Ikt.sz.: SZFE/1095/2024

SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

SZFE 1865

8/2024. (05.06.) számú rektori szabályzat

A Színház-és Filmművészeti Egyetem Hozzáférésvédelmi Szabályzata

Hatályos: 2024. május 7. napjától

1. §
A jelen Szabályzat célja

A jelen Hozzáférésvédelmi Szabályzat (a továbbiakban: Szabályzat) célja, hogy meghatározza a Színház- és Filmművészeti Egyetemen (továbbiakban: Egyetem):

a) az infokommunikációs eszközök kezelésének rendjét;
b) a saját azonosítási és hitelesítési funkcióval rendelkező infrastruktúra elemek és alkalmazások jogosultságigénylési folyamatait;
c) a jelszókezelési szabályokat;
d) az azonosítási és hitelesítési funkcióval rendelkező elemekkel kapcsolatos elvárásokat;
e) a szerepköröket és a felelősöket, az elvégzendő feladatok, nyilvántartások és szükséges dokumentáció körét.

2. §
A jelen Szabályzat hatálya

(1) A Szabályzat személyi hatálya kiterjed az Egyetem valamennyi szervezeti egységére, az Egyetemmel hallgatói jogviszonyban álló hallgatókra akik tanulmányi 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 személyi hatálya kiterjed továbbá 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 az Egyetem vagy más személy üzemelteti;
b) a számítástechnikai eszközök (laptop, mobiltelefon, egyéb adathordozók, belépőkártyák) alkalmazásának (kiadás, használat, visszavétel) teljes folyamatára, tevékenységeire.

(4) A Szabályzat hatálya nem terjed ki azon alkalmazásokra, melyek esetében felhasználónév nem kerül kialakításra, hanem technológiailag az előre megadott technikai felhasználókat, illetve azok azonosítási és hitelesítési információit megosztottan szükséges alkalmazni.

3. §
A Szabályzat megalkotása, felülvizsgálata és módosítása

(1) A Szabályzat megalkotása, felülvizsgálata és szükség szerinti módosítása az információbiztonsági felelős feladata és felelőssége.

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

(3) A 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.

(4) A felülvizsgálatok eredményéről az információbiztonsági felelős tájékoztatja a rektort.

(5) 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.

4.§
Kivételkezeléssel kapcsolatos feladatok

(1) Kivétel alatt kell érteni minden olyan technológiai vagy szervezeti kontroll nem teljesülését, mely a jelen Szabályzatban rögzített követelményeket nem tudja teljesíteni. Új, bevezetés alatt álló (elektronikus) információs rendszer esetén a szabályzati követelmények teljesülésére vonatkozó kivétel nem alkalmazható.

(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 rektorengedélyével történhet.

(3) A szabályok alól ideiglenesen kivételt képezhetnek azon rendszerek melyek a Szabályzat hatályba lépésének időpontjában már bevezetésre vagy kiválasztásra kerültek, ugyanakkor ezen rendszerek tekintetében a hiányosságokat a kockázatelemzésben szükséges értékelni.

(4) A jelen Szabályzatban megfogalmazott azonosítókkal és hitelesítési eszközökkel kapcsolatos szabályok alól ideiglenesen kivételt képezhetnek azon rendszerek melyek a Szabályzat első kiadásának pillanatában már bevezetésre vagy kiválasztásra kerültek, ugyanakkor ezen rendszerek tekintetében a hiányosságokat a kockázatelemzésben szükséges értékelni.

5.§
Infokommunikációs eszköz és jogosultság igénylése

(1) Új alkalmazás vagy infrastruktúra elem hozzáférési jogosultság igénylését / módosítását az alábbiak szerint lehet kezdeményezni.

(2) Új belépő esetében a Humán Erőforrás Iroda emailben **helpdesk@szfe.hu** email címen) igényli meg a szükséges biztosítandó eszközöket és O365 jogosultságokat (levelezés, hálózati hozzáférés, intranet, belépőkártya, notebook, laptop, mobil eszközök stb.).

(3) A szakrendszerekhez történő hozzáférés igénylést a közvetlen vezető az információbiztonsági felelőssel egyeztetve kezdeményezi emailben. (**helpdesk@szfe.hu**)

(4) Az informatikai szervezet tagjai számára a jogosultság igényléseket az információbiztonsági felelőssel is jóvá kell hagynia.

(5) A hallgatók számára levelezési címet és O365 jogosultságot az Oktatástámogatási Igazgatóság igényelhet.

(6) A hallgatók számára a könyvtári rendszer távoli használatához VPN hozzáférést a hallgató saját maga önállóan igényelhet.

6.§
Jogosultságok megadása

(1) A rendszerhozzáférésekhez a jogosultságokat a rendszerekben elkülönítetten kerülnek kialakításra, a rendszerekhez definiált rögzített felhasználói csoportok (szerepkörök) alapján. Ilyenkor a kezdő jelszónak meg kell felelni a felhasználói jogosultságnak megfelelő jelszóösszetettségi követelményeknek.

(2) A jóváhagyott jogosultságot, illetve az eszközöket és belépőkártyát az informatikus állítja be és adja ki.

(3) Eszköz és belépőkártya kiadásakor átadás-átvételi dokumentum kerül kitöltésre két példányban, mely egyik példánya a informatikáért felelős szakterületnél kerül megőrzésre, másik példányát a felhasználó kapja meg.

(4) A belépőkártyák kiadásánál kivételt képeznek az Infopark épületében használatos belépőkártyák, melyeket a Humán Erőforrás Irodán lehet átvenni, és ott kerülnek regisztrációra is.

7.§
Jelszó küldése

(1) A kezdeti jelszavak meghatározása vagy a rendszer által véletlenszerűen generált karaktersor meghatározásával megengedett, vagy az informatikus által a jelen Szabályzat rendelkezéseinek megfelelően kialakításával történik.

(2) Jelszót nyílt távközlési csatornán (e-mail) kell küldeni vagy papíron lehet átadni. Az eredeti jelszót minden esetben módosítani kell belépéskor.

8.§
Infokommunikációs eszköz és jogosultság nyilvántartása

(1) Az eszközöknek a felhasználó részére történő kiadását tételes, 2 példányban kitöltendő átadás-átvételi elismervényen kell rögzíteni. Informatikai eszközt kiadni csak a Szabályzatnak megfelelően jóváhagyott igénylés, illetve a felhasználó által aláírt átadás-átvételi formanyomtatvány birtokában lehet.

(2) Az eszközök nyilvántartása ily módon papír alapon ezen dokumentumok megőrzésével valósul meg.

(3) A jogosultság igénylések a levelezésből visszakereshetők, hogy ki, miért és mikor igényel jogosultságot, azokat ki hagyta jóvá. A mindenkori jogosultság információk az elektronikus információs rendszerekből kinyerhetők, ezeket rendszeresen az Informatikai Biztonsági Szabályzatnak megfelelően évente szükséges az informatika és a Humán Erőforrás Irodával együttműködve karbantartani és ellenőrizni.

9.§
Jogosultságok módosítása

(1) Amennyiben bármely felhasználó számára jogosultságainak módosítása vagy új eszköz kiadása szükséges, azt a közvetlen vezetőjének szükséges igényelnie emailben, és a jelen Szabályzat rendelkezéseinek megfelelően azt ismét jóvá kell hagyni.

(2) Elhagyott eszközt incidensként szükséges bejelenteni az Incidenskezelési Szabályzatnak megfelelően.

10.§
Infokommunikációs eszköz és jogosultság visszaszolgáltatása / visszavétele

(1) Munkavállaló munkaviszonyának megszűnése esetén a Humán Erőforrás Iroda levélben (helpdesk@szfe.hu) igényelheti a jogosultságok visszavonását, a távozást elősegítő leszerelési lap („Kilépő dolgozó elszámolási jegyzőkönyve") kezelése folyamán pedig az informatikus vételezi vissza a távozó munkavállaló eszközeit és belépőkártyáját. A jogosultságok visszavonásáért az informatikus felelős.

(2) Együttműködés megszűnése, a használati jogosultság visszavonása vagy az ideiglenes jogosultság hatályának lejárta esetén a felhasználók kötelesek az általuk használt infokommunikációs eszközöket és annak tartozékait, az informatikus részére legkésőbb a jogosultság megszűnése napján visszaszolgáltatni.

(3) Az eszközök visszavételének igazolását az informatikus két példányban kitöltött átadás - átvételi elismervénnyel igazolja. Az elismervény egyik példánya a felhasználót illeti meg, míg a második példány megőrzéséről az informatikusköteles gondoskodni.

11.§
Jogosultságok inaktiválása, hozzáférés megvonása

(1) A kilépő munkavállaló, vagy jogosultsági periódusának végére érő külsős felhasználó esetében az utolsó munkában töltött nap végén, egyéb jogviszonyban álló személyek esetében a jogosultságot megalapozó jogviszony lejártakor a felhasználónevet inaktiválni kell.

(2) Felhasználónevet előzetes engedély hiányában törölni kifejezetten tilos.

(3) A kilépő, vagy feladatkört váltó munkavállalókról az informatikust a Humán Erőforrás Iroda vagy a külsős személyért felelős szervezeti egység értesíti a változás napját megelőzően, az inaktiválás érdekében.

(4) Amennyiben egy felhasználó fiókja nem privilegizált fiókról privilegizált fiókra vagy technikai fiókra kerül módosításra, a hitelesítési információk módosítása elvárt annak érdekében, hogy az új hitelesítési információ megfeleljen a szervezeti elvárásoknak.

(5) A hallgató távozását és kapcsolódó jogosultságainak (levelezés, O365, VPN) megszűntetését
   a) év közben az Oktatástámogatási Igazgatóság által az helpdesk@szfe.hu email címre küldött információ alapján;
   b) évente egyszer az informatikus az Oktatástámogatási Igazgatósággal való egyeztetés (új / távozó hallgatók) alapján végzi.

12.§
Jogosultság/hozzáférések kezelése

(1) A hozzáférési jogosultság kialakítása során figyelembe kell venni az adatok és eszközök biztonsági kockázatait. Az alkalmazásoknak azonosítás és hitelesítés nélkül elérhető funkciójának használata során csak publikus információk érhetők el.

(2) A nyilvántartásban szereplő adatoknak megfelelően választ kell tudni adni arra a kérdésre, hogy egy felhasználó számára milyen jogosultsági igények lettek jóváhagyva és beállítva. Ezen információkat a levelezések megőrzése szolgáltatja.

13.§
Definiált jogosultsági szabályok

(1) Az üzemeltetők az üzemeltetési feladatok ellátásához nem használhatnak rendszer adminisztrátori hozzáféréseket.

(2) Az eljáró auditoroknak csak olvasási joguk lehet, ugyanakkor sérülékenység vizsgálathoz adható ennél magasabb szintű hozzáférés is a megfelelő engedélyek megléte mellett.

(3) Kiemelten fontos a következők védelme:
   a) Eseménynaplók,
   b) Bizalmas adatok, személyes adatok,
   c) Rendszer segédprogramokhoz való hozzáférés,
   d) Forráskódhoz való hozzáférés.

(4) Jelen pontban írtakhoz hozzáférés az információbiztonsági felelős engedélyével történhet.

(5) A jogosultságokat mindig a „legszűkebb hozzáférés” elve alapján szükséges meghatározni úgy, hogy azok biztosítsák a feladatok elvégzésének lehetőségét a legszűkebb hozzáférés segítségével.

(6) Privilegizált szerepkörök – ezekből egy felhasználó nem tölthet be többet, csak egyet:
   a) információbiztonsági felelős: felelőssége a biztonsági szabályok és eljárásrendek megvalósításának felügyelete;
   b) rendszer adminisztrátor: jogosult telepíteni, konfigurálni és karbantartani az Egyetem alkalmazásait, de korlátozott a hozzáférése a biztonsággal kapcsolatos adatokhoz;

c) rendszer operátor: felelős a rendszerek napi üzemeltetéséért, és feladata a rendszer mentése/visszaállítása, de nem jogosult és köteles felügyelni vagy konfigurálni a rendszerek működését;
d) rendszer auditor: jogosult a rendszerek naplóeseményeibe és archívumaiba betekinteni a biztonsági szabályzatokkal összhangban végzett vizsgálatok céljából, nem jogosult és köteles felügyelni vagy konfigurálni a bizalmi szolgáltatás működését.

(7) A jogosultságkezelési szabályok a helyi és a távoli hozzáférések igénylésére is kiterjednek, automatikus VPN hozzáférés az Egyeteminformatikai rendszeréhez nem biztosítható.

(8) A vezeték nélküli hálózat használata az Egyetem munkavállalói számára automatikusan engedélyezett, a hallgatóka „Student" a vendégek a „Guest" wifi szolgáltatást használhatják, ahol ezek kiépítésre kerültek.

14.§
Alkalmazásokkal kapcsolatos elvárások

(1) Minden a jelen Szabályzat hatálya alá bevont alkalmazásnak és azonosítási-hitelesítési funkciót ellátó infrastruktúra elemnek biztosítania kell a következőket:
a) Funkciót/felületet a szerepkörök kezeléséhez;
b) Funkciót/felületet a felhasználói fiókok kezeléséhez: azonosítók létrehozására, érvényességük letiltására, módosítására, ideiglenes fiókok kezelésére előre meghatározott lejárati idővel;
c) Funkciót/felületet a jogosultságok kezeléséhez;
d) Minden azonosító csak egyszer felhasználható legyen;
e) a felhasználók adminisztrálásának lehetőségét;
f) az információbiztonsági funkciókhoz való hozzáférést elkülönített jogosultsághoz kötött módon;
g) Auditori felhasználói csoport létrehozásának lehetőségét
h) Az alkalmazott hitelesítésre szolgáló eszközök tartalom védelmének (pl.: titkosított jelszó tárolás) és hozzáférés jogosultságainak (pl.: korlátozás) kezelését;
i) A hitelesítésre szolgáló eszközök kezelése során az ellenőrző elemeket titkosított tárolásának lehetőségét (jelszó hash lenyomatok megfelelő algoritmus és salt alkalmazásával);
j) fedett visszacsatolás lehetőségét a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.
k) A hitelesítésre szolgáló eszközök közül a jelszókezelés esetében az eljárásrendben leírt szabályok kikényszerítését, amennyiben ez technológiailag nem lehetséges, ahhoz legközelebb eső jelszó elvárási szabályok alkalmazását;
l) Sikertelen bejelentkezési kísérlet esetén ne adjon támadáshoz felhasználható információt a hiba természetéről; korlátos számú sikertelen bejelentkezési kísérlet után blokkolja a felhasználót;
m) Jelszavak nem látható módon történő megjelenését;
n) A jelszómódosítás lehetőséget a felhasználói felületen is;
o) A privilegizált felhasználók jogosultságainak kezelésére többfaktoros hitelesítési lehetőséget.

Amennyiben egy rendszer használatához szükséges ismeret vagy a jogosultságkezelés módja megváltozik, esetleg a rendszer funkciója relevánsan kiterjesztésre kerül, az alkalmazásgazda értesíti

az informatikust és az információbiztonsági felelőst a szükséges jogosultsági változtatásokról és az esetleges oktatási igényről.

15.§
Azonosító és jelszókezelés, jelszóvédelem

(1) A felhasználó azonosítóját a felhasználó neve alapján képzik. Amennyiben a személy neve alapján a felhasználónév megegyezne egy már létező aktív vagy inaktív felhasználónévvel, az esetben módosított szabállyal kell a felhasználónevet megképezni a személy nevéből. Felhasználónevet újra felhasználni akkor sem lehet, amennyiben az inaktív.

(2) Minden jelszó, mely rendszer által a felhasználónak készül, egyedi, generálásuk véletlenszerű értékeken alapul.

(3) Az alkalmazásokhoz és infrastruktúrához való hozzáféréshez használt jelszavakat bárhol elmenteni, azokat megosztani titkosítás nélkül tilos. Jelszavak tárolására többek között lehetőséget adhat pl.: keepass alkalmazás.

(4) Amennyiben a felhasználói jelszó biztonsága sérül vagy sérelme felmerül, a jelszót azonnal meg kell változtatni. Ebben az esetben az incidenst az incidenskezelési szabályok szerint jelenteni kell.

16.§
Nem privilegizált fiókok – nevesített felhasználók

(1) Minden jogosultságnak egyedi, természetes személyhez rendelhetőnek kell lennie. Nem szabad több felhasználó által használt ún. csoport jogosultságokat létrehozni. 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 meg kell követelni a komplexitást, vagyis minimum tartalmaznia kell kis- és nagybetűket, 1 számot és 1 speciális karaktert (pl.: %,#,&,@,$).
   d) A kiadott (default, kiindulási) jelszavak nem lehetnek triviálisak, kitalálhatóak. A jelszavakat az informatikusszemélyesen, vagy telefonon adhatja át a felhasználóknak, azt e-mail-ben, vagy SMS-ben küldeni tilos.
   e) Jelszó nem lehet könnyen megjegyezhető nem köthető 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.
   f) A rendszernek a rendszeres jelszómódosítást ki kell kényszerítenie 180 naponként.

(2) Korlátos számú (5 db) bejelentkezési kísérlet után a bejelentkezés lehetőségét blokkolni kell, mely blokkolást vagy az informatikusa tudja feloldani, vagy a rendszer automatikusan 30 perc után feloldja amennyiben ez idő alatt nincs további hibás bejelentkezési kísérlet.

17.§
Privilegizált fiókok – nevesített felhasználók

(1) Privilegizált felhasználók azon felhasználók melyek adminisztrátori, illetve jogosultságkezelési jogkörrel rendelkeznek alkalmazásokban, illetve bármilyen jogosultsággal rendelkeznek infrastruktúra eszközök menedzseléséhez.

(2) Ezen felhasználók kéttényezős hitelesítés segítségével kapcsolódhatnak az elektronikus információs rendszerekhez.

(3) Minden jogosultságnak egyedi, természetes személyhez rendelhetőnek kell lennie. Nem szabad több felhasználó által használt, úgynevezett csoport jogosultságokat létrehozni. A jelszavakkal kapcsolatban a 16. § (1) bekezdésben foglaltakon túl biztosítani szükséges, hogy a

a privilegizált felhasználók bejelentkezéséhez a második faktort a „Microsoft authenticator" biztosíthassa.

(4) Privilegizált felhasználói fiókkal rendelkező felhasználóknak kötelező a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött – ún. nem privilegizált - fiókjukat vagy szerepkörüket használniuk.

18.§
Technikai felhasználók

(1) Technikai felhasználók azon felhasználók melyek a rendszerben automatikus feladatvégzésre vannak feljogosítva, mint ilyen speciális funkciókat látnak el.

(2) A technikai felhasználók létrehozását a következők kezdeményezhetik:
a) Informatikai rendszerért általánosan felelős vezető;
b) Rendszer adminisztrátor.

(3) Minden technikai felhasználónak jól behatárolt jogosultsággal kell rendelkeznie, mely lehetővé teszi, hogy a jogosultságok és a szerepkörök megfelelően el legyen különítve nem csak a jogszabályi és szabályozási elvárásoknak megfelelően, de funkcionális szempontokat is figyelembe véve.

(4) A technikai felhasználókhoz beállított jelszavakat jegyzőkönyvezett módon az információbiztonsági felelős páncél szekrényében papír alapon zárt sérülés biztosított módon borítékban szükséges elhelyezni.

(5) A technikai felhasználók jelszavaira a következő elvárások vonatkoznak:
a) A jelszavaknál meg kell követelni a komplexitást, vagyis minimum tartalmaznia kell kis- és nagybetűket, 1 számot és 1 speciális karaktert (pl.: %,#,&,@,$).
b) A jelszavak nem lehetnek rövidebbek mint 16 karakter.
c) A kiadott (default, kiindulási) jelszavak nem lehetnek triviálisak, kitalálhatóak. Az indulási jelszavakat személyesen, vagy telefonon lehet átadni, e-mail-ben, vagy SMS-ben küldeni tilos.

d) A rendszernek rendszeres jelszómódosítást nem kell kikényszerítenie, mivel ez olyan kockázattal járhat, ami kiesést okoz.
e) A jelszó nem lehet egyező a megelőző 5 jelszóval, az utolsó jelszótól való eltérés minimum 2 karakter.

Korlátos számú (5 db) bejelentkezési kísérlet után a bejelentkezés lehetőségét blokkolni kell, mely blokkolást vagy az informatikus tudja feloldani, vagy a rendszer automatikusan 30 perc után feloldja amennyiben ez idő alatt nincs további hibás bejelentkezési kísérlet.

19.§
Az egyetemi szervezeten kívüli felhasználók

(1) Az Egyetemen kívüli felhasználók esetében a hozzáférési igénylést az említett felhasználóért felelős szervezeti egység vezetője kezdeményezheti. A jogosultságok jóváhagyásának folyamata megegyezik a belső felhasználói folyamattal kiegészítve azzal, hogy az informatikuscsak az után állíthat be ilyen jellegű hozzáférést, miután meggyőződött a hozzáférési igény alapjául szolgáló jogviszony vagy kötelezettség meglétéről.

(2) Az egyetemi szervezeten kívüli felhasználóval kapcsolatos hitelesítési elvárások megegyeznek a szervezeten belüli technikai felhasználóknál leírtakkal.

(3) A szervezeten kívüli felhasználó számára biztosított hozzáférés esetében – amennyiben a rendszer erre lehetőséget ad - a felhasználó hitelesítési információinak le kell járniuk a szerződéses viszony lejáratát követő 3 munkanapon belül.

20.§
Távoli bejelentkezés, távmunka biztonsága

(1) Az erre kijelölt felhasználók számára (jóváhagyott igénylés alapján) VPN kapcsolaton keresztül lehetőség van távoli bejelentkezésre, munkavégzésre. A távoli hozzáféréshez való jogosultságot az információbiztonsági felelős által jóváhagyott igénylés alapján az informatikus állítja be.

(2) A távoli bejelentkezéshez elsődlegesen olyan számítógép használható, melyet az Egyetem bocsátott a felhasználó rendelkezésére, vagy olyan privát eszköz, melynek a biztonsági beállításai megfelelnek az Egyetem elvárásainak (lásd IBSZ) és a meghatározott beállítások érvényesek rajta (pl.: naprakész rendszer frissítések, naprakész vírusvédelmi rendszer stb.).

(3) Távoli hozzáférések esetében a bejelentkezési azonosítási és hitelesítési elvárások azonosak a helyszíneken életbe léptetett szabályokkal.

21.§
Elfelejtett azonosítási / hitelesítési információk kezelése

(1) Elfelejtett azonosítási információ esetén a felhasználóazonosítót az informatikus küldi meg a felhasználó kérésére sms-ben vagy emailben a felhasználó kétséget kizáró azonosítása után.

(2) Elfelejtett hitelesítési információ esetén a felhasználó kérésére – a felhasználó kétséget kizáró azonosítása után – új jelszó generálása szükséges az informatikus által. Az új hozzáférési információkat telefonon vagy személyesen lehet átadni a felhasználónak. Az így kapott jelszavakat a rendszerbe történő első bejelentkezéskor meg kell változtatni.

Az elektronikus információs rendszerek felhasználói fiókjait, email címeit évente legalább egyszer ellenőrizni szükséges. Az ellenőrzést az informatikáért felelős szakterület támogatásával a Humán Erőforrás Iroda végzi. Az inaktív szükségtelen felhasználói fiókokat ezen felülvizsgálatok után meg kell szüntetni.

22.§
Záró rendelkezések

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

(2) A Jelen Szabályzat hatálybelépésével a 29/2021. (09.16.) számú rektori-kancellári közös utasítással elfogadott Hozzáférésvédelmi Szabályzata hatályát veszti.

(3) Jelen Szabályzatot a Campus Igazgatóság gondozza.

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

Budapest, 2024. május 06.

……..
Dr. Sepsi Enikő s. k.
rektor

Mellékletek:

1. számú melléklet: Átadás_átvételi_elismervény_IT_eszköz
2. számú melléklet: Nyilatkozat magáncélú tartalom törléséről

1. számú melléklet

Átadás-átvételi Elismervény

Alulírott……...(név/beosztás)

elismerem, hogy a ……(név)……..(egység/beosztás)

munkavállalójától a …… (IT eszköz típusa, megnevezése) 20……év ……hó ……..napján átvettem.

Budapest, 202…….

…… ……..

Átvevő **Átadó**

Előttünk, mint tanúk előtt:

Tanú 1.

Neve:
Lakóhelye:
Szig.száma:

Tanú 2.

Neve:
Lakóhelye:
Szig.száma:

2. számú melléklet

Nyilatkozat magáncélú tartalom törléséről:

Alulírott……...(név/beosztás) kérem a Színház-és Filmművészeti Egyetemet, hogy a ……(fórum, tartalmat rögzítő eszköz, magáncélú tartalom)……..törölni szíveskedjenek.

Budapest, 202

Tisztelettel:

…….