP-címekről való hozzáférést korlátozhatnak a magas kockázatú régiókból történő illetéktelen bejelentkezések megelőzése érdekében.

3.2. Spam- és phishing-védelem

1. **Automatikus szűrőrendszer:**

- A Microsoft Defender for Office 365 automatikusan átvizsgálja az összes bejövő és kimenő e-mailt, hogy kiszűrje a kéretlen üzeneteket, a rosszindulatú csatolmányokat és a potenciális phishing-kísérleteket.
- A kéretlen üzenetek a „Spam" mappába kerülnek, ahonnan 30 nap után automatikusan törlődnek.

2. **Csatolmányok és linkek ellenőrzése:**
   - A rendszer automatikusan blokkolja a potenciálisan veszélyes csatolmányokat (pl. .exe, .bat fájlokat).
   - Minden beérkező e-mailben található linket a rendszer átvizsgál, hogy megakadályozza az adathalász támadásokat.
3. **Felhívás az adathalász üzenetek jelentésére:**
   - Ha a felhasználó gyanús e-mailt kap, azt köteles jelenteni az Informatikai Osztálynak a dedikált „Jelentés spamként" funkcióval vagy közvetlenül a rendszergazdák felé.

3.3. Adatvédelem

1. E-mailek titkosítása:
   - A levelek átvitele során TLS (Transport Layer Security) protokollt használnak a biztonságos kommunikáció biztosítása érdekében.
   - Az érzékeny információkat tartalmazó e-mailek esetén a felhasználóknak kötelező a Microsoft 365 titkosítási funkcióját használniuk.
2. Adathozzáférési jogosultságok:
   - Az e-mailekhez való hozzáférést szigorúan szabályozzák a felhasználói szerepkörök alapján.
   - Az Informatikai Osztály csak akkor férhet hozzá egy felhasználói fiókhoz, ha ahhoz megfelelő jóváhagyást kapott. A felhasználói fiókokhoz való hozzáféréshez megfelelő jóváhagyás a felhasználó közvetlen felettesének, az adatvédelmi tisztviselőnek, valamint az Informatikai Osztály vezetőjének jóváhagyása esetén áll fenn.

3. Adatmegőrzés és adattörlés:

- Az e-maileket a szabályzatban meghatározott ideig kell megőrizni (hallgatóknál 5 év, alkalmazottaknál 7 év), majd automatikusan törlődnek.

4. Adatvédelmi incidensek kezelése:
   - Minden adatvédelmi incidenst azonnal jelenteni kell az adatvédelmi tisztviselőnek és az Informatikai Osztálynak.
     Az Informatikai Osztály Elérhetőség: it@helpdesk.ppke.hu, https://helpdesk.ppke.hu
     Adatvédelmi tisztviselő elérhetősége: dpo@ppke.hu
   - Az incidensek kivizsgálása és kezelése során az egyetem az ISO 27001 szabvány előírásait követi.

3.4. Rendszeres ellenőrzés és audit

1. **Biztonsági auditok:**
   - Az Informatikai Osztály negyedévente rendszeres biztonsági auditokat végez a levelezési rendszerben, beleértve a hozzáférési naplók és a biztonsági események elemzését.
   - Az auditok során felmerülő biztonsági hiányosságokat azonnal javítják.
2. **Hozzáférési naplózás:**
   - Minden bejelentkezési kísérlet és hozzáférési esemény automatikusan naplózásra kerül.
   - Az adminisztrátorok jogosulatlan bejelentkezési kísérletek esetén automatikusan értesítést kapnak.
3. **Felhasználói viselkedésfigyelés:**
   - A rendszer figyeli az atipikus felhasználói viselkedést, például a szokatlan időpontban vagy helyről történő bejelentkezéseket.
   - Az ilyen tevékenységek esetén a felhasználó fiókja ideiglenesen zárolásra kerül, amíg a helyzetet tisztázásra kerül.

3.5. Oktatás és tudatosítás

1. **Felhasználói képzések:**

A PPKE rendszeresen tart képzéseket a biztonságos e-mail használatról, különös tekintettel az adathalász támadások felismerésére és a biztonságos fájlkezelésre az egyetem Moodle felületén. A felhasználók segítése érdekében, a PPKE Levelezésbiztonsági Szabályzatából kivonat készül, mely jelen szabályzat 1. sz. mellékletét képezi.

2. **Tudatosító kampányok:**
    - A PPKE éves kampányokat szervez Moodle rendszer keretein belül a kiberbiztonsági hónap keretében, ahol a felhasználók gyakorlati példákon keresztül tanulhatják meg, hogyan védjék meg adataikat.

4. Migráció a korábbi rendszerekből

A levelezési rendszer átállása a Microsoft 365 platformra átfogó előkészítést és precíz kivitelezést igényel annak érdekében, hogy az átállás zökkenőmentes legyen, az adatok ne vesszenek el, és az új rendszer használata minél gyorsabban megkezdhető legyen. Ez a rész részletesen tárgyalja a migráció előkészítését, folyamatát, ellenőrzését, valamint az archívumok kezelését.

4.1. Migráció előkészítése:

4.1.1. Adatok kategorizálása:

- **Hallgatói e-mailek:** Az aktív hallgatók fiókjai prioritást élveznek, beleértve a mappastruktúrákat és a fontos archívumokat.
- **Alkalmazotti e-mailek:** Kiemelten kezelendők az adminisztratív dolgozók és oktatók fiókjai, különösen azok, amelyek érzékeny, vagy olyan adatokat tárolnak melyeknek tárolását jogszabály írja elő.
- **Archívumok:** A régi rendszerben található archívumok áttekintése, felesleges vagy duplikált adatok eltávolítása.

4.1.2. Migrációs terv kidolgozása:

- **Időzítés**: Az átállás ütemezése olyan időszakra, amely minimális fennakadást okoz (pl. szorgalmi időszakon kívül).
- **Szerepkörök meghatározása**: Az Informatikai Osztályon belül dedikált személyek kijelölése a migráció különböző szakaszaira (pl. adatellenőrzés, technikai támogatás).
- **Tesztelési terv**: A migráció pilot verziójának előkészítése egy kisebb felhasználói csoporttal.

4.1.3. Felhasználói tájékoztatás:

- Minden érintett felhasználót időben értesíteni kell az átállás részleteiről, beleértve a várható leállásokat és a szükséges teendőket (pl. régi e-mailek mentése).

4.2. Migrációs folyamat

A migráció több szakaszban történik annak érdekében, hogy minimalizáljuk az adatok elvesztésének kockázatát és az átállásból adódó fennakadást.

4.2.1. Pilot szakasz:

- A migráció megkezdése előtt egy kisebb csoport (pl. Informatikai Osztály) fiókjainak tesztelése.
- A rendszer kompatibilitásának ellenőrzése, beleértve a mappastruktúrákat, automatikus szabályokat és csatolmányokat.

4.2.2. Adattisztítás:

- Az Informatikai Osztály átvizsgálja a régi rendszert az inaktív vagy felesleges adatok kiszűrésére.
- Duplikált e-mailek, hibás vagy sérült fájlok eltávolítása.

4.2.3. Teljes migráció:

- **Adatok átvitele:** Az összes e-mail átmásolása a Microsoft 365 platformra.
- **Másodlagos mail címek, aliasok:** A felhasználóknak korábban beállított másodlagos mail címek, aliasok, csoportcímek beállítása.
- **Csatolmányok kezelése:** Nagyméretű fájlok migrációjának biztosítása, szükség esetén külön tárhelyre való áthelyezéssel.

4.2.4. Ellenőrzés:

- Az adatok migráció utáni ellenőrzése manuálisan és automatikus szkriptekkel.
- Felhasználói visszajelzések gyűjtése a pilot szakasz után, és az esetleges problémák megoldása.

4.2.5. Átadás a felhasználóknak:

- Az új rendszerhez való hozzáférés biztosítása.

- Útmutatók és támogatás biztosítása az első bejelentkezéshez.

4.3. Archívumok kezelése

4.3.1. Archívumok áttekintése:

- A régi levelezési rendszerben tárolt archívumok teljes körű felmérése.
- Duplikációk eltávolítása és az adatok kategorizálása, például fontos és kevésbé fontos tartalmak szerint.

4.3.2. Adatok áttelepítése:

- A régi archívumok migrálása külön dedikált tárhelyre.
- Automatikus indexelés az archívumok könnyebb kereshetősége érdekében.

4.3.3. Archiválási szabályok alkalmazása:

- A szabályzatnak megfelelően a hallgatói archívumokat 5 évig, az alkalmazotti archívumokat 7 évig kell megőrizni.
- Az archívumok automatikus törlése a megőrzési időszak lejárta után.

4.3.4. Hozzáférés biztosítása:

- A felhasználók számára hozzáférés biztosítása a migrált archívumokhoz, szükség esetén külön felületen keresztül.

4.4. Felhasználói tájékoztatás és támogatás

4.4.1. Migráció előtti tájékoztatás:

- Minden felhasználót e-mailben értesítenek a migráció pontos időpontjáról, a várható leállási időszakról és a migráció utáni teendőkről.

4.4.2. Új rendszer bemutatása:

- Az átállás után az Informatikai Osztály rövid útmutatókat és oktatóvideókat biztosít a felhasználók számára az egyetem Moodle felületén keresztül a Microsoft 365 levelezési rendszer alapvető funkcióinak használatáról.

4.4.3. Technikai támogatás:

- Az Informatikai Osztály dedikált támogatási vonalat működtet az átállás utáni 30 napban, hogy segítséget nyújtson az esetleges problémák megoldásában.

4.5. Folyamatos felügyelet és visszajelzés

4.5.1. Migrációs hibák nyomon követése:

- Az Informatikai Osztály részletes naplót készít a migráció során felmerülő hibákról és azok megoldásáról.

4.5.2. Felhasználói elégedettség mérése:

- Az átállás után kérdőívek és visszajelzési rendszerek segítségével mérik a felhasználók elégedettségét.

4.5.3. Folyamatos rendszeroptimalizálás:

- A migráció során azonosított problémák és kihívások alapján az Informatikai Osztály optimalizálja a rendszert, hogy a jövőbeni átállások gördülékenyebbek legyenek.

5. Archívumkezelés és adatmegőrzés

Az archívumkezelés és adatmegőrzés szabályozása kulcsfontosságú az egyetem Microsoft 365 alapú levelezési rendszerének működésében. Az e-mailek archiválásának célja az adatok hosszú távú tárolása és visszakereshetősége, miközben biztosítja, hogy a rendszer megfeleljen az adatvédelmi és egyéb jogszabályi követelményeknek. Az adatok megőrzési időszaka és törlési szabályai biztosítják, hogy a rendszer hatékonyan működjön, és ne terhelje túl a tárhelyet.

5.1. Megőrzési időszakok

Az e-mailek és archívumok megőrzési időszakai a felhasználói csoportok igényei és jogi előírásai alapján kerültek meghatározásra:

- **Hallgatók**:
  - Az e-mailek automatikusan archívumba kerülnek 1 év után.
  - Az archívumokat az egyetem 5 évig megőrzi.
  - A hallgatói fiók deaktiválása után az archívumok további 6 hónapig hozzáférhetők a felhasználó számára, ezt követően törlésre kerülnek.
- **Alkalmazottak:**
  - Az e-mailek automatikusan archívumba kerülnek 2 év után.
  - Az archívumokat az egyetem 7 évig megőrzi.
  - Az alkalmazotti fiók deaktiválása után az archívumok további 1 évig hozzáférhetők, majd törlésre kerülnek.
- **Vendégfelhasználók:**
  - A vendégfiókokban létrehozott e-mailek és adatok az időkorlátos hozzáférés lejárta után azonnal törlésre kerülnek.
  - Archívumok nem kerülnek létrehozásra.

5.2. Automatikus archiválás

Az automatikus archiválási funkció célja a rendszer hatékony működésének fenntartása és a felhasználók számára könnyen hozzáférhető hosszú távú adattárolás biztosítása:

Archiválási folyamat:

- A levelezési rendszer az 1 évnél régebbi hallgatói és a 2 évnél régebbi alkalmazotti e-maileket automatikusan áthelyezi az archívumba.
- Az archívum külön tárolóegységen kerül elhelyezésre a fő levelezési tárhelytől függetlenül, így csökkentve a fő tárhely terhelését.

Archívum elérése:

- A felhasználók az archívumokat közvetlenül elérhetik a Microsoft 365 felületén keresztül, az „Archívum” mappában.
- Az archívumban tárolt e-mailek kereshetőek és olvashatóak, azonban módosításuk nem engedélyezett.

Értesítések:

- Az archívum közeledő megteltéről a rendszer automatikus értesítést küld a felhasználónak, amely tartalmazza a további mentési vagy törlési lehetőségeket.

5.3. Adatok törlése

A törlési szabályok célja, hogy biztosítsák a megőrzési időszak lejárta után az adatok biztonságos és végleges eltávolítását:

Automatikus törlés:

- A megőrzési időszak lejárta után az archívumban tárolt adatokat a rendszer automatikusan törli.
- A törlés előtt 2 héttel a rendszer értesítést küld a felhasználónak, amelyben tájékoztatja az adatmentési lehetőségekről.

Törlés előtti értesítés:

- Az értesítés tartalmazza:
    - A törlés pontos időpontját.
    - Az adatok exportálásának vagy letöltésének módját.
    - Az IT-támogatás elérhetőségét további segítség érdekében.

Biztonságos törlés:

- **Az adatok törlése a Microsoft 365 rendszer által biztosított biztonságos törlési eljárásokkal történik, amelyek megfelelnek az adatvédelmi előírásoknak.**
- **Az adatok végleges törlése után azok helyreállítása nem lehetséges.**

5.4. Adatok helyreállítása

Az adatok helyreállítása csak a megőrzési időszak alatt lehetséges, az alábbi szabályok szerint:

Adatok helyreállításának folyamata:

- A felhasználók az archívumból saját maguk helyreállíthatják az adatokat.
- Ha a helyreállítás nem lehetséges, a felhasználó kérheti az Informatikai Osztály segítségét, amely naplózza a helyreállítási kérelmet és végrehajtja azt.

Helyreállítás időkorlátjai:

- Az e-mailek és egyéb adatok a törlési értesítést követően 14 napig még helyreállíthatók.

5.5. Adatok exportálása

A felhasználók számára lehetőség van az adatok exportálására a megőrzési időszak lejárta előtt:

Exportálási lehetőségek:

- Az adatok exportálása a Microsoft 365 felületén keresztül önkiszolgáló módon történik.
- Az exportált adatok szabványos formátumban (pl. PST vagy CSV) kerülnek letöltésre.

Technikai támogatás:

- Az Informatikai Osztály biztosítja a felhasználók számára az exportálási folyamat technikai támogatását, különösen nagy mennyiségű adat exportálása esetén.

5.6. Archívumok és jogszabályi megfelelés

Adatvédelmi előírások:

- Az egyetemi ügymenetre vonatkozó adatvédelmi és adatbiztonsági szabályokat az Adatvédelmi és Adatbiztonsági Szabályzat (AVBSZ) tartalmazza.

Jogszabályi kötelezettségek:

- Ha az archívumban tárolt adatok jogszabályi kötelezettségek miatt hosszabb megőrzést igényelnek (pl. peres ügyek, auditok), az Informatikai Osztály erről külön rendelkezik.

5.7. Felhasználói oktatás és tájékoztatás

Archívumkezelési útmutatók: Az egyetem oktatási anyagokat és videókat biztosít az archívumok eléréséről, kereséséről és kezeléséről.

Képzések: Az új felhasználók számára az egyetem Moodle felületén keresztül rendszeresen szervezett képzések során bemutatják az archívumkezelési szabályokat és lehetőségeket.

Rendszeres tájékoztatás: Az Informatikai Osztály évente tájékoztatót küld a felhasználóknak az archívumkezelési szabályok változásairól és a legjobb gyakorlatokról.

6. Felhasználói képzések

A Microsoft 365 levelezési rendszer hatékony és biztonságos használata érdekében az egyetem kiemelt figyelmet fordít a felhasználók képzésére és tudatosítására. A képzések célja, hogy minden felhasználó megértse a rendszer működését, ismerje a szabályzat előírásait, és elsajátítsa a levelezési rendszer biztonságos használatához szükséges készségeket.

6.1. Hallgatói képzés (Moodle):

Bevezető képzések az új hallgatók számára:

- **Tartalom:** Az alapvető funkciók bemutatása, mint például e-mail küldése és fogadása, csatolmányok kezelése, és a mappák használata.
- **Időzítés:** Az első félév elején, kötelező jelleggel.
- **Formátum:** Online oktatóanyagok.

Speciális témák:

- **Adathalászat és spam felismerése:** Bemutató arról, hogyan lehet azonosítani a gyanús e-maileket és elkerülni az online csalásokat.
- **Adatvédelem:** Az e-mailekben szereplő személyes és érzékeny információk védelmére vonatkozó legjobb gyakorlatok.
- **Fiókhelyreállítás:** Mit tegyenek, ha elveszítik a hozzáférést a fiókjukhoz.

Rendszeres frissítések:

- **Az Informatikai Osztály évente frissíti a képzési anyagokat az új funkciók és biztonsági irányelvek alapján.**

6.2. Alkalmazotti képzés (Moodle)

Átfogó tréningek az új alkalmazottak számára:

- **Tartalom:** Az egyetem levelezési szabályzatának részletes ismertetése, a levelezési rendszer funkciói, valamint a dokumentummegosztási és -tárolási lehetőségek.
- **Időzítés:** Az alkalmazotti jogviszony kezdetén, kötelező részvétellel.

Haladó képzések:

- **Automatikus szabályok és szűrők:** Hogyan lehet hatékonyan használni a szabályokat az e-mailek automatikus rendszerezéséhez és időmegtakarításhoz.
- **Adatbiztonság:** A bizalmas adatok védelme, beleértve a titkosítási lehetőségeket és a jogosulatlan hozzáférések elleni védelmet.
- **Archívumkezelés:** Az automatikus archiválási folyamat és az archívumok visszakeresése.

Adathalászat-megelőzési tréning:

- Rendszeresen frissített program az adathalász kísérletek felismerésére és jelentésére.
- Gyakorlati példák és szimulációk, amelyek segítik az alkalmazottakat a valós helyzetek kezelésében.

Továbbképzések:

- Az Informatikai Osztály évente legalább egy alkalommal haladó tréningeket szervez az új funkciókról és a rendszer használatának optimalizálásáról.

6.3. Vendégfelhasználók képzése (Moodle)

Gyorsított képzések:

- Rövidített útmutatókat és videóanyagokat biztosítanak a vendégfelhasználók számára a rendszer alapvető funkcióiról.
- A képzések különösen a biztonságos hozzáférésre és a rendszer etikus használatára koncentrálnak.

Segédanyagok:

- Egyszerű, vizuális útmutatók a bejelentkezésről, a levelezési szabályokról és az adatvédelemről.

6.4. Képzési formátumok

Online tananyagok:

- Interaktív e-learning modulok, amelyeket a Microsoft 365 platform felhasználói felületére szabtak.
- Rövid, 5-10 perces videók az alapvető funkciókról és a leggyakoribb problémák megoldásáról.

Dokumentáció és útmutatók:

- PDF formátumban letölthető kézikönyvek és GYIK (Gyakran Ismételt Kérdések).
- Az IT-portálon elérhető részletes útmutatók, kereshető formátumban.

6.5. Tudatosító kampányok

Esettanulmányok és példák:

- Valós esetek bemutatása, amelyek segítik a felhasználókat a kockázatok felismerésében.
- Sikeres védekezési stratégiák ismertetése.

Hírek és figyelmeztetések:

- Az Informatikai Osztály rendszeresen értesíti a felhasználókat az aktuális kiberfenyegetésekről és az új biztonsági frissítésekről.

6.6. Felhasználói támogatás

Dedikált IT-támogatás:

- Az IT Helpdesk a https://helpdesk.ppke.hu felületen elérhető a felhasználók számára.
- Gyors válaszidő az e-mailekhez és technikai problémákhoz kapcsolódó kérdések esetén.

Személyre szabott segítségnyújtás:

- Egyéni konzultációk lehetősége, ha a felhasználónak speciális kérdései vagy problémái vannak.

Visszajelzés gyűjtése:

- A felhasználóktól rendszeresen gyűjtenek visszajelzéseket a képzések hatékonyságáról és az Informatikai Osztály által nyújtott támogatás minőségéről.

6.7. Képzési hatékonyság ellenőrzése

Felhasználói tesztek:

- A képzések után rövid online tesztek segítenek a felhasználóknak elmélyíteni a tanultakat.
- Az eredményeket az Informatikai Osztály elemzi, hogy azonosítsa a további fejlesztési lehetőségeket.

Követési mutatók:

- Az Informatikai Osztály figyelemmel kíséri a biztonsági incidensek számát és típusát, hogy mérje a képzések hatékonyságát.

Éves értékelés:

- Az Informatikai Osztály évente kiértékeli a képzési programokat és javaslatokat tesz azok továbbfejlesztésére.

7. Szankciók szabályszegés esetén

A Microsoft 365 levelezési rendszer használata során az egyetem szigorúan szabályozza a felhasználói magatartást, hogy biztosítsa a rendszer biztonságát, hatékonyságát és megfelelését az adatvédelmi szabályoknak. Az előírások megszegése esetén az egyetem különböző szankciókat alkalmaz, amelyek arányosak a szabálysértés súlyosságával. Ez a rész részletesen bemutatja a lehetséges szabályszegéseket, azok kategorizálását, valamint a kiszabható szankciókat.

7.1. Szabálysértések kategóriái

7.1.1. Enyhe szabályszegések:

- A levelezési kvóta túllépése, amely figyelmeztetést vagy rendszerkorlátozást eredményezhet.
- Tömeges üzenetek küldése az egyetemi rendszer irányelveinek megszegésével (pl. reklámanyagok, nem hivatalos események hirdetése).

7.1.2. Mérsékelt szabályszegések:

- A levelezési rendszer nem oktatási, kutatási vagy adminisztratív célú használata.
- Olyan tartalmak küldése, amelyek etikátlanok vagy potenciálisan sértők, de nem sértik az adatvédelmi vagy jogi előírásokat.
- Az automatikus külső továbbításra vonatkozó szabályok megsértése.

7.1.3. Súlyos szabályszegések:

- [4] Tiltott tartalom (pl. jogellenes, sértő vagy zaklató anyagok) küldése vagy fogadása (egyetemi e-mail címmel ilyen jellegű csatornákra történt szándékos regisztrálásból adódóan).
- Adathalász vagy rosszindulatú e-mailek terjesztése, szándékosan vagy gondatlanságból.
- A felhasználói fiókhoz kapcsolódó adatvédelmi előírások szándékos megsértése, például érzékeny adatok titkosítás nélküli továbbítása.

[4] Módosította az Egyetemi Tanács 51/2026. (V. 7.) számú határozata. Hatályos 2026. május 11. napjától.

- Jogosulatlan személyek hozzáférésének engedélyezése (pl. jelszó megosztása harmadik féllel).

7.2. Szankciók szintjei és alkalmazási szabályai

7.2.1. Enyhe szabálysértések esetén:

- **Első alkalom:** Írásbeli figyelmeztetés a felhasználó számára, amely tartalmazza a szabályszegés részleteit és a helyes eljárásokat.
- **Második alkalom:** Ideiglenes korlátozás a rendszer bizonyos funkcióira (pl. csatolmányküldés tiltása, kvóta növelési kérelmek elutasítása).
- **Harmadik alkalom:** Részletes audit és további korlátozások, például a levelezési fiók részleges felfüggesztése.

7.2.2. Mérsékelt szabálysértések esetén:

- **Első alkalom:** Az Informatikai Osztály figyelmeztetése, valamint kötelező konzultáció a szabályok megértéséről.
- **Második alkalom:** Ideiglenes fiókzárás (pl. 24-72 órára), amelynek célja a felhasználó figyelmének felhívása a szabályok betartására.
- **Harmadik alkalom:** Az adatvédelmi tisztviselő bevonása, a fiók részleges vagy teljes felfüggesztése, és szükség esetén fegyelmi eljárás kezdeményezése.

7.2.3. Súlyos szabálysértések esetén:

- **Első alkalom:** Azonnali fiókzárás, amelynek célja a további károk megelőzése. Az Informatikai Osztály értesíti az adatvédelmi tisztviselőt és az illetékes vezetőt.
- **Vizsgálat:** Az incidens részletes kivizsgálása, amely magában foglalja az érintett adatok és események naplóinak elemzését.
- **Jogkövetkezmények:** Súlyosabb esetekben (pl. jogsértő tartalom terjesztése) az egyetem jogi lépéseket tehet és ennek érdekében együttműködhet az adott eljárás lefolytatására hatáskörrel rendelkező hatóságokkal. A PPKE a jelen szabályzatba foglalt

jogkövetkezményeken túl, egyéb munkavállalók esetén munkajogi, hallgatók esetén a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvényben meghatározott jogkövetkezményt is alkalmazhat.

7.3. Speciális esetek és kivételes eljárások

Automatikus külső továbbítás megsértése:

- Az automatikus vagy manuális külső továbbítási szabály megszegése esetén az Informatikai Osztály azonnali intézkedésként deaktiválja az érintett szabályokat, és értesíti a felhasználót.

Adathalász kísérletek jelentése:

- Ha egy felhasználó szándékosan részt vesz adathalász támadások terjesztésében, fiókját azonnal zárolják, és az egyetem az ügyet az adatvédelmi hatóságok elé terjeszti.

Fiók kompromittálása esetén:

- Amennyiben egy fiók kompromittálódik (pl. jelszólopás vagy illetéktelen hozzáférés miatt), az Informatikai Osztály zárolja a fiókot, és értesíti a felhasználót a helyreállítási lépésekről.

7.4. Szankciók dokumentációja és nyomon követése

7.4.1. Incidensnaplózás:

- Minden szabályszegési esetet az Informatikai Osztály dokumentál az egyetemi naplózási rendszerben.
- A dokumentáció tartalmazza az esemény időpontját, részleteit, a felhasználó értesítését és a meghozott intézkedéseket.

7.4.2. Éves jelentések:

- Az Informatikai Osztály és az adatvédelmi tisztviselő évente összegzést készít a szabályszegésekről és az alkalmazott szankciókról.

- Az összegzés alapján javaslatokat tesznek a rendszer fejlesztésére és a szabályok pontosítására.

7.5. Fellebbezési lehetőségek

7.5.1. Felhasználói jogok:

- Minden felhasználónak joga van fellebbezni a szabályszegés miatti szankció ellen.
- A fellebbezést írásban kell benyújtani az Informatikai Osztályhoz, amely továbbítja azt az egyetemi adatvédelmi tisztviselőnek vagy a fegyelmi bizottságnak.

7.5.2. Fellebbezési eljárás:

- A beadványt 15 napon belül megvizsgálják, és a döntésről értesítik a felhasználót.
- Súlyosabb esetekben (pl. tanulmányi jogviszony megszüntetése) az ügyet az egyetem vezetősége bírálja el.

7.6. Szankciók preventív hatása

A szabályszegések kezelésének célja nem csupán a szabályok megszegésének szankcionálása, hanem a felhasználók tudatosítása és a hasonló esetek megelőzése. Az Informatikai Osztály rendszeresen elemzi a szabályszegéseket, hogy azonosítsa a leggyakoribb hibákat, és képzési programokat indítson ezek csökkentésére.

8. Felelősségi körök és felügyelet

A Microsoft 365 alapú levelezési rendszer hatékony működése érdekében az egyetem különböző szervezeti egységei és szereplői között egyértelműen meghatározott felelősségi körökre van szükség. Ez a rész részletesen ismerteti az Informatikai Osztály, az adatvédelmi tisztviselő, az egyetemi vezetőség és a felhasználók szerepét, valamint a felügyelet és ellenőrzés folyamatát.

8.1. IT-osztály feladatai

8.1.1. Rendszerkarbantartás és üzemeltetés:

- Felelős a Microsoft 365 levelezési rendszer folyamatos karbantartásáért, konfigurálásáért.
- Biztosítja a rendszer frissítéseit és a legújabb biztonsági javításokat.

8.1.2. Hibaelhárítás:

- Gyors és hatékony technikai támogatás nyújtása a felhasználók számára.
- A jelentett problémák megoldása, például fiók-hozzáférési nehézségek, rendszerhibák vagy adatvisszaállítás.

8.1.3. Biztonsági intézkedések:

- Felügyeli a rendszer biztonságát, beleértve a kétfaktoros hitelesítés, a titkosítás és a spam- vagy adathalászat-ellenes védelem működését.
- Azonnali intézkedéseket tesz adatvédelmi incidensek esetén.

8.1.4. Migrációs és archiválási feladatok:

- Az adatok áttelepítése a korábbi rendszerekből.
- Az automatikus archiválási szabályok beállítása és az archívumok kezelése.

8.1.5. Ellenőrzések és auditok:

- Rendszeres biztonsági auditokat végez.
- Naplózza és elemzi a rendszer használatával kapcsolatos tevékenységeket, különös tekintettel a szabályszegésekre vagy gyanús viselkedésekre.

8.2. Adatvédelmi tisztviselő (DPO) feladatai

8.2.1. Adatvédelmi megfelelőség biztosítása:

- Ellenőrzi, hogy a levelezési rendszer működése megfelel a GDPR, valamint az egyéb nemzeti és nemzetközi adatvédelmi előírásoknak.
- Tanácsot ad a felhasználóknak és az egyetemi vezetőségnek az adatvédelemmel kapcsolatos kérdésekben.

8.2.2. Adatvédelmi incidensek kezelése:

- Felelős az adatvédelmi incidensek kivizsgálásáért és jelentéséért.
- Kapcsolatot tart az illetékes hatóságokkal, ha szükséges.

8.2.3. Felügyeleti funkció:

- Rendszeresen auditálja a levelezési rendszer adatkezelési gyakorlatát.
- Felügyeli az adatok archiválási és törlési folyamatait.

8.2.4. Oktatás és tanácsadás:

- Felhasználói és IT-képzések szervezése az adatvédelemmel és biztonsággal kapcsolatos témákban.
- Írásos iránymutatások és gyakorlati útmutatók biztosítása.

8.3. Egyetemi vezetőség feladatai

8.3.1. Stratégiai irányítás:

- Meghatározza a levelezési rendszer működésével kapcsolatos stratégiai irányvonalakat és prioritásokat.
- Biztosítja az Informatikai Osztály és az adatvédelmi tisztviselő munkájának támogatását.

8.3.2. Fegyelmi ügyek kezelése:

- Felelős a súlyos szabályszegések kezeléséért és a fegyelmi eljárások elindításáért.
- Döntéseket hoz az adatvédelmi incidensek kezelésével kapcsolatban.

8.3.3. Erőforrások biztosítása:

- Gondoskodik az IT-infrastruktúra fenntartásához szükséges pénzügyi és emberi erőforrások rendelkezésre állásáról.

8.4. Felhasználók feladatai

8.4.1. A szabályzat betartása:

- A felhasználók kötelesek a levelezési rendszer használati szabályait és az adatvédelmi előírásokat betartani.
- Különös figyelmet kell fordítaniuk a külső címekre történő továbbítás tilalmára, valamint az adathalász e-mailek felismerésére.

8.4.2. Fiók biztonságának fenntartása:

- Az erős jelszavak használata és a kétfaktoros hitelesítés aktiválása kötelező.
- Az illetéktelen hozzáférés gyanúja esetén azonnal értesíteniük kell az Informatikai Osztályt.

8.4.3. Adatvédelmi incidensek jelentése:

- Ha a felhasználó adatvédelmi szabálytalanságot vagy biztonsági incidenst tapasztal, köteles azt jelenteni az Informatikai Osztály vagy az adatvédelmi tisztviselő felé.

8.4.4. Képzéseken való részvétel:

- A felhasználók számára biztosított képzéseken való részvétel ajánlott, a rendszer biztonságos és hatékony használatának elsajátítása érdekében.

8.5. Felügyelet és ellenőrzés

8.5.1. Rendszeres auditok:

- Az Informatikai Osztály és az adatvédelmi tisztviselő negyedévente ellenőrzéseket végez, amelyek során vizsgálják a rendszer használatát, a biztonsági szabályok betartását, és a felmerült incidenseket.

8.5.2. Hozzáférés naplózása:

- Az összes bejelentkezési és adathozzáférési eseményt a rendszer automatikusan naplózza, lehetővé téve a visszamenőleges ellenőrzéseket.
- Gyanús tevékenységek esetén az Informatikai Osztály automatikus értesítéseket kap, és vizsgálatot indít.

8.5.3. Felhasználói viselkedés figyelése:

- A rendszer figyeli az atipikus felhasználói tevékenységeket, például az IP-címek vagy bejelentkezési időpontok szokatlan változásait.

- Gyanús tevékenységek esetén a felhasználói fiók automatikusan zárolható.

8.6. Jelentési kötelezettségek

8.6.1. Adatvédelmi incidensek jelentése:

- Minden adatvédelmi incidenst az Informatikai Osztály jelent az adatvédelmi tisztviselőnek.
- Súlyos esetekben a tisztviselő köteles jelentést készíteni az illetékes hatóságok számára.

8.6.2. Éves jelentés az egyetemi vezetőség számára:

- Az Informatikai Osztály és az adatvédelmi tisztviselő évente részletes jelentést készít a levelezési rendszer működéséről, a szabályszegésekről, valamint a rendszer fejlesztési lehetőségeiről.

9. Kapcsolat és támogatás

Az egyetem Microsoft 365 levelezési rendszerének hatékony működtetéséhez elengedhetetlen, hogy a felhasználók gyors és megbízható támogatást kapjanak bármilyen technikai vagy felhasználói problémájuk megoldásában. Ez a rész részletesen ismerteti a támogatási csatornákat, az elérhetőségeket, a kapcsolattartási pontokat, valamint a támogatási folyamatokat és eszközöket.

9.1. IT Helpdesk

9.1.1. Szerepe:

- Az IT Helpdesk az elsődleges kapcsolattartási pont a felhasználók számára technikai problémák, kérdések és egyéb támogatási igények esetén.
- Felelős a felhasználók bejelentéseinek fogadásáért, priorizálásáért és megoldásáért.

9.1.2. Elérhetőség:

- **E-mail:** it@helpdesk.ppke.hu
- **Online felület:** Egyetemi IT-portál (TOPDESK) https://helpdesk.ppke.hu

9.1.3. Feladatok:

- Jelszó-visszaállítási kérelmek kezelése.
- Technikai problémák (pl. bejelentkezési hibák, csatolmányok küldésének problémái) megoldása.
- Rendszerfrissítésekkel és új funkciókkal kapcsolatos információk biztosítása.
- Felhasználói kérdések megválaszolása és továbbítása a megfelelő szakértői csoporthoz, ha szükséges.

9.1.4. Prioritási szintek:

- **Sürgős:** Rendszerszintű hibák vagy hozzáférhetetlenség esetén azonnali intézkedés.
- **Magas:** Adatvédelmi incidensek, illetéktelen hozzáférések vagy biztonsági problémák.
- **Közepes:** Egyéni felhasználói problémák, például fiókbeállítási gondok vagy archívum-hozzáférési nehézségek.
- **Alacsony:** Általános kérdések és útmutatás iránti igény.

9.2. Támogatási eszközök

9.2.1. Online IT-portál:

- Egy központi platform, ahol a felhasználók jelenthetik a problémáikat, nyomon követhetik a bejelentések állapotát, és hozzáférhetnek a gyakran ismételt kérdésekhez (GYIK) és útmutatókhoz. (TOPDESK)

9.2.2. Önkiszolgáló eszközök:

- **Jelszó-visszaállítás:** Automatikus jelszó-helyreállítási folyamat a Microsoft 365 rendszerén keresztül.
- **Adatmentés:** Saját archívumokból történő adat-helyreállítás lehetősége.

9.2.3. Chatbot:

- Egy mesterséges intelligenciával működő virtuális asszisztens, amely gyors válaszokat ad a leggyakoribb kérdésekre (pl. hogyan lehet létrehozni egy új mappát, vagy hogyan kell konfigurálni az e-mail kliensét).

9.3. Támogatási folyamat

9.3.1. Probléma bejelentése:

- A felhasználó az IT Helpdesk elérhetőségein keresztül bejelenti a problémát, amelyet az IT-csapat nyilvántartásba vesz.
- A bejelentés során szükséges információk:
    - Felhasználói név és e-mail cím.
    - A probléma pontos leírása.
    - Ha lehetséges, képernyőképek csatolása.

9.3.2. Probléma azonosítása és priorizálása:

- Az IT-csapat azonosítja a probléma jellegét és fontosságát, majd kijelöli a megfelelő szakértőt a megoldásra.

9.3.3. Hibaelhárítás:

- A szakértői csapat a lehető leggyorsabban megoldja a problémát.
- Ha a megoldás időt vesz igénybe, a felhasználót folyamatosan tájékoztatják az előrehaladásról.

9.3.4. Probléma lezárása és visszajelzés:

- A probléma megoldása után az IT-csapat értesíti a felhasználót, és visszajelzést kér a támogatás minőségéről.

9.4. Adatvédelmi tisztviselő elérhetősége

9.4.1. Szerepe:

- Tanácsot ad, és tájékoztatja a szervezetet, valamint az adatkezelésben részt vevő munkavállalót adatvédelmi kötelezettségeiről.
- Ellenőrzi, hogy a szervezet megfelel-e az adatvédelmi jogszabályoknak és a releváns hatósági és bírósági gyakorlatnak.
- Kapcsolatot tart a felügyeleti hatósággal, valamint az érintettekkel.

9.4.2. Elérhetőség:

- **E-mail : dpo@ppke.hu**

9.5. Képzések és tudatosság növelése

9.5.1. Útmutatók és videók:

- Az IT-portálon elérhetők a rendszer használatát bemutató oktatóanyagok, például:
  - „Hogyan lehet visszaállítani a jelszót?”
  - „Archívumok kezelése a Microsoft 365-ben.”

9.5.2. Interaktív képzések:

- Az Informatikai Osztály rendszeresen frissíti az interaktív tananyagokat a Moodle rendszeren keresztül, ahol a felhasználók gyakorlati példákon keresztül tanulhatják meg a levelezési rendszer használatát.

9.5.3. Rendszerfrissítések ismertetése:

- Új funkciók bevezetésekor az IT-csapat értesítést küld, amely tartalmazza az újítások leírását és az azokra vonatkozó útmutatókat.

9.6. Felhasználói visszajelzések gyűjtése

9.6.1. Értékelési rendszer:

- A felhasználók minden támogatási eset után értékelhetik az IT Helpdesk által nyújtott szolgáltatást.

9.6.2. Javaslatok és fejlesztések:

- A felhasználók által benyújtott javaslatokat az Informatikai Osztály elemzi, és figyelembe veszi a rendszer fejlesztése során.

9.6.3. Éves elégedettségi felmérés:

- Az Informatikai Osztály évente kérdőívet küld ki a felhasználóknak, hogy felmérje a támogatási rendszer hatékonyságát és az esetleges hiányosságokat.

9.7. Rendkívüli helyzetek kezelése

9.7.1. Rendszerleállás vagy nagyszabású hibák esetén:

- Az Informatikai Osztály azonnal értesíti a felhasználókat e-mailben és a weboldalon keresztül.
- Az értesítés tartalmazza a probléma jellegét, a várható helyreállítási időt és az alternatív megoldásokat.

9.7.2. Adatvédelmi incidensek:

- Az IT Helpdesk és az adatvédelmi tisztviselő közösen dolgozik az incidens kivizsgálásán.

Elfogadási záradék:

A jelen szabályzat módosítását a Pázmány Péter Katolikus Egyetem Egyetemi Tanácsa **51/2026. (V. 7.)** számú határozatával elfogadta. Hatályos: 2026. május 11. napjától.

Adatvédelmi státusz: **nyilvános**

Kelt: Budapest, 2026. május 7.

PÁZMÁNY PÉTER KATOLIKUS EGYETEM * REKTOR * BUDAPEST

Dr. Kuminetz Géza György
rektor

1. sz. melléklet:

Munkavállalói tájékoztató a Pázmány Péter Katolikus Egyetem Levelezésbiztonsági Szabályzatához (2025)

A Pázmány Péter Katolikus Egyetem levelezési rendszere a mindennapos oktatási, kutatási és adminisztratív munka egyik legfontosabb digitális eszköze. Az alábbi összefoglaló segít eligazodni a legfontosabb szabályok között, azonban nem pótolja a Levelezésbiztonsági Szabályzat teljes körű megismerését. Egyetemünk levelezési rendszere nem csak eszköz, hanem stratégiai erőforrás, felelős használata elengedhetetlen a Pázmány Péter Katolikus Egyetem zökkenőmentes működéséhez.

1. A rendszer használatának célja

- A levelezési rendszer munkahelyi (oktatási, adminisztratív, kutatási) feladatokhoz használható.
- A levelezési rendszer használata magáncélú levelezéshez nem megengedett.
- Nem megengedett továbbá magán (Gmail, Yahoo stb…) e-mail cím használata az egyetemi ügyrendben való ügyintézés során.

2. Fiók- és Adatbiztonsági előírások

- A levelezési rendszer használata során kötelező az erős jelszó (12 karakter, kis- és nagybetű, valamint szám és speciális karakter) használata, valamint a két faktoros hitelesítés.
- Tilos az egyetemi rendszerhez tartozó jelszó megosztása más személlyel.
- Tilos az egyetemi e-mailek automatikus továbbítása privát külsős (Gmail, Yahoo stb…) címekre.
- Az Informatikai Osztály a jogviszony fennállása alatt vagy megszűnését követően, kizárólag megfelelő jóváhagyás esetén megismerheti a fiók tartalmát és a jogviszony megszűnése esetén határozhat a levelezés átirányításáról.

3. Mire Figyeljünk a biztonságos használat érdekében?

- Ne nyissunk meg ismeretlen forrásból érkező csatolmányt vagy linket, ezek akár adathalász üzenetek is lehetnek.

- Ha bármilyen gyanús e-mailt kapunk használjuk a „Jelentem spamként” funkciót, valamint jelezzük az Informatikai Osztály felé.

3. Támogatás és kapcsolattartás

- Bármilyen technikai kérdés vagy probléma esetén az alábbi elérhetőségeken kérhet segítséget:

IT helpdesk:

- it@helpdesk.ppke.hu
- www.helpdesk.ppke.hu

Adatvédelmi tisztviselő (főleg személyes adatokat veszélyeztető esetekben)

- dpo@ppke.hu

Köszönjük, hogy körültekintő munkájával Ön is hozzájárul a Pázmány Péter Katolikus Egyetem digitális biztonságához! Kérdés, probléma vagy javaslat esetén az IT csapat, illetve az adatvédelmi tisztviselő készséggel áll rendelkezésére.