Ikt.sz.: SZFE/1092/2024

SZÍNHÁZ- ÉS FILMMŰVÉSZETI EGYETEM
SZFE 1865

4/2024. (05.06.) számú rektori szabályzat

A Színház-és Filmművészeti Egyetem Incidenskezelési Szabályzata

Hatályos: 2024. május 07. napjától

Preambulum

(1) A Színház- és Filmművészeti Egyetem (a továbbiakban: Egyetem) jelen incidenskezelési szabályzatban (a továbbiakban: Szabályzat) határozza meg a biztonságos működése egyes alapelveit, továbbá a tevékenysége során felmerülő rendkívüli események, incidensek bejelentésének, kivizsgálásának és kezelésének rendjét.

(2) A rendkívüli események kezelése kapcsán alapvető fontosságú a megelőzés. A megelőzés érdekében az Egyetemnek:
   a) rendelkeznie kell a biztonságos működéshez szükséges szabályzatokkal;
   b) eleget kell tennie a biztonságos informatikai környezet működtetéséhez szükséges technológiai feltételeknek; továbbá
   c) meg kell hoznia azokat a technikai és szervezési intézkedéseket, amelyek hozzájárulnak az Egyetem biztonságos működéséhez (például: zárt és tűzbiztos irattár, iratmegsemmisítő, szigorúan szabályozott hozzáférési jogosultságok, titkosított adattárolás, biztonsági másolat, naplózás stb.);
   d) a munkavállalókat rendszeres adatvédelmi, információbiztonsági és biztonsági képzésben kell részesítenie, továbbá magas szinten kell tartania a biztonsági tudatosságot; valamint
   e) a biztonsági intézkedéseket és azok hatásosságát folyamatosan vizsgálnia kell, valamint szükség szerint a változó körülményekhez kell igazítania.

(3) A Szabályzat hatálya alá tartozó személyek kötelesek a tevékenységük során az adott tevékenységre vonatkozó szabályzatokban vagy szerződésekben foglalt rendelkezések mellett a jelen Szabályzat előírásai szerint eljárni. A Szabályzat előírásait minden munkafolyamat és az Egyetem területén végzett tevékenység során, annak teljes tartama alatt figyelembe kell venni.

1.§
A Szabályzat célja

A Szabályzat célja, hogy meghatározza az Egyetem tevékenysége során felmerülő rendkívüli esemény bejelentésének, kivizsgálásának és kezelésének szabályait.

2.§
A Szabályzat hatálya

(1) A Szabályzat személyi hatálya kiterjed az Egyetemmel foglalkoztatási jogviszonyban állókra (a továbbiakban: munkavállalók) és az Egyetemmel hallgatói jogviszonyban állókra (a továbbiakban: hallgatók).

(2) A Szabályzat egyes előírásainak személyi hatálya továbbá a rájuk vonatkozó mértékben mindazon természetes személyekre (a továbbiakban: külső személyek) is kiterjed, akik az Egyetemmel szerződéses kapcsolatba kerülnek vagy az Egyetem területén tartózkodnak, illetve az Egyetem honlapját használják. A külső személyekre vonatkozó szabályokat az adott szerződés létrejötte előtt, továbbá az Egyetem területére belépéskor, valamint a honlap használata során ismertetni kell.

(3) A Szabályzat tárgyi hatálya mindazon rendkívüli eseményekre kiterjed, amelyek az Egyetem tevékenysége keretében vagy a területén, továbbá a honlapjának üzemeltetése során merülnek fel.

(4) A Szabályzat elsősorban a rendkívüli események bejelentésével, előzetes vizsgálatával és elhatárolásával kapcsolatos eljárási rendet tartalmazza, a részletes kivizsgálást a rendkívüli esemény szerinti megfelelő kategóriájával kapcsolatos más szabályzatok előírásai szerint kell elvégezni.

3.§
A rendkívüli esemény észlelése és bejelentése

(1) A rendkívüli esemény észlelése az az időpont, amikor a munkavállaló, a hallgató vagy a külső személy valamely szokásos tevékenységét technikai vagy más akadály, jelenség miatt nem tudja elvégezni.

(2) Az Egyetem tevékenysége vagy a honlapja használata során észlelt rendkívüli eseményt az észlelés után haladéktalanul, a melléklet szerinti nyomtatvány kitöltésével, és a(z) **incidens@szfe.hu** e-mail címre megküldéssel, be kell jelenteni. Azt a rendkívüli eseményt, amelyről már az észlelés pillanatában megállapítható, hogy általános biztonsági incidens (pl. tűz, árvíz, betörés) az Egyetem belső működési rendje szerint kell kezelni, az elhárítást az észszerűen elvárható módon meg kell kezdeni. Amennyiben az általános biztonsági incidens következményeinek elhárítása során vagy azt követően felmerül, hogy a környezeti kár érinti a személyes adatok kezelését, haladéktalanul értesíteni kell az adatvédelmi tisztviselőt. Amennyiben az általános biztonsági incidens olyan környezeti kárt okozott, amely az informatikai biztonsági intézkedések sérelmét jelenti, értesíteni kell az információbiztonsági felelőst.

(3) Ha a rendkívüli eseményről az észlelés pillanatában megállapítható, hogy információs rendszereket érint, az Információibiztonsági Szabályzat szerinti és észszerűen elvárható haladéktalan informatikai intézkedéseket meg kell tenni.

4.§
Incidensvizsgáló bizottság

(1) A rendkívüli eseményről, valamint incidensről szóló bejelentést az adatvédelmi tisztviselő és az információbiztonsági felelős fogadja.

(2) A rendkívüli esemény előzetes kivizsgálásához incidensvizsgáló bizottságot kell felállítani, melynek állandó tagjai az adatvédelmi tisztviselő és az információbiztonsági felelős, azonban a létszám további szakértőkkel bővíthető.

(3) A rendkívüli esemény kategóriájának megállapításáig az incidensvizsgáló bizottság munkáját az információbiztonsági felelős koordinálja.

(4) Az incidensvizsgáló bizottság összetétele a rendkívüli esemény jellegétől függően változhat. Az incidensvizsgáló bizottság összetétele a rendkívüli esemény előzetes, illetve a részletes kivizsgálása során felmerült tények ismeretében is változhat.

(5) Az információbiztonsági felelős értesíti mindazon szakterületeket, amelyek a rendkívüli esemény előzetes kivizsgálásában érintettek lehetnek. A szakterületek megfelelő felkészültséggel és tapasztalattal rendelkező munkavállalót kötelesek delegálni az incidensvizsgáló bizottságba.

(6) Az incidensvizsgáló bizottság koordinálásával kapcsolatos feladatokat a rendkívüli esemény kategóriába sorolását követően az a felelős személy látja el, akinek hatáskörét a rendkívüli esemény érinti. Az incidensvizsgáló bizottságot adatvédelmi incidens esetén az adatvédelmi tisztviselő koordinálja és képviseli az Egyetem szervezeti egységei felé. Az incidensvizsgáló bizottságot informatikai biztonsági incidens esetén az információbiztonsági felelős koordinálja és képviseli az Egyetem szervezeti egységei felé. Az incidensvizsgáló bizottságot általános biztonsági incidens esetén a rektor által kijelölt munkavállaló koordinálja és képviseli az Egyetem szervezeti egységei felé.

(7) Amennyiben a rendkívüli esemény több szakterületet is érint, az Egyetem rektora dönt az incidensvizsgáló bizottságot koordináló személyről.

(8) Az incidensvizsgáló bizottság tagjainak – szükség esetén – munkaidőn kívül is rendelkezésre kell állniuk.

(9) Az incidensvizsgáló bizottság megalakulásáról az incidensvizsgáló bizottság koordinálását végző személy az előzetes kivizsgálás megkezdésével egyidejűleg értesíti a rektort.

(10) Az adatvédelmi tisztviselő és az információbiztonsági felelős munkaköri leírásában szerepeltetni kell az incidensvizsgáló bizottságban történő részvételüket, illetve a rendkívüli események előzetes és részletes kivizsgálással kapcsolatos teendőiket.

5.§

A rendkívüli esemény előzetes kivizsgálása, a rendkívüli események elhatárolása

(1) Az incidensvizsgáló bizottság az előzetes kivizsgálás keretében megvizsgálja a rendkívüli eseményről szóló bejelentés adatait, valamint besorolja a rendkívüli eseményt.

(2) A rendkívüli eseményről szóló adatok előzetes megvizsgálása során az alábbi szempontokat kell figyelembe venni:

a) a rendkívüli esemény személyes adatot érint-e,

b) a rendkívüli esemény az informatikai biztonsági előírások sérelmére utal-e,

c) a rendkívüli esemény környezeti kárt, illetve a működés zavarát okozta-e.

(3) A rendkívüli esemény – az előzőekben felsorolt szempontok alapján – lehet adatvédelmi incidens, informatikaibiztonsági incidens és általános biztonsági incidens (vagy kettő, esetleg mindhárom egyidejűleg).

(4) Az adatvédelmi incidens az adatvédelmi tisztviselő, az informatikai biztonsági incidens az információbiztonsági felelős, az általános biztonsági incidens az általános biztonsági feladatokat ellátó munkatárs (a továbbiakban: biztonsági felelős) hatáskörébe tartozik. Amennyiben egy incidens adatvédelmi és információbiztonsági incidens is, annak kivizsgálása és a megfelelő intézkedések megtétele az adatvédelmi tisztviselő kötelessége, míg az incidensekkel kapcsolatos felelősséget a vonatkozó jogszabályi rendelkezések alapján elsődlegesen az adatkezelő viseli.

(5) A rendkívüli esemény érinthet egyszerre több szakterületet is. Az előző pont alapján kijelölt személynek gondoskodnia kell a szakterületek zökkenőmentes együttműködéséről, valamint az érintett szakterületek alapvető előírásainak érvényesítéséről a rendkívüli esemény előzetes vizsgálata során.

(6) A rendkívüli események elhatárolásához a hatályos Adatvédelmi Szabályzat, az Információbiztonsági Szabályzat, továbbá az általános biztonsági előírásokat figyelembe kell venni.

(7) A rendkívüli események kategóriába sorolásával kapcsolatos problémák esetén a rektor dönt.

(8) A rendkívüli események előzetes kivizsgálását lehető leghamarabb, legfeljebb 3 naptári napon belül el kell végezni.

(9) Az előzetes vizsgálat eredményeként el kell dönteni, valamint írásba kell foglalni, hogy a rendkívüli esemény melyik jelen Szabályzatban rögíztettkategóriába tartozik. Az előzetes vizsgálat eredményének rögzítésével egyidejűleg – szükség szerint – intézkedni kell a további, részletes vizsgálat megindításáról. Amennyiben az előzetes vizsgálatot követően nem indul további, részletes vizsgálat, annak tényét és okát az előzetes vizsgálat eredményét rögzítő dokumentumban fel kell tüntetni.

(10) Amennyiben a rendkívüli esemény adatvédelmi incidens, a tudomásra jutás időpontja az az időpont, amikor az incidensvizsgáló bizottság írásba foglalta, hogy adatvédelmi incidens történt. Az adatvédelmi incidens részletes vizsgálatát a hatályos Adatvédelmi Szabályzatban rögzített eljárási rend szerint kell folytatni. Az adatvédelmi incidens részletes vizsgálata során szem előtt kell tartani az adatvédelmi felügyeleti hatóságnak történő bejelentés határidejét.

(11) Amennyiben a rendkívüli esemény informatikai biztonsági incidens:
   a) figyelembe kell venni a különböző informatikai biztonsági szabályozásokban a sérülékenységek elhárítására vonatkozó rendelkezéseket;
   b) amennyiben az Egyetem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni;
   c) ha az Egyetem nem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt manuális módon kell azonnal elkezdeni;
   d) amennyiben a sérülékenység elhárítása belső erőforrásból nem kivitelezhető, akkor külső szakértőket kell bevonni az elhárítás folyamatába.

(12) Az informatikai biztonsági incidens részletes vizsgálatát az Információbiztonsági Szabályzat szerint kell folytatni.

(13) Amennyiben a rendkívüli esemény általános biztonsági incidens, a további részletes vizsgálatot az Egyetem belső működési rendje szerint kell lefolytatni.

6.§
A rendkívüli eseménnyel kapcsolatos dokumentációs kötelezettség

(1) Az incidensvizsgáló bizottság üléseiről emlékeztetőt, döntéseiről indoklást is tartalmazó jegyzőkönyvet, vizsgálatairól pedig intézkedési javaslatokat is tartalmazó jelentést kell készíteni.

(2) Az incidensvizsgáló bizottság munkáját tartalmazó dokumentumok kezelésére az Egyetem mindenkori iratkezelési szabályai az irányadók.

(3) Amennyiben az incidens vizsgálata során az Egyetem tevékenységével kapcsolatban olyan megállapításra kerül sor, amelynek nyilvánosságra hozatala vagy közismertsége a befolyásmentes működést veszélyezteti, az incidensvizsgáló bizottság korlátozhatja a tevékenységéről szóló dokumentumokba betekintők körét (ide nem értve a rektort).

(4) Az Egyetem a hatályos Adatvédelmi Szabályzat szerinti nyilvántartást vezet a bekövetkezett adatvédelmi incidensekkel kapcsolatos tényekről és intézkedésekről.

(5) Az Egyetem az Információbiztonsági Szabályzatnak megfelelő nyilvántartást vezet a bekövetkezett informatikai biztonsági incidensekkel kapcsolatos tényekről és intézkedésekről.

(6) Az Egyetem a belső működési rendje szerinti nyilvántartásokat vezeti a bekövetkezett általános biztonsági incidensekkel kapcsolatos tényekről és intézkedésekről.

(7) Az adatvédelmi incidensek vizsgálata során keletkezett, papíralapú és elektronikus, iktatott dokumentumokat az adatvédelmi tisztviselő az adatvédelmi incidens vizsgálatának lezárásától számított 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

(8) Az informatikai biztonsági incidensek vizsgálata során keletkezett, papíralapú és elektronikus, iktatott dokumentumokat az információbiztonsági felelős az informatikai biztonsági incidens vizsgálatának lezárásától számított 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

(9) Az általános biztonsági incidensek vizsgálata során keletkezett, papíralapú és elektronikus, iktatott dokumentumokat a rektor által kijelölt szervezeti egység az általános biztonsági incidens vizsgálatának lezárásától számított 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

7.§
Záró rendelkezések

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

(2) A jelen Szabályzat hatálybelépésével 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

Mellékletek:

1. számú melléklet: Alapfogalmak
2. számú melléklet: Incidensbejelentő űrlap
3. számú melléklet: Incidens kivizsgálási jegyzőkönyv

1. számú melléklet
Alapfogalmak

Jelen Szabályzat alkalmazása során az alábbi fogalmakat kell alkalmazni:

a) ***adat*:** valaki vagy valami megismeréséhez, jellemzéséhez hozzásegítő, nyilvántartott tény, részlet, értelmezhető, de még nem értelemzett ismeret.

b) ***információ*:** a kapott adat felruházása az adott helyzetben általunk tulajdonított jelentéssel, értelmezett ismeret.

c) ***adatvédelem*:** a személyes adatok (magánszféra) jogi védelme, alkotmányos alapjog.

d) ***biztonság*:** valakinek vagy valaminek veszélytől, kártól, jogtalan beavatkozástól, bántódástól való védett állapota, helyzete. A biztonság az Egyetem azon állapota, amelyben a folyamatos, zavartalan és teljes körű felsőoktatási és a kapcsolódó üzemeltetési, üzleti tevékenység folytatható, fenntartható, illetve a rendeltetésszerű működést veszélyeztető szándékos vagy gondatlan, jogellenes magatartások, valamint az ezekkel szemben állított védelmi erőforrások és intézkedések kiegyenlítik egymást.

e) ***adatbiztonság*:** a személyes adatok jogosulatlan kezelése, így különösen jogosulatlan megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben a személyes adatok sérülésének, illetéktelen felhasználásának, megsemmisülésének kockázati tényezőit – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik.

f) ***információbiztonság*:** bizalmasság, sértetlenség, rendelkezésre állás elvének érvényesülése (részterületei: személyi, fizikai, adminisztratív, elektronikus biztonság).

g) ***alapkövetelmények:*** rendelkezésre állás (elérhetőség a jogosultaknak), sértetlenség (sérthetetlenség, valódiság), az adatok jellegétől függő bizalmas kezelés, hitelesség, a teljes információs rendszer működőképessége.

h) ***informatikai biztonság*:** ha az információs rendszer védelme az alapkövetelmények szempontjából zárt (minden fontos fenyegetést figyelembe vesz), teljes körű (a rendszer összes elemére kiterjed), folyamatos (az időben változó körülmények ellenére is megszakítás nélküli) és kockázatarányos (a feltehető kárérték és a kár valószínűségének szorzata nem haladja meg az előre rögzített küszöbértéket).

i) ***rendkívüli esemény vagy incidens:*** bármilyen tevékenység vagy gyanús jelenség, amely kívül esik a szokásos gyakorlaton és paramétereken, váratlan, nem kívánt, általában kellemetlen esemény vagy jelenség, az Egyetem tevékenységének ellátását lassító, akadályozó vagy megbénító gondatlan vagy jogellenes magatartások és a természeti csapások eseményeinek összessége.

j) ***általános biztonsági incidens:*** olyan esemény vagy jelenség, amely vagy a természet erőinek hatására következik be (villámcsapás, vihar, belvíz, árvíz, szélsőséges időjárás stb.), vagy egyéb módon (pl. tűz, csőtörés, áramszünet, betörés, bombariadó stb.) környezeti vagy vagyoni kárt, illetve a működésben zavart okoz.

k) ***adatvédelmi incidens:*** a(z adat)biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi, s ez az érintett jogaira és szabadságaira valószínűsíthetően kockázattal jár.

l) ***információbiztonsági incidens:*** nem kívánt vagy nem várt egyedi, vagy sorozatos információbiztonsági esemény, amely nagy valószínűséggel veszélyezteti az üzleti tevékenységet és fenyegeti az informatikai rendszert.

m) ***kockázat:*** fenyegetettségek bekövetkezési valószínűsége és a bekövetkezéskor keletkező károk függvénye.