Az elektronikus levelezés szabályai

67. § (1) Az e-mail címek lehetnek személyhez, szervezethez vagy egyéb csoporthoz (pl. projekt) rendelve. Minden esetben egyetemi- hallgatói azonosítóhoz kapcsolódnak.

(2) Egyetemi e-mail cím az egyetemi tevékenységgel összefüggésben használható, az alábbi alapvetésekre figyelemmel:

a) egyetemi polgárok a foglalkoztatásra irányuló jogviszonyukhoz, vagy hallgatói jogviszonyukhoz kapcsolódó ügyintézésre kizárólag egyetemi e-mail cím (az Informatikai Igazgatóság által biztosított központi e-mail cím, illetve postafiók) fogadható el;
b) minden egyetemi felhasználó egyedi e-mail címet kap, azt kizárólag a felhasználó maga veheti igénybe;
c) a felhasználó azonosítójának és jelszavának átadása más felhasználó részére tilos;
d) a munkahelyi e-mail címmel magánjellegű regisztrációt tenni különböző szabadon hozzáférhető, nem a munkavégzés céljával összeegyeztethető weboldalakon tilos;
e) a felhasználó elektronikus levelezésébe incidens megalapozott gyanúja esetén az IBF az informatikai igazgató engedélye alapján, a vonatkozó adatvédelmi és egyéb jogszabályi feltételek biztosítása mellett, betekintést nyerhet az informatikai és biztonsági szolgáltatókkal együttműködve;
f) az elektronikus üzenetek bizalmasságának, illetve hitelességének, letagadhatatlanságának védelme érdekében – az adatok biztonsági osztályba sorolásának megfelelően –aláírást (teljes név, beosztás és szervezeti egység) és titkosítást kell alkalmazni;
g) az egyetemi polgár köteles a jogviszonyával kapcsolatban tudomására jutott üzleti titkot megőrizni, ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot, amely foglalkoztatásra irányuló jogviszonya, hallgatói jogviszonya betöltésével összefüggésben jutott a tudomására, és amelynek közlése az egyetemre vagy más személyre hátrányos következménnyel járhat;
h) az elektronikus levél mérete, a hozzá csatolható állománnyal együtt nem haladhatja meg a mindenkori szolgáltató által meghatározott korlátot, az ennél nagyobb levelek nem kerülnek elküldésre;
i) a felhasználók kötelesek rendszeresen frissíteni e-mail fiókjaik jelszavát, és biztosítani azok erősségét az Egyetem által meghatározott jelszópolitika szerint;
j) a felhasználóknak részt kell venniük az éves információbiztonsági képzésen és az azt követő teszten, amelynek célja az információbiztonsági tudatosság növelése;
k) a felhasználók kötelesek azonnal jelenteni az PTE IT Ügyfélszolgálatnak minden gyanús e-mailt, csatolmányt vagy linket, amelyet nem vártak, vagy amely biztonsági fenyegetést jelenthet. Ennek legegyszerűbb módja, az eredeti gyanús levél továbbítása az sd@pte.hu e-mail címre;
l) a hivatalos kommunikáció során az érintett felhasználók kötelesek aláírást (teljes név, beosztás és szervezeti egység) használni, különösen érzékeny vagy bizalmas információk továbbítása esetén;
m) a felhasználók nem tárolhatnak egyetemi e-mail fiókjukban olyan személyes adatokat vagy információkat, amelyek nem kapcsolódnak közvetlenül az egyetemi tevékenységükhöz;
n) a felhasználók kötelesek az e-mail fiókjaikhoz való hozzáférést megfelelően védeni, beleértve a kéttényezős hitelesítés alkalmazását, ha az elérhető.

(3) Az e-mailek küldésére vonatkozó főbb előírások az alábbiak:

a) a feladó köteles együttműködni az információbiztonsági kockázatok csökkentésében, ennek keretében különösen gondoskodnia kell annak ellenőrzéséről, hogy a címzettek jogosultak az emailben foglalt tartalom megismerésére, köteles továbbá a biztonsági eljárások betartására, a káros tartalmak elkerülésére és az adatvédelmi jogszabályoknak való megfelelésre;
b) más felhasználó nevében e-mailt küldeni tilos, kivéve a rendszerbeli meghatalmazási eljárás alkalmazásán keresztül (pl. asszisztens), továbbá a kifejezetten ilyen célra létrehozott alkalmazásokon és rendszereken, mint (pl.: hírlevélküldő);

c) a felhasználók kötelesek rendszeresen ellenőrizni e-mail fiókjaik tartalmát és törölni a szükségtelen vagy lejárt érvényességű üzeneteket, ezzel is csökkentve a biztonsági kockázatokat;
d) a rendszer a törölt elemeket meghatározott napig tárolja, utána véglegesen törlődnek a levelező rendszerből;
e) a leveleket mindig célzottan kell kiküldeni, a címzettek számosságára és megjelenítésére vonatkozó korlátozások figyelembevételével (a címzettek számát minimalizálni szükséges, csak a tárgyhoz köthető foglalkoztatottak részére címezzük, kivéve hírlevelek;
f) a címzettek listáját minden egyes küldés előtt gondosan ellenőrizni kell;
g) automatikus válaszüzenetek tartalmát minden esetben úgy kell meghatározni, hogy a benne megadott információkkal rosszindulatú fél ne tudjon visszaélni;
h) a felhasználók nem hozhatnak létre automatikus továbbítási szabályokat, amelyekkel a munkahelyi email fiókjuk tartalmát külső címekre irányítják, kivéve, ha erre kifejezett engedélyt kaptak az Egyetemtől;
i) az Egyetem levelezőrendszerében tiltott a lánclevelezés, a kéretlen levelek (spam) tartalmak küldése. (A vizsgálat során biztosítani kell, hogy csak és kizárólag a biztonsági eseményhez kapcsolódó levelek kerüljenek vizsgálat alá);
j) az elektronikus levelezési rendszerbe beérkező leveleket minden esetben ellenőrizni kell, hogy nem tartalmaznak-e valamilyen, az Egyetem informatikai rendszerét veszélyeztető programot, kódrészletet, scriptet;
k) tilos a címinformáció hamisítása vagy a fejléc egyéb módon történő módosítása a feladó vagy a címzett személyazonosságának elrejtésére;
l) tilos vírusos levelek szándékos küldése;
m) tilos üzleti szempontból titkos, bizalmas, illetve belső információk jogosulatlan nyilvánosságra hozatala;
n) tilos minden ismeretlen kiterjesztésű e-mailhez csatolt állomány megnyitása;
o) tilos ismeretlen feladótól származó nem üzleti célú levelekben található csatolmány megnyitása; p) tilos kéretlen levelek küldése, továbbítása;
q) tilos valótlan információt hordozó levelek tudatos továbbítása;
r) tilos az elküldött levél járulékos adatainak (pl. feladó e-mail címe, küldés időpontja) meghamisítása;
s) tilos privát postafiók tartalom automatikus továbbítása munkahelyi e-mail címre;
t) tilos az Egyetem elektronikus levelezési címjegyzékének kiadása harmadik fél számára.

(4) Az e-mailek fogadására vonatkozó főbb irányelvek az alábbiak:
a) Bizalmas információk továbbítását kérő elektronikus levelek esetében mindig meg kell győződni az információkérés hitelességéről;
b) ismeretlen, gyanús feladótól érkezett csatolmányok, linkek megnyitása tilos. Kérdéses tartalmak megnyitása esetén a felhasználónak PTE IT Ügyfélszolgálatához kell fordulnia;
c) téves címzés miatt kapott e-mailt, annak felismerése után a felhasználónak haladéktalanul jeleznie kell a feladó- és a PTE Ügyfélszolgálata felé, és a levél tartalmának olvasása nélkül törölni kell. Az abban lévő tartalmak, információk, adatok jogtalan megismerése és kezelése tilos.
d) a felhasználók kötelesek minden kapott e-mail tartalmát hitelességi és biztonsági szempontból ellenőrizni, különösen, ha az ismeretlen feladótól származik.

(5) Az egyetemi elektronikus levelezési rendszeren keresztül küldött e-mailek naplózásra kerülnek biztonsági és audit célokra. A naplózott adatokhoz való hozzáférés szigorúan szabályozott, és csak az erre kijelölt biztonsági személyzet férhet hozzá a vizsgálatok során. A felhasználók kötelesek aktívan részt venni az

Egyetem által szervezett biztonsági auditokban és ellenőrzésekben, és minden szükséges információt megadni az auditoroknak.

(6) A felhasználók kötelesek az e-mailek küldésekor és fogadásakor betartani a levélszűrésre és vírusvédelemre vonatkozó előírásokat, és együttműködni a PTE IT Ügyfélszolgálattal minden gyanús tevékenység jelentése és kezelése során.