Ikt.sz.: SZFE/1094/2024

SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

SZFE 1865

7/2024. (05.06.) számú rektori szabályzat

A Színház-és Filmművészeti Egyetem Felhasználói Szabályzata

Hatályos: 2024. május 07. napjától

1.§
A jelen szabályzat célja

(1) A jelen felhasználói szabályzat (a továbbiakban: Szabályzat) célja, hogy a Színház- és Filmművészeti Egyetem (továbbiakban: Egyetem) által biztosított elektronikus információs rendszerek, alkalmazások informatikai eszközök és szolgáltatások felhasználói megismerjék a rájuk vonatkozó kötelezettségeket és szabályokat.

(2) A Szabályzat általános célja továbbá, hogy az Egyetem által használt és működtetett információs rendszer biztonságát garantáló eljárások és előírások átlátható és nyomon követhető formában egységes keretbe foglalva rögzítésre kerüljenek.

2.§
A jelen Szabályzat hatálya

(1) A Szabályzat személyi hatálya kiterjed az Egyetem valamennyi szervezeti egységére, az Egyetemmel hallgatói jogviszonyban álló diákokra akik feladataik teljesítése során vagy egyéb céllal, jogosultsággal, vagy annak hiányában felhatalmazással, az Egyetem által biztosított informatikai eszközöket, alkalmazásokat és szolgáltatásokat (továbbiakban együtt informatikai rendszert) használnak, adatokat vagy dokumentumokat, információkat hoznak létre, tárolnak, használnak vagy továbbítanak, valamint azokra, akik ilyen tevékenységekkel kapcsolatosan döntéseket hoznak.

(2) A Szabályzat hatálya kiterjed az Egyetem által foglalkoztatott valamennyi munkavállalóra, illetve munkavégzés céljából egyéb jogviszonyban álló jogi és természetes személyre.

(3) A Szabályzat tárgyi hatálya kiterjed:
- a) az Egyetem által biztosított, felhasználók által használt információs rendszerekre, függetlenül attól, hogy azt a szervezet vagy más vállalkozó üzemelteti;
- b) egyes papír alapon rögzített, tárolt, használt vagy továbbított adatokra;
- c) a számítógépes feldolgozásra szánt, feldolgozás alatt álló, és a feldolgozás után számítógépes adathordozókon tárolt, a feldolgozás eredményeként létrejött adatra;
- d) a számítástechnikai eszközök (laptop, mobiltelefon, egyéb adathordozók, belépőkártyák) alkalmazásának (kiadás, használat, visszavétel) teljes folyamatára, tevékenységeire.

3.§
A Szabályzat elkészítése felülvizsgálata és módosítása

(1) A Szabályzat elkészítése, felülvizsgálata és szükség szerinti módosítása az információbiztonsági felelős ő ki- Rektori Hivatal vezetője? feladata és felelőssége, együttműködve az Egyetemvezetőségével.

(2) A Szabályzatot legalább évente felül kell vizsgálni és szükség esetén módosítani kell.

4.§
Rendkívüli felülvizsgálat

(1) A jelen Szabályzatot az időszakos felülvizsgálaton túl felül kell vizsgálni és szükség esetén módosítani kell:
   a) a Szabályzatban hivatkozott szervezetek vagy munkakörök változása esetén;
   b) súlyos információbiztonsági események bekövetkezése esetén;
   c) az információs vagy informatikai biztonság szabályozását érintő jogszabályváltozások esetén;
   d) az információs vagy informatikai rendszer nagy mértékű változása esetén.

(2) A felülvizsgálatok eredményéről az információbiztonsági felelős tájékoztatja az Egyetemvezetőségét.

5.§
A Szabályzat betartásának ellenőrzése

A Szabályzat betartásának ellenőrzése az információbiztonsági felelős feladata, melyben közreműködnek az információbiztonsági feladatok ellátásában közreműködő személyek, szervezeti egységek, munkacsoportok, valamint az elektronikus információs rendszer üzemeltetéséért, fejlesztéséért felelős szervezeti egység vezetője.

6.§
Kivételkezeléssel kapcsolatos feladatok

(1) Kivétel alatt kell érteni minden olyan technológiai kontroll nem teljesülését, mely a jelen Szabályzatban rögzített követelményeket nem tudja teljesíteni.

(2) A jelen Szabályzattól való kivételeket minden esetben jegyzőkönyvben dokumentálni szükséges, illetve rendszerek esetében az adott rendszer rendszerbiztonsági tervében kell dokumentálni. A kivételek bevezetése a rektor engedélyével történhet.

7.§
Felhasználókra vonatkozó rendelkezések

(1) A felhasználóknak a felhasználási jogosultságuk első napjától szükséges az Egyetem üzleti információit a titoktartási elvárásoknak megfelelően kezelni és a vonatkozó egyetemi belső szabályokat betartani.

(2) Minden felhasználónak kötelessége évente információ biztonsági oktatáson részt venni.

(3) Az Egyetem minden felhasználója saját egyedi felhasználói azonosítót kap, valamint minden fő informatikai alapszolgáltatást, alkalmazást, így internet, levelezés és alap irodai alkalmazáscsomag használatára jogosult. Egy felhasználói fiókot nem használhat több személy.

(4) A felhasználó köteles az Egyetem információs rendszereinek használata során birtokába kerülő üzleti titkokat és személyes adatokat megőrizni.

(5) Az Egyetem tulajdonát képező, valamint a felhasználó által közvetlenül a munkavégzésére használt fájlokat és mappákat nem javasolt a számítógép lokális meghajtóján tárolni, az ilyen jellegű fájlokat

és mappákat a hálózati meghajtókon javasolt elhelyezni. A nem megfelelő helyen tárolt, és nem megfelelően védett információk és dokumentumok hardveres- és vagy egyéb üzemzavarból, elvesztésből fakadó rendelkezésre nem állása / illetéktelen kezekbe kerülése a felhasználók felelőssége.

(6) Az informatikai rendszer erőforrásaihoz, valamint a különböző meghajtókhoz, mappákhoz, almappákhoz, fájlokhoz történő hozzáférés a felhasználók számára jogosultság alapján korlátozott. Mindennemű változás a jogosultsági rendszerben kizárólag a Rektori Hivatal vezetőjének engedélye alapján történhet. A módosítások technikai érvényesítéséről az informatikai szakterület gondoskodik.

(7) A felhasználónak joga van az Egyetem informatikai eszközeit és az Egyetemnél fellelhető informatikai szolgáltatásokat a munkavégzés érdekében, rendeltetésszerűen használni. Az Egyetem informatikai rendszereinek technikai problémáiról (tervezett vagy rendkívüli eseményekről) a felhasználónak joga van értesülni. Erre a célra az Egyetem elektronikus levelezési rendszerét használja.

(8) A felhasználó felelős azért a számítógépért vagy bármely más informatikai vagyontárgyért, adatvagyonért, szoftvervagyonért, amelyen munkát végez. A felhasználó felelős minden műveletért, amely felhasználói azonosítójával kerül végrehajtásra.

(9) Az Egyetem által biztosított eszközökkel kapcsolatosan a felelősség a következő tevékenységekre terjed ki:

a) állagmegóvó tárolásra,
b) rendeltetésszerű használatra,
c) adatvagyon és szoftvervagyon védelmére sérülés, károsodás, elvesztés vagy adatszivárgás ellen,
d) a saját számítógépén és megosztott mappáin lévő állományokra,
e) az informatikai eszközök, perifériák, beviteli eszközök tisztántartására.

(10) A felhasználó köteles a rá vonatkozó szabályzatokban foglaltakat megismerni és betartani. A felhasználó köteles a rábízott berendezéseket, szoftvereket és adatvagyont munkakörének megfelelően, a kezelési utasítások szerint, a tőle elvárható gondossággal rendeltetésszerűen használni.

(11) A felhasználó köteles állományai, adatai között rendet tartani saját számítógépén és a file szerveren (M365) egyaránt, azaz köteles a fájlokat áttekinthető módon tárolni és kerülni a redundanciát. A felhasználó köteles takarékoskodni az informatikai erőforrásokkal, így például az energiával, sávszélességgel, tárkapacitással stb.

(12) A felhasználó köteles együttműködni az informatikai eszközök üzemeltetését végző szakemberekkel, rendszergazdával vagy az Egyetem információtechnológiai infrastruktúrájához vagy rendszereihez szerződéses keretek között hozzáférő partnerekkel.

(13) A felhasználó, amennyiben szabálytalanságot tapasztal, köteles más felhasználókat is figyelmeztetni a nem rendeltetésszerű vagy a szabályzatokba, jogszabályokba ütköző használat tilalmára.

8.§
Felhasználókra vonatkozó tiltások

(1) Tilos az Egyetem bármilyen informatikai eszközén hackertevékenységet végezni vagy ezt bármilyen módon elősegíteni, illetve eltűrni.

(2) Tilos a szoftver licensz, illetve a szellemi tulajdonnal kapcsolatos jogok megsértése, a szerzői joggal védett tartalmak másolása.

(3) Tilos illegális tartalmak, így például filmek vagy hangfájlok, torrentfájlok stb. letöltése, tárolása, másolása. A munkavégzéssel kapcsolatos ingyenes programok letöltése, tárolása vagy használata az Egyetem eszközein különös elővigyázatossággal és saját felelőségre történhet. Tiltott a nem jogtiszta, illegális programok letöltése, tárolása vagy használata.

(4) Tilos a felhasználónak a szervezet informatikai infrastruktúrájában bármilyen módosítást végrehajtása, a számítógépek vagy más informatikai eszközök szétszedése, megbontása, illetve a munkaállomások konfigurációjának megváltoztatása.

(5) Tilos jogosultságok (például jelszavak) más felhasználónak történő átadása, átengedése.

(6) Tilos a felhasználói azonosítók titkosítatlan (clear text) tárolása, illetve azok megosztása még szervezeten belül is. Amennyiben a felhasználói azonosítók (pl.: felhasználónév/jelszó) tárolása indokolt, akkor ezeket megfelelő titkosítású (pl. KeePass) rendszerben kell tárolni.

(7) A felhasználó az Egyetem számítógépein, illetve az Egyetem által biztosított egyéb tárhelyeken magánjellegű adatokat nem tárolhat.

9.§
Szankciók

(1) A Szabályzat megsértésének gyanúja esetén az esetet az információbiztonsági felelősnek kell kivizsgálnia, meg kell tennie a szükséges intézkedéseket, amelyre a következők az irányadók:

a) A Szabályzat előírásainak nem ismerete nem mentesít a következmények vállalásának kötelezettsége alól.
b) A Szabályzat gondatlan megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni.
c) A Szabályzat szándékos megsértése esetén az eset súlyosságától függően fegyelmi eljárás folytatható le a felhasználó ellen.

(2) A fenti (1) bekezdésben meghatározott vizsgálat eredményéről az információbiztonsági felelős tájékoztatja a rektort, valamint hallgatói felhasználó, valamint olyan munkavállalói felhasználó esetében, aki felett a munkáltatói jogkört a rektor gyakorolja a rektort, akik jogosultak dönteni a felhasználóval szemben alkalmazandó szankciókról.

10.§
Eszközök és jogosultságok

(1) Az eszközök és jogosultságok igénylésének folyamatának részleteit a Hozzáférésvédelmi Szabályzat tartalmazza. Fő szabályként minden jogosultságot és igénylést

a) új munkavállalók részére a Humán Erőforrás Iroda,
b) már dolgozó munkavállalók esetén azok közvetlen felettese,
c) hallgatók számára a rektor indíthat.

(2) A jogosultsági igényeket a Rektori Hivatal vezetője hagyja jóvá, a megfelelő beállításokat rendszergazda, vagy Rektori Hivatal vezetője által kijelölt személyek teszik meg a megfelelő rendszerekben.

(3) Az Egyetem által biztosított eszközöket az informatikus adja át a munkavállalóknak.

(4) Az Egyetem által biztosított laptoppal rendelkező felhasználók, a laptopot alkalmankénti engedélyezési procedúra nélkül jogosultak az Egyetem területéről kivinni.

11.§
Jelszókezelés és jelszóhasználat

(1) A jelszavakkal kapcsolatban az alábbi előírásoknak kell eleget tenni:

a) Jelszóként tilos a jelszó tulajdonosával kapcsolatba hozható szót, kifejezést használni, a jelszó nem lehet azonos a felhasználói azonosítóval.
b) A jelszavak nem lehetnek rövidebbek, mint 8 karakter.
c) A jelszavaknál komplex kódot kell használni, vagyis minimum tartalmaznia kell kis- és nagybetűket, 1 számot és 1 speciális karaktert (pl.: %,#,&,@,$).
d) A jelszavak nem lehetnek triviálisak, kitalálhatóak, nem lehetnek könnyen megjegyezhetők nem lehetnek köthetők a felhasználóhoz, annak bármely más azonosítójához (telefonszám, lakcím, név), nem lehet szótár alapú támadás esetében sem sérülékeny (értelmes szavak), nem tartalmazhat egymást követő csak számból, vagy csak betűből álló sorozatokat.

(2) Elfelejtett azonosítási információ (felhasználónév) esetén a felhasználó azonosítót az informatikus küldi meg a felhasználó kérésére sms-ben vagy emailben a felhasználó hitelt érdemlő azonosítása után. Az új azonosítót az **helpdesk@szfe.hu** email címen lehet igényelni.

(3) Elfelejtett hitelesítési információ (jelszó) esetén a felhasználó kérésére – a felhasználó hitelt érdemlő azonosítása után – új jelszó generálása szükséges az informatikus által. Az új jelszót az **helpdesk@szfe.hu** email címen lehet igényelni.

12.§
Adatvagyon kezelése, hozzáférése

(1) Az adatok kezelésével, illetve a számítógépes rendszer üzemeltetésével kapcsolatos feladatok ellátására felhatalmazott munkavállalók az adatokhoz csak a feladatuk ellátásához szükséges mértékben férhetnek hozzá.

(2) Az Egyetem adatvagyonát csak az Egyetem eszközein, illetve az Egyetem által biztosított rendszerekben, adattárhelyeken lehet kezelni (tárolni, módosítani, törölni…stb.) Kivételt jelent ideiglenesen - amennyiben máshogy nem megoldható – külső adattároló eszközök használata. Külső adattároló eszköz lehet a pendrive, mobiltelefon, illetve az otthoni számítógép is. Ezen eszközökön az Egyetem adatainak titkosított tárolása elvárt az adatok bizalmasságának megőrzése érdekében. Pendriveon jelszóval védett zip állományok; nem a szervezet tulajdonában lévő eszköz: részleges vagy teljes drive titkosítás (Veracrypt, Bitlocker…stb.) használata elvárt.

(3) Az adattárolásra engedélyezett tárhelyekhez (lokális, hálózati és felhő) hozzáférés minden munkavállalószámára a munkavégzéshez szükséges megfelelő jogosultságok biztosítása mellett korlátozottan biztosított.

(4) A biztosított tárhelyek nem használhatóak az alábbi tevékenységekre:

a) a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása;
b) a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység;
c) a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben igénybevevő tevékenység;
d) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, használatának megkísérlése;
e) a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység;
f) másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység;
g) hálózati üzenetek, hálózati eszközök hamisítása: olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna.

(5) A munkavállalókés a hallgatók számára elsődlegesen a Microsoft Cloud (Onedrive) használata javasolt a munkavégzéshez és a tanulmányokhoz szükséges adatok tárolására. Mindemellett a munkavállalók munkájának folytonosságát a munkavégzéshez biztosított informatikai eszközök (asztali számítógépek és laptopok) rendszeres Microsoft Cloudba (Onedrive) való mentése, biztosítja.

(6) Az automatikus mentés kiterjed a következő mappákra:

a) Dokumentumok,
b) Képek,
c) Asztal.

13.§
Hozzáférés az adathordozókhoz

(1) Az Egyetem elektronikus információs rendszerében minden felhasználó jogosult adathordozók használatára a kapcsolódó – egyes esetekben adathordozó specifikus (pl.: mobiltelefon, mentési adattároló) – szabályozások alkalmazása mellett.

(2) Az adathordozókat mindenkinek biztonságos helyen kell tárolni, védve azokat az illetéktelen hozzáféréstől, elvesztéstől. Ez a szabály nem mentesíti a felhasználót a mobil adathordozókon tárolt személyes adatok titkosítása alól, mely szükséges minden esetben.

(3) Az Egyetem tulajdonát képező számítástechnikai eszközöket, adathordozókat, kizárólag a információbiztonsági felelős engedélyével szabad kivinni az Egyetem területéről.

(4) Ez alól kivételt képez a felhasználó számára biztosított laptop, mobiltelefon, adattároló eszköz, mely eszközök szabadon kivihetők, ugyanakkor amennyiben védendő szervezeti adatot vagy személyes adatot tartalmaznak, az adatok titkosítása javasolt.

(5) Az Egyetem megtiltja az olyan hordozható adathordozók használatát az elektronikus információs rendszerben, melyek tulajdonosa nem azonosítható.

14. §
A felhasználó feladatai a munkahely elhagyásakor

(1) A munkavállaló a munkavégzés befejezése után köteles a számítógépet és a hozzá kapcsolódó eszközöket kikapcsolni. A munkaidő lejártát követően az irodát utoljára elhagyó munkavállaló köteles ellenőrizni, hogy minden számítástechnikai eszközt kikapcsoltak-e.

(2) A munkavállaló amennyiben szünetelteti munkavégzését és felügyelet nélkül hagyja számítógépét, úgy azt zárolni köteles.

(3) A munkaidő lejártát követően az irodát utoljára elhagyó munkavállaló köteles ellenőrizni, hogy az iroda minden helyisége, ablakai, ajtói zártak legyenek, és - ahol van – a biztonsági berendezések (pl. riasztó) élesítve legyenek.

15.§
Tiszta asztal és tiszta képernyő

(1) A munkavállaló mindig csak a munkával kapcsolatos dokumentumok tarthatja elérhetően az íróasztalon és a képernyőn. Az érzékeny / személyes adatokat tartalmazó dokumentumokat, IT adathordozókat, mobil eszközöket a munka végeztével, illetve hosszabb távollét esetén munkanap közben is megfelelően el kell zárni.

(2) Számítógép és mobil eszközök képernyő asztalaira egyidejűleg minimális, csak a munkával kapcsolatosan szükséges adatokat, illetve dokumentumok helyezhetőek ki. Az eszközök fizikai elhagyása esetén megfelelő eljárással (zárolás, jelszavas képernyővédelem alkalmazásával) gondoskodni kell arról, hogy harmadik személyek ne tudjanak betekinteni a rendszerbe, ne férjenek hozzá a rendszerhez.

(3) A munkavégzés során keletkező jegyzeteket, vázlatokat, illetve példányokat meg kell semmisíteni amennyiben már nincs szükség rájuk.

(4) Prezentációk során oda kell figyelni, hogy mi kerül kivetítésre. Megbeszélések után a tárgyalókból minden dokumentumot el kell távolítani, a táblák tartalmát le kell törölni.

16.§
Viselkedési szabályok az interneten

(1) Az Egyetemen internethasználati jogokkal rendelkező felhasználói a munkájukkal kapcsolatban korlátlanul használhatják az Egyetem által biztosított internet szolgáltatást.

(2) A felhasználók az Egyetem nevében csak a vezetőség előzetes engedélyével tölthetnek fel internetre adatokat, anyagokat.

(3) Az Egyetem tulajdonát képező adatbázisok tartalmának interneten keresztül történő hozzáférésének lehetővé tétele megfelelő jogosultságigénylés mellett az informatikáért felelős szakterület feladata. Az

engedély megadása ilyen esetben vonatkozhat egyedi esetre vagy egyes rendszerekkel kapcsolatos feladatok elvégzésére az arra felhatalmazott munkatársak részére.

(4) Az internet magáncélú használata tiltott, az alábbi szabályokat kell betartani:
   a) tilos a pornográf, online játék, fogadási oldalak, csevegő oldalak, letöltő oldalak és törvénybe ütköző tartalmakat szolgáltató oldalak látogatása.
   b) Az internetről magán céllal tilos fájlokat letölteni.
   c) Informatikai biztonsági megfontolásokból tilos az Egyetemen a csevegő és azonnali üzenetküldő programok használata. Kivétel ez alól az Egyetem által esetlegesen biztosított hasonló szolgáltatást nyújtó szoftver (Teams) Egyetemen belüli használata.

17.§
Nyomtatás

A kinyomtatott dokumentumok, függetlenül azok tartalmától, nem dobhatók szemétkosárba, csak megfelelő iratmegsemmisítés (iratmegsemmisítő vagy apróra tépés) után.

18.§
Távoli elérés / Távoli munkavégzés

(1) Távmunka végzése technológiai szempontból a laptoppal rendelkező kollégák számára engedélyezett, ugyanakkor az Egyetem belső szabályainak megfelelően a távoli munkavégzést a közvetlen vezetővel kell engedélyeztetni.

(2) Távmunka esetén is gondoskodni kell a helyszínen a biztonsági követelmények és előírások betartásáról, a megfelelő és rendszeres ellenőrzésről.

(3) VPN hozzáférés biztosítás a felhasználók számára lehetséges, amennyiben azt az Információbiztonsági Szabályzatnak és a Hozzáférésvédelmi Szabályzatnak megfelelően jóváhagyják, illetve használják.

(4) A bejelentkezés időtartamára a felhasználóra érvényesek az Egyetemadatvédelmi szabályzatai.

(5) A rendszerbe való belépéshez szükséges a belépő személy azonosítása (felhasználói azonosító /jelszó/ tanúsítvány használatával).

(6) A belépési azonosítókat másra átruházni, illetve más azonosítóját használni tilos.

(7) A bejelentkezéseket ellenőrzik és naplózzák.

(8) A távoli elérésnek biztonságos kapcsolaton keresztül kell megvalósulnia (telnet helyett SSH, FTP helyett SFTP vagy SCP, vagy valamilyen biztonsági protokollon keresztül).

(9) A bejelentkezett végpontot (számítógép, laptop, mobiltelefon) nem szabad felügyelet nélkül hagyni, még rövid időre sem.

(10) A mobil számítástechnikai eszközökön az felhasználónak gondoskodni kell a rejtjelezett adattárolásról és adatátvitelről. Távmunka (távoli hozzáférés) esetén az Egyetem érintett szervezeti egységeinek

gondoskodniuk kell a biztonságos adatkapcsolat létrehozásáról, a kapcsolatot tartó hely és eszköz védelméről.

19. §
Az Egyetem által biztosított informatikai eszközök

(1) Az Egyetem által a munkaviszonyhoz vagy egyéb jogviszonyhoz kapcsolódó feladatok ellátásához biztosított eszközök (asztali számítógép, laptop, mobiltelefon, levelezés, tárhelyek) csak a feladatok ellátásához kapcsolódó módon használhatóak, azok privát célból történő használata nem megengedett.

(2) Az eszközök informatikai biztonsági paramétereinek állítása a felhasználók számára jogosultság mellett sem megengedett (például vírusírtó kikapcsolása).

(3) Az Egyetem által biztosított eszközökön kizárólag jogtiszta szoftverek és dokumentációk használhatók, amelyek megfelelnek a rájuk vonatkozó szerződéses elvárásoknak, és a szerzői jogi, vagy más jogszabályoknak.

20.§
Magántulajdonú eszközök használata a feladatok ellátására

Az Egyetemhez kapcsolódó feladatok ellátásához magántulajdonú eszközök is használhatók, melyek segítségével távolról érhetők el a rendszerek. Ezen eszközök tekintetében a következő elvárásokat kell betartani:

a) a kapcsolódó eszközt védeni kell illetéktelen hozzáféréstől, azt úgy kell használni, hogy az Egyetem adataihoz jogosultsággal nem rendelkező személy az eszközhöz ne férhessen hozzá;
b) a kapcsolódás során meg kell győződni arról, hogy a kapcsolat biztonságos és védett, nyilvános wifi hálózat a kapcsolódáshoz nem javasolt;
f) a bejelentkezést megfelelő komplex jelszóval védeni;
c) az eszközön automatikusan frissülő vírusírtó használata;
d) az eszköz zárolása amennyiben a felhasználó eltávolodik tőle.
e) Magántulajdonú eszközön az Egyetem adata csak ideiglenes jelleggel tárolható, amennyiben lehetséges az adatok tárolását el kell kerülni. Amennyiben ez nem lehetséges, elvárt az adatok titkosított tárolása vagy jelszóvédelemmel, vagy jelszóvédett titkosított meghajtón történő tárolással.

21.§
Mobil eszközök használata

A mobil eszközök (laptopok, notebook-ok, otthoni munkaállomások, tabletek, mobiltelefonok) használóinak mind a fizikai biztonság, mind a logikai védelem területén a jelen Szabályzatban, valamint az Egyetem Információbiztonsági Szabályzatában foglaltakat kell figyelembe venniük. Ezek közül a legfontosabbak:

g) A távmunka során is be kell tartani az Egyetem szabályzataiban foglaltakat.
h) A mobil eszközök nem hagyhatók felügyelet nélkül, amennyiben nem biztosítható azok előírt védelme.
i) A kommunikációhoz védett csatornáról kell gondoskodni, nyilvános publikus hálózatok használata, nem javasolt.
j) Vírus- és behatolás védelmi eszközöknek működniük kell a mobil eszközön.
k) A mobil eszközökön tárolt adatok bizalmasságának védelmére fokozott figyelmet kell fordítani.

l) A mobil számítástechnikai berendezéseket nyilvános helyeken használóknak ügyelni kell arra, hogy elkerüljék a jogosulatlan személyek általi betekintés kockázatát.
m) Bizalmas üzemeltetési információkat hordozó eszközt nem szabad felügyelet nélkül hagyni, és ha lehetséges, fizikailag el kell zárni vagy különleges zárat kell alkalmazni a berendezés biztosítására.
n) A hordozható informatikai eszközök gazdája felelős az eszköz teljes biztonságáért és annak ellenőrzéséért.
o) A rendszer csak limitált visszacsatolási információt szolgáltathat a felhasználónak a hitelesítési eljárás alatt, így megakadályozza a felhasználót abban, hogy ismereteket szerezzen a hitelesítési folyamatról.
p) Az interaktív kapcsolatok zárolása felhasználó 15 perc inaktivitása után a rendszer megszakítja a kapcsolatot.
q) Az aktuális képernyőtartalmat olvashatatlanná kell tenni, le kell tiltani minden felhasználói tevékenységet, a hozzáférést,kijelzőket és zárolni kell a munkameneteket.

22.§
Levelezés

(1) A Szabályzat érvényes minden levélre, amit az Egyetem által birtokolt domainek valamelyikéhez tartozó e-mail címről küldtek, ugyanis a belső hálózaton hozzáférhető levelezőrendszer munkaeszköznek minősül, adattartalmának ellenőrzésére az Egyetemjogosult.

(2) A szervezeti levelezőrendszer magáncélú levelezésre nem használható. A megvalósuló adatkezelés (informatikai rendszerben történő tárolás, törlés stb.) során fokozottan érvényesíteni kell a célhoz kötöttség elvét és a levéltitok védelmét. A nem kívánatos adatkezelés elkerülése érdekében a felhasználó köteles magáncélú leveleit – magáncélú használat tiltása ellenére beérkezett vagy küldött(!) - 48 órán belül törölni/eltávolítani, ennek elmaradása esetén azok adattartalma indokolt esetben (informatikai üzemzavar, hibakeresés stb.) vizsgálható.

23.§
Levelezési szabályok

(1) Az általános levelezési szabályok:
r) A levelek nem képviselhetnek a hatályos magyar jogszabályokba ütköző magatartást.
s) A levelek nem sérthetik mások becsületét, emberi méltóságát és egyéb jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
t) A levelek tartalma nem sérthet meg szerzői és szomszédos jogokat.
u) A levelek nem ronthatják az Egyetem jó hírnevét, megítélését, nem terjeszthetnek róla szándékosan valótlan információkat.
v) Tilos az Egyetemhez tartozó emailcímekről, az Egyetem eszközeit használva spameket, az Egyetem számára kompromittáló adatokat, leveleket elküldeni vagy továbbítani.
w) Tilos az e-mailen keresztül történő zaklatás bármely formája.
x) Tilos az e-mail fejlécében található információ meghamisítása vagy jogosulatlan használata.
y) Tilos az e-mail címek külső címre való átirányítása, kivéve, ha ezt az információbiztonsági felelős külön engedélyezte.

(2) Levelezési tanácsok:

a) Ismeretlen feladótól érkezett, különös témájú, csatolt fájlt tartalmazó levelekkel legyünk nagyon óvatosak, a jelek vírusfertőzésre utalhatnak, töröljük a levelet!
b) Nagyméretű fájlokat ne küldjünk belső címzettnek, mert ez túlzott mértékben terheli a hálózat forgalmát, helyette tegyük elérhetővé a vonatkozó linket a fájlszerveren tárolt adathoz.
c) Bizalmas és személyes adatokat tartalmazó leveleket, fájlokat ne küldjük külső címzettnek titkosítatlanul, mindig használjunk titkosítást.

(3) Informatikai biztonsági vizsgálat, auditálás, illetve hibakeresés céljából az Egyetem informatikai rendszereinek teljes hálózati forgalma megfigyelhető és rögzíthető. A felhasználó az Információbiztonsági Szabályzat ismeretéről és elfogadásáról szóló nyilatkozatával elfogadja, hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti az adatkezelésbe. Elektronikus levelek esetén a vizsgálat, illetve megfigyelés nem szükségképpen terjed ki a levelek tartalmára, de kivételesen indokolt esetben (pl. hibaelhárítás) a levelek megnyitására az információbiztonsági felelős utasítása alapján sor kerülhet.

24.§
Vírusvédelem

(1) Az alábbi utasítások betartása erősen ajánlott a vírusfertőzések megelőzése, illetve azok kockázatának csökkentése érdekében:

z) Felhasználóknak nem szabad kikapcsolni az eszköz vírusvédelmét biztosító szoftvert.
aa) Soha nem szabad ismeretlen vagy gyanús helyről fájlokat letölteni.
bb) Idegen állományokat (MS Office) csak „makrók futtatása nélkül”? opcióval szabad megnyitni.
cc) Ismeretlen, megbízhatatlan forrásból származó furcsa, gyakran vicces e-mail-ek csatolt fájljait nem szabad megnyitni, azonnal törölni kell őket. Az e-mailben küldött vírusok, férgek rendszeresen operálnak valamilyen különös megjegyzéssel a levelek tárgy bejegyzésében.
dd) A külső feleknél is használt írható adathordozók (újra írható CD, DVD, pendrive, hard-drive) vagy a tőlük kapott adathordozók vírusmentességét felhasználás előtt ellenőrizni kell a számítógépekre telepített víruskeresővel.

(2) Vírusfertőzés esetén tájékoztatni kell az informatikáért felelős szakterületet fertőzésről vagy annak gyanújáról. A hibaelhárításig a számítógép további használata tilos.

25.§
Informatikai problémák bejelentése

(1) Az Egyetem felhasználói minden olyan problémát, amely nem igényli az azonnali beavatkozást, kötelesek bejelenteni levélben az helpdesk@szfe.hu emailcímen.

(2) Az Egyetem felhasználói minden azonnali beavatkozást igénylő problémát (amely gátolja a rendeltetésszerűnapi munkavégzést) munkaidőn belül (hétköznapokon 8:00-tól 16:00-ig) és kívül az alábbi telefonszámon kötelesek jelezni: +36 1 551-5022

26.§
Belépés, látogatók fogadása

Az Egyetem épületeibe az arra jogosultak belépőkártyával léphetnek be, a látogatókat a látogatás teljes időtartama alatt kísérni szükséges.

27. §
A jogviszony megszűnésének, megszüntetésnek biztonsági kérdései

(1) A jogviszony megszűnése után a felhasználóknak titoktartási nyilatkozatot szükséges aláírniuk az Egyetem adatainak és információinak megfelelő biztonsága érdekében.

(2) Az eszközök visszaadásához, a jogosultságok visszavonásához kapcsolódó részletes szabályozást az informatikai rendszerekhez és eszközökhöz való hozzáférés, kiadás és visszavétel tekintetében a Hozzáférésvédelmi Szabályzat tartalmazza.

28. §
Fegyelmi eljárás

Azokkal szemben, akik a szervezet Információbiztonsági szabályait és eljárásait vétkesen megszegték, fegyelmi eljárást kell kezdeményezni és lefolytatni. A fegyelmi, felelősségi, kártérítési eljárásra a mindekor hatályos Munka Törvénykönyve vagy a mindekor hatályos Polgári Törvénykönyv vonatkozó rendelkezései az irányadóak.

29. §
Információbiztonsági és adatvédelmi incidens kezelése

(1) Információbiztonsági esemény a rendszer működésében beállt olyan kedvezőtlen változás, amelynek hatására a rendszerben kezelt adatok bizalmassága, sértetlensége, rendelkezésre állása, vagy a rendszer sértetlensége vagy rendelkezésre állása sérült vagy sérülhet.

(2) A jellemző információbiztonsági események lehetnek a következők:
   a) A szolgáltatás leállása;
   b) Berendezés vagy az eszközök elvesztése;
   c) A rendszer hibás működése vagy túlterhelések;
   d) Emberi hibák;
   e) A fizikai biztonsági rendelkezések megsértése;
   f) Nem ellenőrzött rendszerbeli változások;
   g) A szoftver vagy hardver hibás működése;
   h) Hozzáférési előírások megsértése;
   i) Kártékony kód általi fertőzés;
   j) A nem teljes vagy nem pontos működési adatokból eredő hibák;
   k) A bizalmasság és sértetlenség megsértése;
   l) A rendszerrel való visszaélés.

(3) Az esemény tényét dokumentálni kell az eset későbbi kivizsgálása érdekében. A jegyzőkönyvben rögzített információknak elégéges adatot kell szolgáltatnia a kockázatelemzés, illetve szabályzatok felülvizsgálata esetén.

(4) Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás, vagy vírustámadás okozta, az érintett információfeldolgozó eszközt azonnal le kell választani a hálózat(ok)ról, szükség esetén ki kell kapcsolni. Ilyen esetekben fokozottan figyelni kell a hordozható adathordozókra is.

(5) Az észlelt biztonsági eseményeket azonnal jelenteni kell az információbiztonsági felelős és az adatvédelmi tisztviselő részére, valamint a közvetlen vezetőnek.

(6) A hibaüzenetet (vagy az incidensre utaló jeleket amennyiben vannak) a felhasználó nem törölheti a képernyőről. A felhasználó semmiféle kísérletet nem tehet a számítógép rendszer, vagy a hálózat működését érintő hiba megszüntetésére (még akkor sem, ha kellő felhasználói ismeretekkel rendelkezik), amíg az illetékes informatikai munkatárs azt nem látta (vagy a pontos hibaüzenetet, képernyőképet e-mailben el nem küldte az IBF részére).

(7) A beérkezett jelentés alapján az információbiztonsági felelős és az adatvédelmi tisztviselő feladata az esemény kivizsgálása és dokumentálása.

30.§
Záró rendelkezések

(1) Jelen Szabályzat annak aláírását követő napon lép hatályba.

(2) A jelen szabályzat hatálybalépésével a 30/2021. (09.16.) számú rektori-kancellári közös utasítással elfogadott Informatikai Biztonsági Szabályzat hatályát veszti.

(3) Jelen Szabályzatot a Rektori Hivatal gondozza.

(4) A Jelen Szabályzat megtalálható és elérhető a www.szfe.hu oldalon.

Budapest, 2024. május 06.

…..……..
Dr. Sepsi Enikő s. k.
rektor