Távmunka információbiztonsági szabályai

Tartalom

1. ELEKTRONIKUS LEVELEZÉSRE VONATKOZÓ ELŐÍRÁSOK

Az otthonról, távmunkában elektronikus levelezési rendszeren keresztül végzett munkatevékenységre a munkahelyen végzett tevékenységre vonatkozó információbiztonsági szabályok érvényesek.

A Szegedi Tudományegyetem – a saját levelező domain-jében biztosított e-mail címmel és levelező rendszeren – az elektronikus levelezési szolgáltatást kizárólag munkavégzés céljából, a munkaköri feladatok hatékonyabb ellátásának érdekében biztosítja. Az elektronikus levelezés használati engedélye személyre szóló, azt kizárólag a felhasználó saját maga veheti igénybe. Szegedi Tudományegyetemmel közalkalmazotti jogviszonyban lévő felhasználó az E-Mail címet automatikusan megkapja, és a jogviszony idejéig igénybe veheti. Egyéb jogviszonnyal rendelkező felhasználó számára E-Mail címet a szervezeti egység vezetője igényelhet.
Az elektronikus levelezést, mint kommunikációs és irányítási eszközt az adott munkakör és munkavégzés feltételeihez igazítottan kell alkalmazni. Az alkalmazás szabályait az adott munkakört betöltőkkel meg kell ismertetni.

A munkahelyi e-mail címmel magánjellegű regisztrációt tenni tilos.

- Az ingyenes levelezőrendszerek (pl. freemail.hu, gmail.com) munkavégzés céljára történő használata tilos.
- A felhasználó saját azonosítójának és jelszavának átadása más felhasználók részére tilos.
- Helyettesítés és távollét esetén a levelezés továbbításának szabálya beállítható, a válaszlevelek küldése esetében az érintett helyettesítő személy rendszerbeli meghatalmazása a helyes, hivatalos eljárás.
- Az elektronikus levelek és csatolmányok kapcsán alkalmazandó intézkedések védelmi szintje megegyezik az abban megjelenő információk, adatok érzékenységi besorolása kapcsán alkalmazandó intézkedések védelmi szintjével.
- A felhasználó részére biztosított fiókok, tárhelyek archiválását a rendszer automatikusan elvégzi, azok rendszeres karbantartása, kiürítése, saját célú archiválása a felhasználó feladata.
- A felhasználók csak a saját postaládájukat és jogosultság alapján a kezelésébe rendelt technikai postafiókokat tudják kezelni, mások postaládáit nem láthatják.

1.1.Az e-mailek küldésére vonatkozó előírások

- A feladó, mint tulajdonos felelős az e-mail tartalmáért.
- Más felhasználó nevében e-mailt küldeni tilos, kivéve a rendszerbeli meghatalmazási eljárás alkalmazásán keresztül (pl. titkárnő).
- Zavaró, félreinformáló levelek küldése, jogtalan megrendelések elindítása TILOS és fegyelmi eljárást vonhat maga után.
- A leveleket mindig célzottan kell kiküldeni, a címzettek számosságára és megjelenítésére vonatkozó korlátozások figyelembe vételével.
- Mivel a Szegedi Tudományegyetemen használatban lévő levelező rendszerek jellemzően 10 MB méretben maximalizálják a küldhető adatmennyiséget, az ezt meghaladó méretű adatmennyiség esetében javasoljuk az adminisztrációs CooSpace felület használatát. (Az oktatási CooSpace használata nagy adatmennyiség megosztása céljára nem javasolt.)
- A szervezet levelezőrendszerében TILTOTT a lánclevelezés, valamint a kéretlen levelek (spam) küldése!
- Bizalmas, érzékeny személyes adatok, információk csak titkosított módon küldhetők elektronikus levélben,

- A levelező rendszer rendeltetésétől és a munkaköri feladatoktól eltérő, zavaró, félreinformáló levelek, tartalmak küldése, tilos.

1.2.Az e-mailek fogadására vonatkozó irányelvek

- A címzett felelős az e-mailek fogadásáért, annak tartalomtól függő feldolgozásáért az adott munkakörre meghatározott feltételek szerint.
- Bizalmas információk továbbítását kérő elektronikus levelek esetében mindig meg kell győződni az információkérés hitelességéről.
- Ismeretlen helyről származó, a levelező rendszer rendeltetésével nem összefüggő vagy nem összeegyeztethető tartalmú e-mailt vagy különösen annak csatolmányát megnyitás nélkül, olvasatlanul törölni kell.
- Téves címzés miatt kapott e-mailt, annak felismerése után annak tartalmának (további) olvasása nélkül ki kell törölni. Az abban lévő tartalmak, információk, adatok jogtalan megismerése és kezelése tilos!
- Az ismétlődően, ugyanabból a forrásból kapott téves címzés esetén – megfelelő körültekintéssel és helyzetértékelés mentén – jelezzen vissza a küldő félnek.
- Külső vagy belső e-mail címről érkező, félrevezető tartalmú, feltehetően ártó szándékú e-mail-ek esetén azonnal értesíteni kell a rendszergazdát és a munkahelyi vezetőt.
- A kapott e-mail mellékleteket először számítógépes víruskeresővel – a rendszeresített eszközöket és beállításokat felhasználva – kell átvizsgálni, különösen, ha azok pl. futtatható programokat tartalmaznak.

1.3.A felhasználók felelőssége

- A **„Távmunka Információbiztonsági Szabályai”** előírásainak megsértése, (akár szándékosan, akár gondatlanságból), felelősségre vonást eredményezhet.
- A felhasználó felelősséggel tartozik munkaidőtől függetlenül:
- A szabályok betartásáért, az engedélyezett és működő biztonsági megoldások használatáért.
- Az általa hozzáférhető adatok és információk bizalmas, az adat biztonsági osztályának megfelelő kezeléséért.
- Az általa rögzíthető vagy módosítható adatok és információk adatrögzítés vagy módosítás során elvárt pontosságáért és teljességéért.
- A számára kiosztott felhasználónevét, jelszavát köteles titokban tartani, azt másnak tilos átadni.
- A felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az informatikai rendszerben.
- Az általa használt eszközök (számítógép, nyomtató, szkenner, stb.) és informatikai rendszerek szoftvereinek, szolgáltatásainak szakszerű és rendeltetésszerű kezeléséért.
- A használatra átvett eszközök megfelelő fizikai védelméért, különös tekintettel a hordozható adathordozókra és számítógépekre.

1.4.A felhasználók jogai

A felhasználó jogosult:

- A számára biztosított informatikai eszközök, szoftverek rendeltetésszerű használatára.
- A beállított jogosultságának megfelelően, a munkájához szükséges adatok és rendszerfunkciók elérésére.
- A munkahelyi vezetője részéről jóváhagyott informatikai és informatikai biztonsági képzésre.

- A számítástechnikai eszközök (szoftver, hardver) működtetéshez szükséges támogatás igénylésére.
- Meghibásodás, üzemzavar esetén a szolgáltatási szerződés feltételeinek megfelelő időn belüli elhárítás igénylésére.

1.5.A felhasználók kötelessége

A felhasználó köteles a használatába adott informatikai eszközök meghibásodása esetén a rendszergazdájánál, illetve a jogosultsági körébe tartozó központi informatikai rendszerek, vagy azok funkcióinak hibája esetén a meghibásodást a rendszer üzemeltetőjénél maradéktalanul jelezni.
Hibabejelentés során a felhasználó köteles a kért információkat maradéktalanul megadni:

- Személyre szóló felhasználói azonosító a jogosult informatikai rendszerekhez.
- Internet-szolgáltató adata.
- A felhasználó számára átadott számítástechnikai eszközök azonosítói (leltári szám, gyári szám).
- A felhasználó köteles együttműködni a rendszergazdával a helyzet kivizsgálása során.
- A felhasználónak fel kell jegyeznie a hibajelenséget, és a képernyőn megjelenő hibaüzenetet – ha mód van rá, akkor a képernyőkép kimentésével (Alt + PrintScreen billentyűkombinációt használva), majd egy új dokumentum létrehozása után abba történő beillesztéssel meg kell őriznie, illetve továbbítania kell szervezeti egysége rendszergazdája felé.
- Az információbiztonsági előírásokat maradéktalanul betartani.

2. A SZÁMÍTÓGÉP ÜZEMELTETÉSÉRE, HASZNÁLATÁRA VONATKOZÓ ELŐÍRÁSOK

2.1. Tiszta asztal, tiszta képernyő politika (clear desk policy) betartása

- Munkavégzés során (lehetőleg) csak azok az adathordozók legyenek elől az asztalon, képernyőn, amelyek az adott munka végzéséhez akkor szükségesek.
- A számítógépes asztalon minél kevesebb alkalmazás, dokumentum legyen egyidejűleg megnyitva, lehetőleg csak azok, amelyek az adott munka végzéséhez akkor szükségesek.
- Munkavégzés megszakításakor minden érzékeny információt és adatot tartalmazó információhordozót el kell tenni az asztalokról, el kell távolítani az előállításra használt eszközből (pl. CD, DVD, pendrive a számítógépből), és elzárt helyre kell biztonságba helyezni.
- Munkavégzés megszakításakor a jegyzeteket, vázlatokat, téves példányokat, az eredetiekkel azonos biztonsági szinten kell kezelni, vagy ha nem szükségesek, megsemmisíteni.
- A számítógép rövid idejű elhagyása esetén megfelelő eljárással (zárolás, jelszavas képernyővédelem alkalmazása) gondoskodni kell arról, hogy kívülállók ne tekinthessenek be rendszerbe.
- Hosszabb idejű – kb. 1 órán túli - távollét esetén ki kell jelentkezni az alkalmazásokból, és a számítógépet ki kell kapcsolni.

2.2. A számítógép üzemeltetésére vonatkozó előírások

- Minden felhasználó köteles az általa használt számítógépet rendeltetésének megfelelően, kizárólag munkájának végzésére, illetve támogatására használni.
- Minden felhasználó köteles az esetleges meghibásodásokat azonnal jelezni a rendszergazdának, és a közvetlen munkahelyi vezetőnek.
- A számítógépet (vagy egyéb informatikai eszközöket) üzem közben letakarni, a szellőző nyílásokat eltakarni, a klimatizációjukat biztosító berendezések beállításait módosítani szigorúan tilos.
- A számítógép (vagy egyéb informatikai eszköz) burkolatát tilos megbontani, az eszköz belső részéhez hozzáférni, azon változtatásokat végezni. A garancia címke épségét folyamatosan fenn kell tartani.
- A telepített (nem hordozható) számítógépet (vagy egyéb informatikai eszközt) a rendszergazda értesítése nélkül tilos más munkahelyre áttelepíteni.
- A használatába kapott számítógép (vagy egyéb informatikai eszközök) konfigurációját a felhasználó által megváltoztatni tilos. A perifériák cseréjét, szoftverek telepítését csak a rendszergazda végezheti.

2.3. A számítógép használatára vonatkozó előírások

- A Szegedi Tudományegyetem tulajdonát képező vagy általa bérelt számítógépek magáncélra vagy személyes haszonszerzésre irányuló felhasználása, valamint az eszközök kezelésére, üzemeltetésére vonatkozó szabályokkal ellenkező módon történő felhasználása szigorúan tilos.

- A felhasználó a rendelkezésre bocsátott számítógépet, perifériát, alkalmazást csak saját azonosítójával és jelszavával belépve használhatja. Lehetőségeinek keretében felelős a saját azonosítójával és jelszavával való visszaélés megakadályozásáért.
- A rendszergazda által installált jelszavas képernyővédő törlése vagy várakozási idejének megváltoztatása TILOS.
- A felhasználó a használatba vett számítógépen a munkájához szükséges új szoftver-igény kielégítését a szervezeti vezetőjén keresztül kezdeményezheti.
- A felhasználó alapértelmezés szerint standard felhasználó (nem rendszergazda) a saját gépén.
- A felhasználó a használatba vett számítógépen semmilyen szoftvert nem telepíthet, nem törölhet, és nem módosíthat. E rendelkezés megszegéséért a felhasználó ellen felelősségre vonás kezdeményezhető.
- A felhasználó semmilyen olyan szoftvert nem futtathat a számítógépén, amit nem a rendszergazda telepített. (Ebbe beleértendők a telepítést nem igénylő, külső eszközről – pl. CD/DVD-ROM, USB Flash drive, stb. – indítható programok, valamint a freeware, shareware szoftverek, illetve bármilyen nem a munkáltató által biztosított szoftverek.)
- A számítógép külső egységről vagy perifériáról történő indítását (külső boot-olást) tilos alkalmazni.
- A felhasználó a Szegedi Tudományegyetem tulajdonát képező vagy általa bérelt számítógépeken csak azokat a szoftvereket használhatja, amelyeket a munkáltató megrendelésére a rendszergazda a munkája elvégzéséhez telepített.

3. EGYEDI ELŐÍRÁSOK HORDOZHATÓ MOBIL ESZKÖZÖKRE

3.1.Mobil eszköz használat

- A felhasználók mobil eszközei alatt azokat a hordozható, egyetemi vagy nem egyetemi tulajdonú elektronikus médiákat (a továbbiakban média) értjük, melyek beépített képességeik révén képesek szöveges, képi, hang és videó információkat tárolni és visszaadni egyéb segédeszköz alkalmazása nélkül. A médiákat a felhasználók az intézmény területén beszéd hívásra használhatják. A hívás során ügyelni kell arra, hogy összekapcsolható személyes adatokat (a továbbiakban szenzitív információkat) illetéktelenek ne hallhassanak, helyben sem és a távoli végen sem. A videó hívások esetében a hanghívások szabályai érvényesek, továbbá ügyelni kell arra, hogy a közvetített kép ne tartalmazzon szenzitív információt. Egyébként szigorúan tilos a médiákon tárolni szenzitív információt tartalmazó dokumentumot, képet, hanganyagot, videót. Szigorúan tilos a médiák felhasználásával szenzitív információt megosztani adatkezelésre jogosulatlan személlyel, szervezettel.
- Mobil eszköz: Mobil eszköz alatt azt a hordozható elektronikus médiát értjük, mely beépített képességei révén képes szöveges, képi, hang és videó információkat tárolni és visszaadni egyéb segédeszköz alkalmazása nélkül. Ilyen például a klasszikus mobil telefon, okos telefon, tablet, laptop, phablet, okos óra, okos szemüveg, fényképezőgép, videó kamera, stb. A mobil eszközök kizárólag munkavégzésre használhatóak

3.2.Az eszközök üzemére vonatkozó általános előírások

- Ne tegye ki mobil eszközét extrém hőmérséklet, mágneses tér, magas páratartalom, erős füstképződés vagy por hatásának.
- Amennyiben nem használja a mobil eszközét, kapcsolja ki és tartsa elzárva. Ha nem lehetséges elzárni, alkalmazzon biztonsági zárat.
- Repülőutak alkalmával a mobil eszközt kézipoggyászként szállítsa. Lehetőség szerint kerülje el a röntgenkészülékkel történő vizsgálatot.
- Külföldi hivatalos útra való utazás előtt ismerje meg a fogadó ország információhordozók, programok és adatok szállítására vonatkozó vám, kiviteli és beviteli előírásait, biztonsági szabályait, és az érintett eszközöket, tartalmakat ezek figyelembe vételével készítse elő az utazásra. Szükség esetén gondoskodjon a szükséges engedélyek beszerzéséről.
- Gondoskodjon megfelelő és időben elegendő áramellátásról – a felhasználási hely sajátosságainak és adottságainak figyelembe vételével.

3.3.Lopás elleni kockázatok csökkentése

- A mobil eszközöket tilos gépkocsiban hagyni vagy tárolni, illetve bárhol felügyelet nélkül szabadon hagyni, kivéve, ha az eszköz és a rajta tárolt adatok érzékenységének megfelelő, kívülről nem látható, zárt biztonsági tárolóban vannak elhelyezve.
- Ügyfélnél, konferencián, vásárokon, illetve egyéb nyilvános helyen való használatkor az erre felkészített, alkalmas eszközök esetén (lehetőleg) használjon ún. Kensington-Lock jellegű biztonsági zárat, amelyet az adott helyen egy elmozdíthatatlan tereptárgyhoz rögzít.
- Szállodában, konferencián, vásárokon, illetve egyéb nyilvános helyen használja a beépített egyedi biztonsági tárolási eszközöket (pl. széf), megőrzőket.

3.4.Adatbiztonsági szabályok

- Érzékeny információ, adat csak az érzékenységnek megfelelő biztonsági osztály szerint meghatározott tartalomban, terjedelemben és formátumban, a meghatározott védelmi eljárások alkalmazásával tárolható és kezelhető hordozható eszközön.
- A külső munkahelyen történő feladat elvégzése után a mobil eszközökön keletkezett vagy tárolt adatokat minősítésüknek megfelelően a hálózati fájlszerverekre, vagy a saját használatú számítógépének központi szerveren definiált privát területére kell menteni, és ezt követően a hordozható számítógépről le kell őket törölni.
- A mobil eszközökön lokálisan tárolt adatok rendszeres mentéséről és törléséről a felhasználó maga köteles gondoskodni.

3.5.Illetéktelenek általi, információhoz való hozzáférések megakadályozása

- Saját használatú eszköz hálózaton történő megosztása tilos.
- Nyilvános helyeken történő használatnál ügyelni kell arra, hogy a nem közlésre szánt tartalmakat illetéktelenek ne láthassák, és ne olvashassák, ne férjenek hozzá.
- Gondoskodjon arról, hogy senki se készíthessen észrevétlenül másolatokat az Ön eszközén található elektronikus adatállományairól.
- Gondoskodjon arról, hogy ott, ahol a hordozható számítógépet megosztva használják, a használatot követően a tárolt adatok törlésére kerüljenek.
- A mobil eszközök rövid idejű elhagyásakor is azonnal zárolja az eszközt, ezzel megakadályozva azt, hogy kívülállók betekinthessenek rendszerébe, adataiba.

3.6.Fokozott vírusveszély kockázatainak csökkentése

- A rendszergazda által installált központi vírusvédelmi rendszer használata kötelező.
- Az idegen külső adathordozók (pl. optikai adathordozók, külső merevlemezek, USB flash drive-ok) vírusmentességét felhasználásuk előtt a felhasználónak kötelező megvizsgálni.
- A mobil számítógép külső hálózatra kapcsolódását (pl. szállodákban, vásárokon, beszállítóknál, otthon, stb.) követően, a Szegedi Tudományegyetem hálózatára csatlakoztatott használata előtt manuálisan indított, teljes gépre vonatkozó vírusellenőrzést kell végrehajtani.

3.7.Hálózati fájlszerverekre való távoli csatlakozás esetén

- Csak a feltétlenül szükséges adatokat vigye át mobil számítógépére, egyéb eszközére.
- A távoli (host) kapcsolatot rögtön bontsa, amikor arra már nincs szüksége.

3.8.Intézkedések, ha a hordozható eszközt ellopták vagy elveszítették

- Az ellopás, elvesztés tényét a lehető leggyorsabban jelenteni kell a rendszergazdának valamint a közvetlen felettes vezetőnek.
- A rendszergazda felé közölni kell, hogy az eszköz tartalmaz-e a Szegedi Tudományegyetem IT rendszereihez távoli hozzáférési lehetőséget.
- A közvetlen felettes vezetőt tájékoztatni kell arról (előzetesen szóban, majd ahogyan lehetőség adódik erre, a meghatározott formátumban írásban is), hogy az eszköz tartalmaz-e bárminemű érzékeny információt, adatot, és javaslatot megfogalmazva a szükség szerinti védelmi intézkedésekre.
- Idegenkezűség és annak gyanúja esetén rendőrségi és/vagy a helyszín biztonsági szolgálata által jegyzőkönyvet kell felvetetni az eset körülményeiről.

3.9.Adathordozók használata

- A munkavállaló a munkaköri feladatához biztosított mobil adathordozókat, függetlenül az adatok rögzítésének módjától, köteles biztonságosan őrizni, és védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.
- Az adatokról készült másolatok érzékenysége megegyezik az eredeti adat érzékenységével, ezért azonos szinten kell védeni a másolatokat is.
- A hordozható adathordozókon lévő adatok illetéktelenek általi hozzáféréséért a felhasználó a felelős. Törekedni kell biztonsági jelszóval védett adathordozó használatára. Konzekvensen használja ki az adathordozók írásvédettségi lehetőségeit.
- Egyértelmű külső jelöléssel, formalizált és egyedi azonosítóval (iktatószámmal) lássa el az adathordozókat.
- Gondosan és elzárva tárolja az adathordozókat, amikor használaton kívül vannak.
- Azokat a mobil adathordozókat, amelyeket privát számítógéppel történő adatcserére használt, újrafelhasználás előtt vizsgálja át vírusellenőrzővel, illetve szükség szerint formázza újra.