SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

SZFE 1865

REKTORI-KANCELLÁRI KÖZÖS UTASÍTÁS

IKT.SZ.: SZFE/2369/2021

Színház- és Filmművészeti Egyetem
29/2021. (09.16.) számú rektori-kancellári közös utasítása
a Színház- és Filmművészeti Egyetem
Hozzáférésvédelmi szabályzatáról

Hatályos: 2021. szeptember 17. napjától

Tartalomjegyzék

1 ALTALANOS RENDELKEZESEK

1.1 A jelen szabályzat célja

1. A Hozzáférésvédelmi szabályzat (a továbbiakban: szabályzat) célja, hogy meghatározza a Színház- és Filmművészeti Egyetemen (továbbiakban: Egyetem):

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

1.2 A jelen szabályzat hatálya

1.2.1 A jelen szabályzat szervezeti hatálya

2. A szabályzat 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.

1.2.2 A jelen szabályzat személyi hatálya

3. A szabályzat hatálya kiterjed az szervezet által foglalkoztatott valamennyi munkavállalóra, illetve munkavégzés céljából egyéb jogviszonyban álló jogi és természetes személyre, valamint a hallgatói jogviszonnyal rendelkező diákokra.

1.2.3 A jelen szabályzat tárgyi hatálya

4. A szabályzat tárgyi hatálya kiterjed:

   - az Egyetem által biztosított, felhasználók által használt információs rendszerekre, függetlenül attól, hogy azt a szervezet vagy más vállalkozó üzemelteti;
   - a számítástechnikai eszközök (laptop, mobiltelefon, egyéb adathordozók, belépőkártyák) alkalmazásának (kiadás, használat, visszavétel) teljes folyamatára, tevékenységeire.

1.2.4 A jelen szabályzat időbeli hatálya

5. A szabályzat érvényes a hatálybalépés napjától, visszavonásig.

A Hozzáférésvédelmi 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.

1.3 A szabályzat elkészítése felülvizsgálata és módosítása

6. A szabályzat elkészítése, felülvizsgálata és szükség szerinti módosítása az Információbiztonsági Felelős (a Kancellári Kabinet vezetője) feladata és felelőssége.

7. A szabályzatot legalább évenként felül kell vizsgálni és szükség esetén módosítani kell.

1.3.1 Rendkívüli felülvizsgálat

8. A szabályzatot az időszakos felülvizsgálaton túl felül kell vizsgálni és szükség esetén módosítani kell:

- a szabályzatban hivatkozott szervezetek vagy munkakörök változása esetén;
- súlyos információ biztonsági események bekövetkezése esetén;
- az információs vagy informatikai biztonság szabályozását érintő jogszabályváltozások esetén;
- az információs vagy informatikai rendszer nagy mértékű változása esetén.

9. A felülvizsgálatok eredményéről az Információbiztonsági Felelős tájékoztatja kancellárt és a rektort.

1.4 A szabályzat betartásának ellenőrzése

10. 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 egységek vezetője

1.5 Kivételkezeléssel kapcsolatos feladatok

11. 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.

12. A jelen szabályzattól való kivételeket minden esetben jegyzőkönyvben dokumentálni szükséges, illetve rendszerek esetében az adott rendszer rendszerbiztonsági tervében kell dokumentálni. A kivételek bevezetése a kancellár engedélyével történhet.

13. 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.

14. 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.

2 INFOKOMMUNIKÁCIÓS ESZKÖZÖK ÉS JOGOSULTSÁGOK

2.1 Infokommunikációs eszköz és jogosultság igénylése

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

- Új belépő esetében a HR emailben (it@szfe.hu email címen) igényli meg a szükséges biztosítandó eszközöket és O365 jogosultságokat (levelezés, hálózati hozzáférés, intranet, belépőkártya, notebook, mobil eszközök stb.),
- A szakrendszerekhez történő hozzáférés igénylést a közvetlen vezető az Információbiztonsági Felelőssel egyeztetve kezdeményezi emailben. (it@szfe.hu)
- Az informatikai szervezet tagjai számára a jogosultság igényléseket az Információbiztonsági Felelőssel is jóvá kell hagynia,
- Diákok számára levelezési címet és O365 jogosultságot az Oktatástámogatási Igazgatóság igényelhet,
- Diákok számára a könyvtári rendszer távoli használatához VPN hozzáférést a diák maga igényelhet.

2.1.1 Jogosultságok megadása

16. 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.

17. A jóváhagyott jogosultságot, illetve az eszközöket és belépőkártyát a Rendszergazda állítja be és adja ki.

18. Eszköz és belépőkártya kiadásakor Átadás-Átvételi dokumentum kerül kitöltésre két példányban, mely egyik példánya a Kancellári Kabinet informatikai területén kerül megőrzésre, másik példányát a felhasználó kapja meg.

19. A belépőkártyák kiadásánál kivételt képeznek az Egyetem Kancelláriájának épületében (Infopark) használatos belépőkártyák, melyeket a Kancellári Kabinet HR területén lehet átvenni, és ott kerülnek regisztrációra is.

2.1.2 Jelszó küldése

20. A kezdeti jelszavak meghatározása vagy a rendszer által véletlenszerűen generált karaktersor meghatározásával megengedett, vagy a Rendszergazda által a jelen szabályzat rendelkezéseinek megfelelően kialakításával történik.

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

2.2 Infokommunikációs eszköz és jogosultság nyilvántartása

22. Az eszközöknek a felhasználó részére történő kiadását tételes, 2példányban 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.

23. Az eszközök nyilvántartása ily módon papír alapon ezen dokumentumok megőrzésével valósul meg.

24. 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 Információ Biztonsági Szabályzatnak megfelelően évente szükséges az informatika és a HR területeknek együttműködve karbantartani és ellenőrizni.

2.2.1 Jogosultságok módosítása

25. 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.

26. Elhagyott eszközt incidensként szükséges bejelenteni az Incidenskezelési szabályzatnak megfelelően.

2.3 Infokommunikációs eszköz és jogosultság visszaszolgáltatása / visszavétele

27. Munkavállaló munkaviszonyának megszűnése esetén a HR levélben (it@szfe.hu) igényelheti a jogosultságok visszavonását, a távozást elősegítő leszerelési lap („Kilépő dolgozó elszámolási jegyzőkönyve") kezelése folyamán pedig a Rendszergazda vételezi vissza a távozó kolléga eszközeit és belépőkártyáját. A jogosultságok visszavonásáért a Rendszergazda felelős.

28. Együttműködés megszűnése, a használati jogosultság visszavonása vagy az ideiglenes jogosultság hatályának lejárta esetén a felhasználók kötelesek az általuk használt

infokommunikációs eszközöket és annak tartozékait, a Rendszergazda részére legkésőbb a jogosultság megszűnése napján visszaszolgáltatni.

29. Az eszközök visszavételének igazolását a Rendszergazda két példányban kitöltött Átadás - átvételi elismervénnyel igazolja. Az elismervény egyik példánya a felhasználót illeti meg, míg a második példány megőrzéséről a Rendszergazda köteles gondoskodni.

2.3.1 Jogosultságok inaktiválása, hozzáférés megvonása

30. 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 felhasználó nevet, inaktiválni kell.

31. Felhasználó nevet törölni tilos.

32. A kilépő, vagy feladatkört váltó munkavállalókról a Rendszergazdát a HR vagy a külsős személyért felelős szervezeti egység értesíti a változás napját megelőzően, az inaktiválás érdekében.

33. 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.

34. Diák távozását és kapcsolódó jogosultságainak (levelezés, O365, VPN) megszűntetését

- év közben az Oktatástámogatási Igazgatóság által az it@szfe.hu email címre küldött információ alapján;
- évente egyszer a Rendszergazda az Oktatástámogatási Igazgatósággal való egyeztetés (új / távozó diákok) alapján végzi.

3 JOGOSULTSÁG / HOZZÁFÉRÉSEK KEZELÉSE

35. 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.

36. 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.

3.1 Definiált jogosultsági szabályok

37. Üzemeltetők az üzemeltetési feladatok ellátásához nem használhatnak rendszer adminisztrátori hozzáféréseket.

38. Auditoroknak csak olvasási joguk lehet, ugyanakkor sérülékenység vizsgálathoz adható ennél magasabb szintű hozzáférés is a megfelelő engedélyek megléte mellett.

39. Kiemelten fontos a következők védelme:

- Eseménynaplók,
- Bizalmas adatok, személyes adatok
- Rendszer segédprogramokhoz való hozzáférés
- Forráskódhoz való hozzáférés

Jelen pontban írtakhoz hozzáférés az Információbiztonsági Felelős engedélyével történhet.

40. A jogosultságokat mindig a „legszűkebb hozzáférés" elve alapján szükséges meghatározni úgy, hogy azok biztosítsák a feladatok elvégzésének lehetőségét a legszűkebb hozzáférés segítségével.

41. Privilegizált szerepkörök – ezekből egy felhasználó nem tölthet be többet, csak egyet:

Információbiztonsági felelős: az ő felelőssége a biztonsági szabályok és eljárásrendek megvalósításának felügyelete;
Rendszer adminisztrátor: jogosult telepíteni, konfigurálni és karbantartani a szervezet alkalmazásait, de korlátozott a hozzáférése a biztonsággal kapcsolatos adatokhoz;
Rendszer operátor: ő a felelős a rendszerek napi üzemeltetéséért, és az ő feladata a rendszer mentése/visszaállítása, de nem tudja felügyelni vagy konfigurálni a rendszerek működését;
Rendszer auditor: jogosult a rendszerek naplóeseményeibe és archívumaiba betekinteni, a biztonsági szabályzatokkal összhangban végzett vizsgálatok céljából, nem tudhatja felügyelni vagy konfigurálni a bizalmi szolgáltatás működését.

42. A jogosultságkezelési szabályok a helyi és a távoli hozzáférések igénylésére is kiterjednek, automatikus VPN hozzáférés a szervezet informatikai rendszeréhez nem biztosítható.

43. A vezeték nélküli hálózat használata a szervezet munkavállalói számára automatikusan engedélyezett, a Diákok a „Student" a Vendégek a „Guest" wifi szolgáltatást használhatják, ahol ezek kiépítésre kerültek.

3.2 Alkalmazásokkal kapcsolatos elvárások

44. Minden a Hozzáférésvédelmi szabályzat hatálya alá bevont alkalmazásnak és azonosítási-hitelesítési funkciót ellátó infrastruktúra elemnek biztosítania kell a következőket:

- Funkciót/felületet a szerepkörök kezeléséhez;
- Funkciót/felületet a felhasználói fiókok kezeléséhez: azonosítók létrehozására, érvényességük letiltására, módosítására, ideiglenes fiókok kezelésére előre meghatározott lejárati idővel;
- Funkciót/felületet a jogosultságok kezeléséhez;
- Minden azonosító csak egyszer felhasználható legyen;
- a felhasználók adminisztrálásának lehetőségét;
- az információbiztonsági funkciókhoz való hozzáférést elkülönített jogosultsághoz kötött módon;
- Auditori felhasználói csoport létrehozásának lehetőségét
- Az alkalmazott hitelesítésre szolgáló eszközök tartalom védelmének (pl.: titkosított jelszó tárolás) és hozzáférés jogosultságainak (pl.: korlátozás) kezelését;
- A hitelesítésre szolgáló eszközök kezelése során az ellenőrző elemeket titkosított tárolásának lehetőségét (jelszó hash lenyomatok megfelelő algoritmus és salt alkalmazásával);
- fedett visszacsatolás lehetőségét a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.
- 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;
- Sikertelen bejelentkezési kísérlet esetén ne adjon támadáshoz felhasználható információt a hiba természetéről; korlátos számú sikertelen bejelentkezési kísérlet után blokkolja a felhasználót;
- Jelszavak nem látható módon történő megjelenését;
- a jelszómódosítás lehetőséget a felhasználói felületen is.
- a Privilegizált felhasználók jogosultságainak kezelésére többfaktoros hitelesítési lehetőséget.

45. Amennyiben egy rendszer használatához szükséges ismeret, vagy a jogosultságkezelés módja megváltozik, esetleg a rendszer funkciója relevánsan kiterjesztésre kerül, az alkalmazásgazda értesíti a Rendszergazdát és az Információbiztonsági Felelőst a szükséges jogosultsági változtatásokról, és az esetleges oktatási igényről.

3.3 Azonosító és jelszókezelés, jelszóvédelem

46. 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.

47. Minden jelszó, mely rendszer által a felhasználónak készül, legyen egyedi; generálásuk alapuljon véletlenszerű értékeken.

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

49. Amennyiben a felhasználói jelszó kompromittálódik vagy kompromittálódása felmerül, a jelszót azonnal meg kell változtatni. Ebben az esetben az incidenst az incidens kezelési szabályok szerint jelenteni kell.

3.3.1 Nem privilegizált fiókok – nevesített felhasználók

50. Minden jogosultságnak egyedi, természetes személyhez rendelhetőnek kell lennie. Nem szabad több felhasználó által használt un. csoport jogosultságokat létrehozni. A jelszavakkal kapcsolatban az alábbi előírásoknak kell eleget tenni:

    - Jelszóként tilos a jelszó tulajdonosával kapcsolatba hozható szót, kifejezést használni, a jelszó nem lehet azonos a felhasználói azonosítóval.
    - A jelszavak nem lehetnek rövidebbek, mint 8 karakter.
    - A jelszavaknál meg kell követelni a komplexitást, vagyis minimum tartalmaznia kell kis- és nagybetűket, 1 számot és 1 speciális karaktert (pl.: %,#,&,@,$).
    - A kiadott (default, kiindulási) jelszavak nem lehetnek triviálisak, kitalálhatóak. A jelszavakat a rendszergazdák személyesen, vagy telefonon adhatják át a felhasználóknak, azt e-mail-ben, vagy SMS-ben küldeni tilos.
    - 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.
    - A rendszernek a rendszeres jelszómódosítást ki kell kényszerítenie 180 naponként.
    - Korlátos számú (5) bejelentkezési kísérlet után a bejelentkezés lehetőségét blokkolni kell, mely blokkolást vagy a rendszergazda tudja feloldani, vagy a rendszer automatikusan 30 perc után feloldja amennyiben ez idő alatt nincs további hibás bejelentkezési kísérlet.

3.3.2 Privilegizált fiókok – nevesített felhasználók

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

52. Ezen felhasználók kéttényezős hitelesítés segítségével kapcsolódhatnak az elektronikus információs rendszerekhez.

53. Minden jogosultságnak egyedi, természetes személyhez rendelhetőnek kell lennie. Nem szabad több felhasználó által használt, úgynevezett csoport jogosultságokat létrehozni. A jelszavakkal kapcsolatban az alábbi előírásoknak kell eleget tenni:

    - Jelszóként tilos a jelszó tulajdonosával kapcsolatba hozható szót, kifejezést használni, a jelszó nem lehet azonos a felhasználói azonosítóval.
    - A jelszavak nem lehetnek rövidebbek, mint 10 karakter.

- A jelszavaknál meg kell követelni a komplexitást, vagyis minimum tartalmaznia kell kis- és nagybetűket, 1 számot és 1 speciális karaktert (pl.: %,#,&,@,$).
- 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.
- A rendszernek ki kell kényszeríteni első bejelentkezéskor a jelszómódosítást a kiadott szabályok szerint, amennyiben valamely rendszer erre nem képes, a felhasználónak a használatba vétel első napján a jelszómódosítást meg kell tennie.
- A rendszernek rendszeres jelszómódosítást kell kikényszerítenie 180 naponként.
- 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.
- Korlátos számú (5) bejelentkezési kísérlet után a bejelentkezés lehetőségét blokkolni kell, mely blokkolást vagy a rendszergazda tudja feloldani, vagy a rendszer automatikusan 30 perc után feloldja amennyiben ez idő alatt nincs további hibás bejelentkezési kísérlet.
- A Privilegizált felhasználók bejelentkezéséhez a második faktort a „Microsoft authenticator" biztosít.
- Privilegizált felhasználói fiókkal rendelkező felhasználóknak kötelező a nem biztonsági funkciók használatához nem a különleges jogosultsághoz kötött - úgynevezett nem privilegizált - fiókjukat vagy szerepkörüket használniuk.

3.3.3 Technikai felhasználók

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

55. A technikai felhasználók létrehozását a következők kezdeményezhetik:

    - Informatikai rendszerért általánosan felelős vezető;
    - Rendszer adminisztrátor.

56. 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 praktikus szempontokat is figyelembe véve.

57. A technikai felhasználókhoz beállított jelszavakat jegyzőkönyvezett módon az Információbiztonsági felelős páncél szekrényében papír alapon zárt sérülés biztosított módon borítékban szükséges elhelyezni.

58. E felhasználók jelszavaira a következő elvárások vonatkoznak:

    - A jelszavaknál meg kell követelni a komplexitást, vagyis minimum tartalmaznia kell kis- és nagybetűket, 1 számot és 1 speciális karaktert (pl.: %,#,&,@,$).
    - A jelszavak nem lehetnek rövidebbek mint 16 karakter.
    - 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.
    - A rendszernek rendszeres jelszómódosítást nem kell kikényszerítenie, mivel ez olyan kockázattal járhat, ami kiesést okoz.
    - A jelszó nem lehet egyező a megelőző 5 jelszóval, az utolsó jelszótól való eltérés minimum 2 karakter.
    - Korlátos számú (5) bejelentkezési kísérlet után a bejelentkezés lehetőségét blokkolni kell, mely blokkolást vagy a rendszergazda tudja feloldani, vagy a rendszer automatikusan 30 perc után feloldja amennyiben ez idő alatt nincs további hibás bejelentkezési kísérlet.

3.3.4 Szervezeten kívüli felhasználók

59. Szervezeten 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 a Rendszergazda csak az után állíthat be ilyen jellegű hozzáférést, miután meggyőződött a hozzáférési igény alapjául szolgáló jogviszony / kötelezettség meglétéről.

60. A szervezeten kívüli felhasználóval kapcsolatos hitelesítési elvárások megegyeznek a szervezeten belüli technikai felhasználóknál leírtakkal.

61. 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.

3.3.5 Távoli bejelentkezés, távmunka biztonsága

62. 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 a Rendszergazda állítja be.

63. 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.).

64. Távoli hozzáférések esetében a bejelentkezési azonosítási és hitelesítési elvárások azonosak a helyszíneken életbe léptetett szabályokkal.

3.3.6 Elfelejtett azonosítási / hitelesítési információk kezelése

65. Elfelejtett azonosítási információ esetén a felhasználó azonosítót a Rendszergazda küldi meg a felhasználó kérésére sms-ben vagy emailben a felhasználó kétséget kizáró azonosítása után.

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

3.4 Jogosultságok felülvizsgálatának folyamata

67. Az elektronikus információs rendszerek felhasználói fiókjait, email címeit évente legalább egyszer ellenőrizni szükséges. Az ellenőrzést az informatikai osztály támogatásával a HR osztály végzi. Az inaktív szükségtelen felhasználói fiókokat ezen felülvizsgálatok után meg kell szüntetni.

4 ZÁRÓ RENDELKEZÉSEK

68. Jelen Szabályzat annak aláírását követő napon lép hatályba.
69. Jelen Szabályzat hatálybalépésével minden hasonló tárgyú szabályzat hatályát veszti.
70. Jelen Szabályzatot a Kancellári Kabinet gondozza.
71. A Jelen Szabályzat megtalálható és elérhető a www.szfe.hu oldalon.

Budapest, 2021. szeptember 16.

Novák Emil
mb. általános rektorhelyettes

SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM
SZFE 1865
PH

dr. Szarka Gábor
kancellár

5 A SZABÁLYZATHOZ TARTOZÓ DOKUMENTUMOK JEGYZÉKE

5.1 Mellékletek

Átadás_Átvételi_ELISMERVÉNY_ITeszköz

Nyilatkozat magáncélú tartalom törléséről

SZFE 1865 SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM

Átadás-Átvételi elismervény informatikai eszközökhöz*

(*számítógép, laptop, monitor, telefon, adathordozó, belépőkártya egyéb)

Alulírott_____

cím:

a mai napon átvettem a következő eszközöket*:
(megnevezés és azonosító, gyári szám, darabszám, RFID kód)

1._____
2._____
3._____
4._____
5._____

eszközöket. Belépőkártya elvesztés esetén az 5.000.-Ft pótlási díj megtérítését vállalom.

Kelt:

_____ _____
Átadó Átvevő

Alulírott_____

€ a mai napon hiánytalanul átadtam a fent megjelölt eszközöket.
€ a mai napon átadtam a fent megjelölt eszközök közül a következőket:

1._____
2._____
3._____

a mai napon a fent megjelölt eszközök közül a következők nem kerültek átadásra:

1._____
2._____
3._____

a hiány oka / pótlása:

Kelt:

_____ _____
Átadó Átvevő

Jelen átadás-átvételi dokumentum kötelező részét képezi a Magáncélú tartalom törléséről szóló nyilatkozat.

Nyilatkozat magáncélú tartalom törléséről

Alulírott ..... (név), ... (munkavállalói / tanulói azonosító) kijelentem, hogy a mai napon a Színház- és Filmművészeti egyetem (a továbbiakban: Munkáltató) Informatikai Osztályának képviselője szóban tájékoztatott arról, hogy a Munkáltató tulajdonában lévő és a munkavégzésemhez használatra átvett eszközöknek a végleges visszavételére, valamint a hozzáférési jogosultságom megszüntetésére kerül sor. E körülményekre tekintettel az felszólított, hogy az eszközökön, a Munkáltató által biztosított adattároló rendszerekben (kiemelten, de nem kizárólag: számítógépen, laptopon, mobil adathordozón, OneDrive tárhelyen... stb.), illetve elektronikus levelezőrendszerben esetlegesen tárolt magáncélú személyes adataimat haladéktalanul mentsem le és töröljem. A tájékoztatást és felhívást tudomásul vettem.

Kijelentem, hogy az átadás-átvételi elismervényen felsorolt eszközökön, az elektronikus levelezőrendszerben és egyéb tárhelyeken tárolt valamennyi magáncélú személyes adatomhoz teljes körű hozzáférést kaptam, majd az érintett eszközökről és elektronikus levelezőrendszerből valamennyi magáncélú személyes adat a részemre maradéktalanul kimentésre és azt követően véglegesen és helyreállíthatatlanul törlésre került. Ennek megfelelően magáncélú személyes adataim kiadásával és törlésével kapcsolatos igényt Munkáltatóval szemben a továbbiakban nem terjesztek elő, más jellegű követelésem nincs, Munkáltató tulajdonában lévő más számítástechnikai eszközön nem helyeztem el magáncélú személyes adatot.

Kijelentem, hogy magántulajdonú, üzleti célból használt eszközeimről Munkáltató utasításának megfelelően minden üzleti célú adatot mentettem Munkáltató központi kiszolgálójára eszközeimről a védett adatokat visszaállíthatatlanul töröltem. Tisztában vagyok a követelmény megszegése esetén releváns jogkövetkeményekkel és kárfelelősséggel.
Kijelentem, hogy a jelen nyilatkozatommal összefüggő adatkezelésről szóló tájékoztatást az Munkáltatótól megkaptam, megismertem és megértettem.
Helység....., Dátum ....

Nyilatkozatot tevő aláírása