ESZTERGOMI SZAKKÉPZÉSI CENTRUM

Esztergomi Szakképzési Centrum
Ikt.sz.: NSZFH/ 615 .000170-1./2025 :

Az Esztergomi Szakképzési Centrum

Informatikai biztonsági szabályzata

(IBSZ)

Egységes szerkezetben az alábbi szabályzatokkal:

Jelszókezelési szabályzat

Eszközkezelési szabályzat

2025. július 31.

Jóváhagyta:

Esztergomi Szakképzési Centrum 3.

....

Kovács Tamás kancellár Simon Attila gazdasági vezető

1. Tartalomjegyzék

2. Verziókövetés

Verzió	Felülvizsgálat/Módosítás dátuma	Módosítás	Módosítást végezte	Kiadás dátuma	Kiadta
1.0	-	Első verzió	Fülöp Tamás Miklós		

3. A szabályzat célja

Az információbiztonsági szabályozás célja az Esztergomi Szakképzési Centrum (a továbbiakban: ESZC) eszköz- és adatvagyon védelmének intézményi szintű meghatározása, ezen belül különösen azoknak a technikai és szervezési intézkedéseknek a meghatározása, amelyeket jogszabály, különösen a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény és jogi környezete, illetve egyéb információbiztonsági szabályozások megkívánnak, valamint a szervezeti célok érvényre juttatásához szükségesek. A szabályozás továbbá meghatározza azokat a védelmi intézkedéseket, amelyek biztosítják az adatok, információk védelmét a bizalmasság, sértetlenség és rendelkezésre állás szempontjából.

Az ESZC az információs vagyona megőrzésére, valamint a törvényi kötelezettségek és felügyeleti szabályok betartására irányuló intézkedések megfogalmazása érdekében kialakította azt az információbiztonsági rendszert, amelynek fő dokumentuma az Információ Biztonsági Szabályzat (a továbbiakban: IBSZ).

4. A szabályzat hatálya

Az IBSZ hatálya kiterjed az ESZC székhelyére és minden telephelyére, valamint minden, az ESZC-vel foglalkoztatásra irányuló, tanulói és egyéb jogviszonyban álló félre, és minden informatikai eszközre, adatkapcsolatra. Amennyiben egy az ESZC által bérelt vagy más jogcímen használt objektumban ESZC tulajdonú informatikai eszköz használatára kerül sor, úgy a használat idejére az IBSZ hatálya kiterjed e helyiségre, valamint az intézet tulajdonában lévő informatikai eszközt vagy rendszert használó személyre is.

A jelen szabályozással kapcsolatos kérdésekben – a 2024. évi LXIX. törvény. 6. § (3) bekezdés 2. pontja szerint az ESZC kancellárja által kinevezett vagy megbízott – az ESZC elektronikus információs rendszerének biztonságáért felelős személy (a továbbiakban: IBF) ad felvilágosítást.

Az IBSZ-ben foglaltak érvényre juttatása érdekében a szabályozás előírásainak betartását minden olyan külső partnerrel kötött szerződésben és megállapodásban kötelezően elő kell írni, amelynek keretében a külső partner (beleértve annak foglalkoztatottjait, alvállalkozóit, illetve az általa meghívott személyeket) a szabályozás hatálya alá eső helyen munkát végez vagy szállít. Ennek érdekében az informatikailag érintett szerződéstervezeteket információbiztonsági szempontú véleményezésre el kell küldeni az IBF-nek.

A szabályzat hatálya nem terjed ki azon rendszerekre, szoftverekre és rendszerelemekre, amelyekre az KKK (Képzési és Kimeneti Követelmények) dokumentumai érvényesek.

5. Fogalommeghatározások

A fogalommeghatározások tekintetében az IBSZ alkalmazása során Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény 4.§-ban meghatározott definíciókat kell alkalmazni, az IBSZ szempontjából nem releváns részek kihagyásával. A számozások a törvényt követik, ezért a számozás nem folyamatos.

1. *adat*: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

2. *adatfeldolgozás*: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

3. *adatfeldolgozó*: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

4. *adatkezelés*: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

5. *adatkezelő*: az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti fogalom;

6. *adatkicserélő szolgáltatás*: az elektronikus hírközlésről szóló törvény szerinti fogalom;

7. *adatközponti szolgáltatás*: olyan szolgáltatás, amely központosított elhelyezést, összeköttetést és működést biztosít adattároló, -feldolgozó és -továbbító információtechnológiai és hálózati berendezések számára, ideértve az energiaellátást és környezeti felügyeletet biztosító létesítményeket és infrastruktúrát is;

8. *adatosztályozás*: a szervezet által az elektronikus információs rendszerben kezelt adatok és információk biztonsági besorolása azok bizalmasságának, sértetlenségének és rendelkezésre állásának szempontjából;

9. *ágazaton belüli kiberbiztonsági incidenskezelő központ*: olyan kiberbiztonsági incidenskezelő központ, amelyet az e törvény hatálya alá tartozó egy vagy több, egy ágazathoz tartozó szervezet az ágazaton belül meghatározott szakterületen előforduló kiberbiztonsági incidenseinek a központosított és egységes kezelése érdekében üzemeltet;

10. *auditor*: az e törvény szerinti kiberbiztonsági audittevékenység végzésére jogosult, független gazdálkodó szervezet;

11. *behatolásvizsgálat*: olyan sérülékenységvizsgálati módszer, amelynek során az IKT-rendszer, valamint az elektronikus információs rendszer gyenge pontjainak feltárására és kihasználhatóságának ellenőrzésére kerül sor a biztonsági intézkedések elleni rosszindulatú támadások szimulációjával;

12. *belső informatikai biztonsági vizsgálat*: olyan sérülékenységvizsgálati módszer, amelynek során az informatikai rendszer sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik, vagy a belső hálózatban használt eszköz, vagy rendszerelem vizsgálata kerül végrehajtásra;

13. *bizalmasság*: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

14. *bizalmi szolgáltatás*: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

15. *bizalmi szolgáltató*: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

16. *biztonsági osztály*: az elektronikus információs rendszer védelmének elvárt erőssége;

17. *biztonsági osztályba sorolás*: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;

18. *digitális szolgáltatás*: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

19. *DNS*: hierarchikusan felépülő elnevezési rendszer, más néven doménnévrendszer, amely lehetővé teszi az internetes szolgáltatások és erőforrások azonosítását, lehetővé téve a végfelhasználók eszközei számára az internetes útvonal-meghatározási és összekapcsolási szolgáltatások igénybevételét e szolgáltatások és erőforrások elérése érdekében;

20. *DNS-szolgáltató*: olyan szervezet, amely a következő szolgáltatások valamelyikét nyújtja a szervezeten kívüli más szervezet vagy személy részére: a) autoritatív DNS-szolgáltatás: a doménnév – doménnév-regisztrációt végző szolgáltató által kezelt – adatainak lekérdezését közvetlenül lehetővé tevő szolgáltatás, amely a legfelső szintű doménnév- nyilvántartó szolgáltatás része, b) rekurzív DNS-szolgáltatás: olyan DNS-szolgáltatás, amely a felhasználók doménnév-lekérdezéseit a megfelelő autoritatív DNS-szolgáltatókhoz továbbítja a hierarchikusan felépülő doménnévrendszerben és az autoritatív DNS-szolgáltató által a lekérdezésre adott válaszokat továbbítja a felhasználó részére, c) DNS-gyorsítótárazás: a doménnév-lekérdezésre adott válaszok átmeneti tárolása és a felhasználói lekérdezéseknek a tárolt doménnévadatok alapján történő kiszolgálása,

21. *doménnév*: az internetes kommunikációhoz használt IP-cím alfanumerikus karakterekből álló megfelelője,

22. *doménnév-regisztrációt végző szolgáltató*: a legfelső szintű doménnév-nyilvántartó által felhatalmazott szolgáltató, amely jogosult domén regisztrálására;

23. *elektronikus hírközlési szolgáltató*: az elektronikus hírközlésről szóló törvény szerinti fogalom;

24. *elektronikus információs rendszer*:
a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlési hálózat,

b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi, ideértve a kiber-fizikai rendszereket, vagy
c) az a) és b) alpontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

25. *elektronikus információs rendszer biztonsága*: az elektronikus információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;

26. *életciklus*: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

27. *esemény*: az elektronikus információs rendszerben bekövetkezett állapotváltozás;

28. *európai kiberbiztonsági tanúsítási rendszer*: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 9. pontja szerinti fogalom;

29. *felhasználó szervezet*: központi rendszert vagy központi szolgáltatást igénybe vevő szervezet;

30. *felhőszolgáltatás*: olyan digitális szolgáltatás, amely önkiszolgáló módon történő hálózati hozzáférést tesz lehetővé igény szerint méretezhető, megosztott fizikai vagy virtuális erőforrások rugalmas készletéhez;

31. *felhőszolgáltató*: felhőalapú számítástechnikai szolgáltatást nyújtó szervezet;

32. *gyártó*: az IKT-termék gyártója, IKT-szolgáltatás nyújtója, valamint IKT-folyamat gyártója vagy nyújtója;

33. *használatbavétel*: az elektronikus információs rendszer adatokkal való feltöltése és rendeltetésszerű használatának megkezdése;

40. *jelentős kiberbiztonsági incidens*:
a) a közvetlenül alkalmazandó európai uniós jogi aktusban ekként meghatározott kiberbiztonsági incidens,
b) közvetlenül alkalmazandó európai uniós jogi aktus hiányában az olyan kiberbiztonsági incidens, amely
ba) a szervezet üzleti szolgáltatásának vagy a szervezet által nyújtott szolgáltatásnak legalább 5%-os csökkenésével vagy a szervezet éves bevételének legalább 5%-os kiesésével jár vagy fenyeget;
bb) súlyos működési zavart okoz vagy képes okozni a szolgáltatásokban, vagy pénzügyi vagy reputációs veszteséget okoz vagy képes okozni a kiberbiztonsági incidens által érintett szervezetnek vagy személynek; vagy
bc) jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett, vagy képes érinteni;

41. *jelentős kiberfenyegetés*: olyan kiberfenyegetés, amelyről – technikai jellemzői alapján – feltételezhető, hogy jelentős vagyoni vagy nem vagyoni hátrányt vagy kárt okozva súlyos hatást gyakorolhat egy szervezet elektronikus információs rendszereire vagy a szervezet szolgáltatásainak felhasználóira;

42. *képviselő*: Magyarországon letelepedett minden olyan természetes vagy jogi személy, akit vagy amelyet kifejezetten kijelöltek arra, hogy valamely, Magyarországon nem letelepedett szervezet nevében eljárjon, és akihez vagy amelyhez a kiberbiztonsági hatóság, vagy a kiberbiztonsági incidenskezelő központ az adott szervezet helyett fordulhat;

43. *kiberbiztonság*: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 1. pontjában meghatározott fogalom;

44. *kiberbiztonsági audit*: az elektronikus információs rendszerek biztonsági osztályba sorolása, valamint a biztonsági osztályba sorolás szerinti védelmi intézkedések megfelelőségének ellenőrzése;

45. *kiberbiztonsági hatóság*: a 23. § (1) bekezdés a) és b) pontja, valamint (2) bekezdése szerinti hatóság;

46. *kiberbiztonsági incidens*: olyan esemény, amely veszélyezteti az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát;

47. *kiberbiztonsági incidenskezelés*: minden olyan tevékenység és eljárás, amelynek célja a kiberbiztonsági incidens megelőzése, észlelése, elemzése és elszigetelése vagy a kiberbiztonsági incidensre való reagálás és a kiberbiztonsági incidenst követően a működés helyreállítása;

48. *kiberbiztonsági incidenskezelő központ*: a 63. § (1) és (2) bekezdése szerinti szerv;

49. *kiberbiztonsági incidensközeli helyzet*: olyan esemény, amely veszélyeztethette volna az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;

50. *kiberfenyegetés*: az (EU) 2019/881 európai parlamenti és tanácsi rendelet 2. cikk 8. pontjában meghatározott fogalom;

51. *kiber-fizikai rendszer*: olyan programozható elektronikus információs rendszerek, amelyek kölcsönhatásba lépnek a fizikai környezettel vagy kezelik a fizikai környezettel kölcsönhatásba lépő eszközöket. Ezek az elektronikus információs rendszerek közvetlenül fizikai változást érzékelnek vagy idéznek elő az eszközök, folyamatok és események megfigyelésével vagy vezérlésével;

52. *kihelyezett (irányított) infokommunikációs biztonsági szolgáltatást nyújtó szolgáltató*: olyan kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató, amely a kiberbiztonsági kockázatok kezelését végzi vagy azzal összefüggő szolgáltatást nyújt;

53. *kihelyezett (irányított) infokommunikációs szolgáltatást nyújtó szolgáltató*: olyan szervezet, amely az IKT-termék, hálózat, infrastruktúra, alkalmazás vagy bármely más elektronikus információs rendszer telepítésével, kezelésével, üzemeltetésével vagy karbantartásával kapcsolatos szolgáltatásokat nyújt a szolgáltatást igénybe vevő telephelyén vagy távolról; 54. kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának, bekövetkezési valószínűségének és az ez által okozott kár nagyságának a függvénye; 55. kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének, fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;

56. *kockázatkezelés*: az elektronikus információs rendszerre ható kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása és az intézkedések végrehajtása;

57. *kockázatmenedzsment keretrendszer*: olyan strukturált, ugyanakkor rugalmas megközelítés és szervezeti folyamatok összessége, amely integrálja a kiberbiztonsággal kapcsolatos kockázatkezelési tevékenységeket a rendszerfejlesztési életciklusban a kockázatokkal arányos védelmi intézkedések azonosításán, bevezetésén, értékelésén, működtetésén és nyomon követésén keresztül az új és már használatban lévő rendszerek fenyegetettségeinek folyamatos felderítése, és kockázatainak hatékony kezelése érdekében;

58. *közigazgatási szerv*: az 1. melléklet 1–13. pontja szerinti szervezet;

59. *közösségimédia-szolgáltatási platform*: olyan platform, amely lehetővé teszi a végfelhasználók számára, hogy több eszközön keresztül kapcsolódjanak, tartalmakat osszanak meg, fedezzenek fel és kommunikáljanak egymással;

60. *központi rendszer*: egyes állami, önkormányzati feladatok ellátását segítő, zárt ügyfélkör számára központosítottan fejlesztett vagy működtetett elektronikus információs rendszer, amelyen keresztül megvalósított funkciókat egy adott intézményi körben kötelezően vagy opcionálisan vesznek igénybe a felhasználó szervezetek;

61. *központi szolgáltatás*: a központi szolgáltató által kötelezően vagy egyedi igény alapján biztosítandó szolgáltatás;

62. *központi szolgáltató*: olyan szervezet, amely állami és önkormányzati feladatot ellátó szervezet részére jogszabály alapján kizárólagos joggal nyújt informatikai és elektronikus hírközlési szolgáltatást;

63. *kutatóhely*: a tudományos kutatásról, fejlesztésről és innovációról szóló törvény szerinti kutatóhely – az oktatási intézmények kivételével –, amelynek elsődleges célja alkalmazott kutatás vagy kísérleti fejlesztés folytatása a kutatás eredményeinek kereskedelmi célokra való hasznosítása céljából;

64. *legfelső szintű doménnév-nyilvántartó*: olyan szervezet, amelyre egy meghatározott legfelső szintű domént bíztak és amely felelős egyrészt a legfelső szintű domén kezeléséért – ideértve a legfelső szintű domén alatti doménnevek nyilvántartásba vételét –, másrészt a legfelső szintű domén technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését,

adatbázisainak karbantartását és a legfelső szintű doménzónafájlok elosztását a névszerverek között, függetlenül attól, hogy ezeknek az üzemeltetési tevékenységeknek bármelyikét maga a szervezet végzi vagy azokat kiszervezi, kivéve azokat az eseteket, amikor a legfelső szintű doménneveket a nyilvántartó kizárólag saját használatra veszi igénybe;

65. *megfelelőségértékelés*: az az értékelési eljárás, amely bizonyítja, hogy egy IKT-termékkel, IKT-folyamattal, IKT-szolgáltatással kapcsolatos, meghatározott követelmények teljesültek;

66. *megfelelőségértékelő szervezet*: a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről szóló, 2008. július 9-i 765/2008/EK európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom;

67. *megfelelőségi nyilatkozat*: a gyártó vagy a szolgáltató által kiállított dokumentum, amely igazolja, hogy egy adott IKT-termék, IKT-szolgáltatás vagy IKT-folyamat esetében értékelték, hogy az megfelel-e valamely nemzeti kiberbiztonsági tanúsítási rendszer biztonsági követelményeinek;

68. *megfelelőségi önértékelés*: az (EU) 2019/881 európai parlamenti és tanácsi rendeletben ekként meghatározott fogalom;

70. *minősített bizalmi szolgáltatás*: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

71. *minősített bizalmi szolgáltató*: a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló törvény szerinti fogalom;

72. *műszaki előírás*: az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/ EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendelet (a továbbiakban: 1025/2012/EU rendelet) 2. cikk 4. pontjában meghatározott fogalom;

74. *nagyszabású kiberbiztonsági incidens*: olyan kiberbiztonsági incidens, amely olyan mértékű zavart okoz, amely meghaladja Magyarországnak az arra való reagálási képességét, vagy amely Magyarországra és legalább még egy másik országra jelentős hatást gyakorol;

75. *nem privát felhőszolgáltatás*: olyan szolgáltató által nyújtott felhőszolgáltatás, amelyet a szolgáltató bárki számára elérhető módon vagy kizárólag a szervezetek egy meghatározott köre számára nyújt;

76. *nemzeti kiberbiztonsági incidenskezelő központ*: az Európai Hálózat- és Információbiztonsági Ügynökség ajánlásai szerint működő, kiberbiztonsági incidensekre reagáló egység, amely a nemzetközi hálózatbiztonsági, valamint kritikus információs infrastruktúrák védelmére szakosodott szervezetekben tagsággal rendelkezik [európai használatban: CSIRT (Computer Security Incident Response Team), amerikai használatban: CERT (Computer Emergency Response Team)];

81. *online keresőprogram*: az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról szóló, 2019. június 20-i (EU) 2019/1150 európai parlamenti és tanácsi rendelet 2. cikk 5. pontjában meghatározott fogalom;

82. *online piactér*: olyan szolgáltatás, amely a kereskedő által vagy a kereskedő nevében működtetett szoftvert, többek között weboldalt, valamely weboldal egy részét vagy valamely alkalmazást használ, és amelynek révén a fogyasztók távollevők közötti szerződést köthetnek más kereskedőkkel vagy fogyasztókkal;

83. *regisztrált felhasználói jogosultság*: a biztonsági vizsgálatot végző személy számára a sérülékenységvizsgálat elvégzése érdekében célzottan létrehozott felhasználói jogosultság;

84. *rendelkezésre állás*: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

85. *sebezhetőség*: IKT-termék, -szolgáltatás, -folyamat gyengesége, érzékenysége vagy hiányossága, amelynek kihasználása veszélyezteti vagy sérti az IKT-termék, -szolgáltatás, -folyamat bizalmasságát, sértetlenségét vagy rendelkezésre állását;

86. *sértetlenség*: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik, azaz hiteles, valamint a származás ellenőrizhetőségét, bizonyosságát, azaz letagadhatatlanságát is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

87. *sérülékenység*: az elektronikus információs rendszer gyengesége, érzékenysége vagy hiányossága, amelynek kihasználása veszélyezteti vagy sérti egy elektronikus információs rendszer bizalmasságát, sértetlenségét vagy rendelkezésre állását;

88. *sérülékenységkezelési terv*: a sérülékenységek megszüntetésére irányuló tervdokumentum;

89. *sérülékenységvizsgálat*: sérülékenységmenedzsment eszköz vagy módszer, amely során informatikai rendszerek, hardverek és szoftverek biztonsági szempontból történő átvizsgálása zajlik, az ellenőrzést automatizált eszközökkel és közvetlen, szakértő által végzett vizsgálatokkal hajtják végre;

90. *szabvány*: az 1025/2012/EU rendelet 2. cikk 1. pontjában meghatározott fogalom;

91. *szervezet*: állami szerv vagy állami szervezet, a Polgári Törvénykönyvről szóló törvény szerinti jogi személy, jogi személyiség nélküli szervezet;

92. *támogató rendszer*: az 1. § (1) bekezdés a)–c) pontja szerinti szervezet alapfeladatainak ellátásában közvetlenül nem részt vevő elektronikus információs rendszer, amely szükséges azon rendszerek működéséhez, amelyek alapfeladatot látnak el;

93. *tanúsítás*: független harmadik fél által végzett megfelelőségértékelési tevékenység;

94. *tartalomszolgáltató hálózat szolgáltatója*: a digitális tartalmak és szolgáltatások széles körű, akadálymentes és gyors rendelkezésre állását biztosító, földrajzilag elosztott szerverek hálózatának szolgáltatója;

95. *távoli sérülékenységvizsgálat*: olyan sérülékenységvizsgálat, amelynek során
a) az elektronikus információs rendszer internet felőli, külső sérülékenységvizsgálatára kerül sor, amelynek keretében az interneten fellelhető, nyilvános adatbázisokban való szabad keresés, célzott információgyűjtés, valamint az elérhető számítógépek szolgáltatásai sebezhetőségének feltérképezése történik,
b) automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei, vagy
c) a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik;

96. *továbbfejlesztés*: az érintett, már működő elektronikus információs rendszer olyan mértékű fejlesztése, amely funkcionalitásának érdemi megváltozásával jár, vagy védelmének elvárt erősségére hatással van;

97. *üzemeltetési kiberbiztonsági incidens*: olyan kiberbiztonsági incidens, amely az elektronikus információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált, vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását nem szándékoltan csökkenti vagy megszünteti;

98. *üzemeltető*: az a természetes személy, jogi személy, jogi személyiség nélküli szervezet vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

99. *zárt, teljes körű, folytonos és a kockázatokkal arányos védelem*: az elektronikus információs rendszer olyan védelme,
a) amely az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósul,
b) amely az elektronikus információs rendszer valamennyi elemére kiterjed,
c) amely az összes számításba vehető fenyegetést, veszélyt figyelembe veszi, valamint d) amelynek költségei arányosak a fenyegetések által okozható károk értékével.

Ezen túlmenően az IBSZ alkalmazásában:

3.1. Fenyegetések

A fenyegetések olyan események vagy mulasztások, amelyek hátrányos következményekkel járhatnak az ESZC számára, vagy amelyek veszteséget vagy kárt okozhatnak a szervezetnek. A fenyegetések eredményezhetik például a működés megszakadását, pénzügyi vagy reputációs veszteséget okozhatnak.

3.2. Kockázatok

A kockázat a fenyegetés bekövetkezésének és az ennek nyomán keletkező veszteségnek vagy kárnak a valószínűségét jelenti. Észszerű egyensúlynak kell lenni a biztonsági intézkedések költsége és azon keletkezhető kárértékek között, amelyeket ezekkel az intézkedésekkel lefedni szándékoznak. A rendszerek folyamatos működésének megszakadásából eredő veszteség, kár vagy a negatív publicitás például általában nem fejezhető ki számok vagy összegek segítségével, ezért a kockázatok becslésére különböző módszertanok léteznek.

Létfontosságú tehát, hogy a szervezet a kockázatokat rendszeres időközönként felbecsülje, kiértékelje, és kockázatcsökkentő intézkedéseket hozzon.

3.3. Védelmi intézkedések

A védelmi intézkedések vagy kontrollok a kockázatok elfogadható szintre történő csökkentését szolgálják.

A védelmi intézkedések az alábbiak szerint csoportosíthatók:

a) Céljuk szerint:

aa) a sértetlenség, megbízhatóság biztosítását célzó intézkedések,

ab) a rendelkezésre állás, folyamatosság biztosítását célzó intézkedések,

ac) a bizalmasság biztosítását célzó intézkedések.

b) Hatásuk szerint:

ba) **preventív (megelőző):** biztonsági incidensek megelőzését szolgáló intézkedések;

bb) **detektív (felderítő):** biztonsági incidensek azonosítását és a veszteség vagy kár korlátozását célzó intézkedések;

bc) **korrektív (helyesbítő):** veszteség vagy kár helyrehozását és az újbóli előfordulás megakadályozását célzó intézkedések.

c) Jellegük szerint:

ca) **adminisztratív:** intézkedések a szervezeten belül, pl. funkciók, irányelvek, folyamatok stb. szétválasztása, dokumentálás;

cb) **technikai:** fizikai biztonsági intézkedések, pl. zárak, számítógépek fizikai szétválasztása, helyek biztosítása, illetve egyéb számítógéprendszerekkel kikényszerített kontrollok;

cc) **képzési:** a foglalkoztatottak információbiztonsági képzése a szükséges információbiztonság-tudatossági szint eléréséhez

3.4 Biztonsági esemény

Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.

3.5 Biztonsági esemény kezelése

Az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység.

3.6 Távmunka

Távmunkavégzés a munkáltató telephelyétől elkülönült helyen rendszeresen folytatott olyan tevékenység, amelyet információtechnológiai vagy számítástechnikai eszközzel végeznek és eredményét elektronikusan továbbítják.

6. A szabályzat leírása

6.1 Jelen szabályzat alapelvei

Az információvédelem megvalósítása során, figyelembe véve az ESZC feladatait, az alábbi irányelveket kell érvényesíteni:

a) ***eredményesség:*** azon információk, amelyek a szervezeti folyamat szempontjából jelentőséggel bírnak, időben, helyesen, ellentmondásmentesen és használható módon rendelkezésre álljanak,

b) ***hatékonyság:*** a rendelkezésre álló információk és erőforrások leghatékonyabb és leggazdaságosabb felhasználása a szervezeti folyamatok kiszolgálása érdekében,

c) ***bizalmasság***: biztosítani kell az ESZC kezelésében és használatában lévő adatok és információk tekintetében a jogosulatlan hozzáférés és közzététel elleni védelmet mind a központi, mind pedig a helyi feldolgozások és az adat- és információcsere során,

d) ***sértetlenség:*** biztosítani kell az ESZC által kezelt adatok folyamatos pontosságát és teljességét mind a feldolgozás, mind pedig az adat- és információcsere-folyamatok során,

e) ***rendelkezésre állás***: biztosítani kell a külső és belső adatkérések során a jogosultak számára a szolgáltatásra vonatkozó előírások szerinti hozzáférhetőséget,

f) ***megfelelőség***: biztosítandó a szervezeti folyamat tárgyához kapcsolódó jogszabályokhoz, szabályozásokhoz, szerződéses megállapodásokhoz és belső irányelvekhez történő igazodás, amelyek meghatározzák a működést,

g) ***megbízhatóság***: megfelelő információk biztosítása a működtetés, pénzügyi megbízhatóság és az irányítási kötelezettségek teljesítése érdekében,

h) ***kockázat*-arányos védelem:** a védelmi intézkedéseknek arányban kell állniuk a kockázatokkal.

6.2 Az elvárt biztonsági szint

AZ ESZC elvárt biztonsági szintjének elérése és fenntartása érdekében az alábbiakról kell gondoskodni:

a) az információvédelem részletes követelményeinek rögzítése,

b) az információbiztonsággal kapcsolatos szervezeti kérdések, valamint a szervezeten belüli és kívüli adatkapcsolatok szabályozása,

c) az ESZC adat- és információs vagyonának védelmét szolgáló minősítési és biztonsági osztályba sorolási eljárás kialakítása, valamint annak ellenőrzési módja,

d) a személyekhez és szerepkörökhöz kapcsolódó biztonsági követelmények, az oktatási és képzési tervek, valamint a biztonsági események és meghibásodások esetén szükséges eljárások kialakítása,

e) az információvédelemhez kapcsolódóan az informatikai rendszerek fizikai és környezeti biztonságának kialakítása,

f) az alkalmazott üzemeltetési és kommunikációs eljárások információvédelmi követelményrendszerének meghatározása,

g) az informatikai eszközökhöz, adatokhoz és informatikai szolgáltatásokhoz történő hozzáférés szabályozásának kialakítása és alkalmazása,

h) az informatikai rendszerfejlesztési és változáskezelési eljárások létrehozása,

i) az informatikai infrastruktúra folyamatos működésének biztosítását szolgáló eljárások kialakítása,

j) az informatikai infrastruktúra, eljárások és szolgáltatások jogszabályi megfelelőségét biztosító szabályozás kialakítása.

6.3 Információbiztonsági politika

Az ESZC információbiztonsági politikájának elsődleges célja, hogy az ESZC céljaival és szervezeti stratégiájával összhangban meghatározza azon irányelveket, amelyek betartása hozzájárul az ESZC által kezelt adatok sértetlenségének, bizalmasságának, megfelelőségének, megbízhatóságának, eredményességének, hatékonyságának és rendelkezésre állásának biztosításához. Az ESZC az információbiztonságot alapvető fontosságúnak tartja, ezért információbiztonsági politikáját a következő elvekre építi:

aa) a hatályos jogszabályoknak és az irányító szerv (az ESZC) elvárásainak megfelelő biztonsági szabályozást alakít ki,

ab) a kockázatokkal arányos biztonsági előírásokat határoz meg, védelmet alakít ki,

ac) mindenki számára érthető és betartható információbiztonsági szabályokat alkalmaz,

ad) magas szintű biztonságtudatosságot tart fenn,

ae) ellenőrzött, szabályozott működést biztosít,

af) az információbiztonság védelme szempontjából a megelőzésre helyezi a hangsúlyt.

b) Az ESZC csak a még elfogadható kockázatokat vállalja fel. Ennek megfelelően kerüli azokat a helyzeteket, szituációkat, amelyek magas kockázatot jelentenek, és amelyek kockázata a várható előnyökkel szembeállítva aránytalanul nagy. Az ESZC információbiztonsági intézkedéseit a különböző forrásokból származó fenyegetettségeinek változásaihoz úgy igazítja, hogy a fennmaradó kockázatok a még felvállalható tartományban maradjanak.

c) Az ESZC az információbiztonság fenntartása érdekében rendszeres kockázatelemzéssel határozza meg és tartja nyilván a kockázatokat, fenyegetéseket.

d) Az ESZC az informatikai szolgáltatások védelme érdekében azok teljes életciklusa alatt gondoskodik

da) az informatikai erőforrások (alkalmazások, információk, infrastruktúra, eszközök, folyamatok, személyek) egyértelmű és visszakereshető azonosításáról,

db) az egyértelmű azonosítás, megbízható hitelesítés megvalósításáról,

dc) a szükséges és elégséges jogokról,

dd) a jogosultságok nyilvántartási rendszeréről,

de) a biztonsági naplózásról és annak ellenőrzéséről,

df) a biztonsági tanúsítvány, a jótállás, a szavatosság, a garancia és szerviz, a dokumentációk, a titoktartási nyilatkozatok és szabályozási feltételek, valamint

dg) a biztonságos adatcsere biztosításáról.

e) Az ESZC az informatikai szolgáltatásainak fejlesztéséhez és üzemeltetéséhez megbízható személyeket, illetve külső szolgáltatókat alkalmaz, akik a szükséges ismeretekkel és felkészültséggel rendelkeznek. Az ESZC törekszik megakadályozni, hogy az informatikai rendszerekhez, azok egyes elemeihez kapcsolódó ismeretek, feladatok vagy jogosultságok úgy koncentrálódjanak, illetve személyhez kötöttségük olyan szintet érjen el, amely az adott informatikai rendszer biztonságos fejlesztését, működését veszélyeztetheti.

f) Az ESZC kiemelt figyelmet fordít az informatikai rendszerek, valamint a tárolt adatok hozzáférési jogosultságainak biztosítására és visszavonására.

g) Az ESZC gondoskodik az üzletmenet-folytonosságról. Informatikai rendszereit elsődleges és tartalékkörnyezetben helyezi el és üzemelteti, a kritikus mentéseket, dokumentációkat pedig külső helyszínen is tárolja.

h) Az ESZC azonosítja védendő informatikai erőforrásait, ennek keretében az informatikai rendszereit az üzleti folyamatok támogatásának biztonsága, üzletmenet-folytonossági és katasztrófaelhárítási szempontból értékeli, biztonsági osztályokba sorolja. Meghatározza az egyes osztályokra és az informatikai rendszerekre vonatkozó fizikai, logikai, humán és adminisztratív biztonsági követelményeket, a rendelkezésre állás paramétereit, valamint azt a maximális kiesési időtartamot, amelyet az adott informatikai rendszer leállása nem haladhat meg. Ehhez bemeneti adatként a felső vezetés által meghatározott, folyamat vagy rendszer rendelkezésre állási követelményt veszi alapul.

i) Az ESZC kizárólag jogtiszta szoftvereket használ, tiltja az illegális szoftverek használatát.

Az ESZC megakadályozza a tulajdonában lévő szoftverek és hardverek illegális felhasználását.

j) Az ESZC a külső személyektől is elvárja a jogtiszta, malware-mentes környezet alkalmazását, és az ESZC teljesítésre vonatkozó belső szabályozási dokumentumaiban foglalt előírások betartását.

k) Az ESZC minden foglalkoztatottjától magas szintű információbiztonsági tudatosságot vár el, minden foglalkoztatott felelős az információs rendszerek, adatok biztonságáért. Az ESZC képzést biztosít minden felhasználó és külső személy számára az információbiztonság

tudatossági szintjének fejlesztéséhez, a rendszerek üzemeltetéséhez és a rendeltetésszerű használatukhoz szükséges biztonsági követelmények, ismeretek elsajátítása céljából.

l) Az ESZC az információbiztonság alapfeltételének tekinti az információbiztonsággal kapcsolatos elvárások, szabályok előírásainak betartását és kiemelt fontosságot tulajdonít az átfogó ellenőrzésnek.

m) Az ESZC valamennyi vezetője és foglalkoztatottja felelős a hatályos jogszabályok, valamint az ESZC információbiztonsági szabályainak betartásáért. Ezért az ESZC valamennyi foglalkoztatottja köteles az információbiztonsági elvárásokat érvényre juttatni, az azt veszélyeztető körülményeket jelezni, elhárításukban részt venni.

6.4 Az adatok biztonsági osztályba sorolási modellje

a) Az adatok biztonsági osztályba sorolási modellje tartalmazza az egyes biztonsági osztályokhoz megkövetelt alapvető védelmi intézkedéseket. A kapcsolódó védelmi intézkedések betarthatóvá tételéért és a betartás ellenőrzéséért az információbiztonsági felelős felel. Az adatvédelmi intézkedés betartásáért az adatkezelők a felelősek.

b) Az ESZC adatainak (és az azokat kezelő rendszereknek) biztonsági osztályba sorolását az **1. táblázat**ban feltüntetett, az – kiberbiztonságról szóló 2024. évi LXIX. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről szóló – 418/2024 (XII.23.) Korm. rendeletben meghatározott módon kell elvégezni bizalmasság, sértetlenség és rendelkezésre állás szempontjából.

c) A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén (például új rendszer bevezetésekor) soron kívül, dokumentált módon felül kell vizsgálni.

Az adatok osztályozásának célja, hogy az elektronikus információs rendszerben kezelt adatok bizalmasság, sértetlenség és rendelkezésre állás szempontjából értékelésre kerüljenek és azok biztonsági súlyának megfelelően kerüljön kialakításra a kockázatarányos védelem. Az adatosztályozás emellett hozzájárul az elektronikus információs rendszerben kezelt adatok külföldön vagy felhőben történő kezelésének egyértelmű meghatározásához. A szervezet a 2. és 3. pontban kötelezően megadott szempontokhoz képest további adatosztályozási szempontokat is figyelembe vehet, amelyeket az adatosztályozás kapcsán köteles dokumentálni.

6.5 Az adatok bizalmasság szerinti besorolása

6.5.1 B1 szintű adatok

Ezen adatok bizalmasságának sérülése vagy elvesztése nem, vagy csak elhanyagolható mértékű anyagi vagy reputációs veszteséget okozhat a szervezetnek.

6.5.2 B2 szintű adatok

Ezen adatok bizalmasságának sérülése vagy elvesztése csak kis mértékben okozhat anyagi vagy reputációs veszteséget a szervezetnek.

6.5.3 B3 szintű adatok

Ezen adatok bizalmasságának sérülése vagy elvesztése jelentős anyagi vagy reputációs veszteséget okozhat a szervezetnek.

6.5.4 B4 szintű adatok

Ezen adatok bizalmasságának sérülése vagy elvesztése kritikus mértékű anyagi vagy reputációs veszteséget okozhat a szervezetnek.

6.6 Az adatok sértetlenség és rendelkezésre állás szerinti értékelése

6.6.1 SR1: az adatok SÉRTETLENSÉGE ÉS RENDELKEZÉSRE ÁLLÁSA NEM KRITIKUS

Az elektronikus információs rendszeren tárolt és kezelt adatok sértetlenségének és rendelkezésre állásának sérülése vagy elvesztése a szervezetnek vagy más személynek nem, vagy nem jelentős mértékben okozhat anyagi vagy reputációs veszteséget.

6.6.2 SR2: az adatok SÉRTETLENSÉGE VAGY RENDELKEZÉSRE ÁLLÁSA KRITIKUS

Az elektronikus információs rendszeren tárolt és kezelt adatok sértetlenségének vagy rendelkezésre állásának sérülése vagy elvesztése a szervezetnek vagy más személynek jelentős, vagy kritikus mértékű anyagi vagy reputációs veszteséget okozhat.

6.7 Az adatosztályozás eredménye

6.7.1 Titkosítás

A B2 szintű adatok esetén: ha technológiai szempontból lehetséges, gondoskodni kell a titkosításról, amennyiben külföldi adatkezelés vagy nem privát felhőszolgáltatás igénybevétele valósul meg.

A B3–4 szintű adatok esetén: minden esetben gondoskodni kell a titkosításról, amennyiben külföldi adatkezelés vagy nem privát felhőszolgáltatás igénybevétele valósul meg.

6.7.2 Az adatkezelés helyszíne

6.7.2.1 SR2 besorolású adatok esetén

Ha jogszabály másként nem rendelkezik, az adatok kezelésére földrajzi korlátozással kerülhet sor. Az adatok csak EGT-tagállam területén tárolhatók. Külföldi adattárolás esetén egyidejűleg gondoskodni kell az adatnak Magyarország területén való rendelkezésre állásáról is.

6.7.2.2 Az előző alpontban foglaltakon túl

Az adatkezelés lehetséges helyszínének meghatározásához összeadandó az adat B és SR kategóriájának megnevezésében szereplő számértéke. Ha jogszabály másként nem rendelkezik, a kapott eredmény alapján az adatok az alábbi F1–F4 kategóriákba sorolhatók, melyekre a következő előírások alkalmazandók:

- F1: ha a B és SR összesített értéke: 2

  Az F1 besorolású adatok
  – földrajzi korlátozás nélkül,
  – nem privát felhőszolgáltatás igénybevétele esetén korlátozás nélkül
  kezelhetők és tárolhatók.

- F2: ha a B és SR összesített értéke: 3

  Az F2 besorolású adatok
  – SR1 besorolású adatok esetén földrajzi korlátozás nélkül, SR2 besorolású adatok esetén kizárólag EGT-tagállam területén,
  – nem privát felhőszolgáltatás igénybevétele esetén
  – EGT-tagállam területén kívül kizárólag az igénybe vett szolgáltatás vonatkozásában harmadik fél általi, a kiberbiztonsági hatóság honlapján közzétett lista szerinti kiberbiztonsági tanúsítással, audittal vagy engedélyezéssel rendelkező (a továbbiakban: harmadik fél által tanúsított) nem privát felhőben vagy
  – EGT-tagállam területén belül akár nem tanúsított nem privát felhőben is
  kezelhetők és tárolhatók.

- F3: ha a B és SR összesített értéke: 4

Az F3 besorolású adatok
– kizárólag EGT-tagállam területén belül
– nem privát felhőszolgáltatás igénybevétele esetén
– harmadik fél által tanúsított nem privát felhőben vagy
– nem tanúsított nem privát felhőszolgáltatás igénybevétele esetén kizárólag Magyarország területén
kezelhetők és tárolhatók.

- F4: ha a B és SR összesített értéke: 5 vagy 6

Az F4 besorolású adatok
– kizárólag Magyarország területén,
– felhőszolgáltatás igénybevétele esetén
– harmadik fél által tanúsított privát felhőben vagy
– kormányzati felhőben
kezelhetők.

6.7.3 Az adatosztályozás eredményének összesítése

	A	B	C
1		SR1	SR2
2	B1	F1	F2
3	B2	F2	F3
4	B3	F3	F4
5	B4	F4	F4

6.8 Információbiztonsági feladatkörök

Az alábbi szerepek esetében felsorolt felelősségek, hatáskörök és feladatok minden esetben a jelen szabályzat tárgykörében értendők.

6.8.1 IBF (elektronikus információs rendszer biztonságáért felelős személy)

Az IBF felügyeli informatikai biztonsági szempontból a teljes informatikai rendszert. Elkészíti és aktualizálja az informatikai szabályzatokat, felhasználói oktatásokat szervez, és elvégzi egy egyéb, IBF-hez jogszabály által rendelt feladatokat.

6.8.2 Vezető rendszergazda

A vezető rendszergazda felügyeli a rendszergazdák munkáját, összefogja azon feladatokat, amelyek nem oldhatóak meg helyi szinten (pl. beszerzések), biztosítja a munkavégzés feltételeit és a rendszergazdák munkavégzését ellenőrzi, a feladatokkal kapcsolatos írásos (intranetes ticketing rendszerben található) dokumentumok áttekintésével.

A vezető rendszergazda az informatikai rendszerekkel kapcsolatos intézkedéseit azok megküldésével egyidőben megküldi az IBF-nek. A ticketing rendszerhez az IBF-nek hozzáférése van, az ott található kommunikációt nem szükséges megküldeni. az utasítások az IBF jóváhagyását követően lépnek életbe.

6.8.3 Rendszergazda

A rendszergazdák üzemeltetik a felelősségi körükbe sorolt informatikai rendszert, figyelembe véve a jelen és egyéb informatikai jellegű szabályzatok előírásait.

A rendszergazdák egyes feladatainak elvégzését egyrészt a vezető rendszergazda, másrészt az iskola igazgatója felügyeli. Az igazgató a helyi, iskolai szintű feladatokat adja ki a rendszergazdának, amelyhez a jogosultságokat olyan szinten kell megkapniuk, hogy az az önálló feladatvégzést lehetővé tegye.

6.8.4 Felhasználó

Felelőssége: jelen szabályzat ismerete és betartása, a rá bízott eszközök állapotának megóvása, valamint a munkájuk során tudomásukra jutó információ bizalmasságának megőrzése.

Hatásköre: biztonsági problémák észlelésének jelentése.

Feladatai:

- bizalmasság megőrzése,
- jelen szabályzat betartása,
- információbiztonság-tudatos viselkedés munkavégzése során,
- részvétel az oktatásokon,
- íróasztalán és munkakörnyezetében rend tartása (clear desk policy) az információszivárgás megelőzése érdekében.

6.9 Titoktartási megállapodások

Az ESZC a külső partnerekkel kötött szerződéseibe, megállapodásaiba belefoglalja a szerződés, megállapodás által szabályozott folyamatban érintett adatok bizalmas kezeléséről szóló pontokat.

6.10 Logikai hozzáférés - kezelés szabályai

Jelen fejezet meghatározza az ESZC-nél használt informatikai szolgáltatások és alkalmazások jogosultságkezelésének módját a kiadott jogosultságok teljes életciklusára.

6.10.1 Jogosultság létrehozása

a) Jogosultság, új felhasználó létrehozását csak az illetékes szervezeti egység vezetője, diákok esetében az erre a feladatra kijelölt tanár, osztályfőnök vagy adminisztratív munkatárs kezdeményezheti az Intranet rendszeren erre a célra létrehozott jogosultságigénylő felületen (workflow). Ezen felület létrehozásáig biztosítani kell azonos tartalmú letölthető papíralapú adatlap letölthetőségét, amelyet kitöltve, aláírva, szkennelve kell a rendszerbe feltölteni.

b) A szervezeti egység vezetője vagy diákok esetén a feladatra kijelölt tanár, osztályfőnök vagy adminisztratív munkatárs csak a saját vagy az irányítása alatt álló szervezeti egység által használt jogosultságokat engedélyezheti.

c) A hozzáférésekkel kapcsolatos döntéseket az adatgazda (amennyiben van), ennek hiányában a szervezeti egység vezetője hozza meg, a technikai kivitelezést az adott iskola vagy központ rendszergazdája hajtja végre.

d) A végrehajtás tényét az Intraneten üzemelő workflow rendszerben az igényléshez kapcsolódva rögzíteni kell. papíralapú igénylés esetén az igénylőlapon kell rögzíteni a végrehajtás időpontját, a feladatot elvégző személy nevét, és az adatlapot szkennelve kell tárolni.

e) A jogosultság vagy új felhasználó iránti igények végrehajtását azt azt végrehajtó dokumentálja, a megadott jogosultságokat vagy jelszavakat egyéb módon nem dokumentálja.

6.10.2 A jogosultság létrehozásának alapelvei

Minden felhasználónak olyan szintű jogosultság engedélyezhető, ami éppen elégséges a munkája elvégzéséhez. A felhasználóhoz csoport szintű vagy egyedi jogosultság rendelhető hozzá.

6.10.3 4.7.3. Jelszóválasztással és használattal szemben támasztott követelmények

A hálózati szolgáltatásokhoz való hozzáférés és az alkalmazásokhoz kapcsolódó jelszóképzési rend a következő:

A jelszó lejárati ideje	90 nap
A jelszó lejárati ideje diákok esetében	Egy félév (tanrend szerinti félév)
A jelszó minimális hossza	10 karakter
Egyediség	10 ciklus
Fiókzárolás	5 sikertelen kísérlet után
Számláló nullázása	Sikeres belépésenként
Zárolási időtartam	Rendszergazda oldhatja fel
A jelszóváltoztatás előtt be kell jelentkezni	
A fenti szabályoktól el lehet térni 2 faktoros hitelesítés alkalmazása esetén, amelynek használatáról az IBF dönt	

A jelszó az információbiztonsági szempontból a legsérülékenyebb terület. Éppen ezért különösen figyelmesen kell eljárni jelszóválasztáskor. A jelszóválasztás legfontosabb alapelvei:

a) a jelszavakat bizalmasan, magántitokként kell kezelni;
b) a jelszót semmilyen módon se lehessen a tulajdonoshoz és családjához kötni (pl. autó rendszám, gyermek neve);
c) a jelszó (és bármilyen más hitelesítő adat vagy eszköz) nem osztható meg más munkatársakkal, diákokkal, illetve külső személyekkel. **Az erre vonatkozó kérés is információbiztonsági incidensnek minősül, amelyet a szabályzatban megjelölt módon kötelező jelenteni és kivizsgálni**;
d) más jelszavát tárolni, menteni tilos. Más jelszavának bármilyen formában történő tárolása **információbiztonsági incidensnek minősül, amelyet a szabályzatban megjelölt módon kötelező jelenteni és kivizsgálni**;
e) a számítógépes rendszereken tárolt jelszófájlokat megfelelő védelemmel kell ellátni, azaz megfelelő kriptográfiai eljárással rejtjelezni kell;
f) jelszavakat vagy jelszófájlokat a hálózaton nyílt, olvasható formában továbbítani tilos;
g) a felhasználónevet és jelszót a felhasználó részére külön csatornán kell eljuttatni;
h) törekedni kell a 2 faktoros autentikáció minél szélesebb körű alkalmazására, különösen a privilegizált felhasználók és külső partnerek/beszállítók esetében.

Mindenkinek tisztában kell lennie azzal, hogy az előírások be nem tartása növeli a harmadik személy által elkövetett, a hozzáférési jogosultságával történő esetleges visszaélés kockázatát. Az informatikai rendszer az így elkövetett adattörléseket, egyéb műveleteket úgy regisztrálja, hogy azt az a felhasználó követte el, akinek a hozzáférési jogosultságát igénybe vették, függetlenül attól, hogy ez a felhasználó beleegyezésével vagy tudtán kívül történt.

Abban az esetben, ha egy adott rendszeren AD (Active Directory) vagy egyéb, erre alkalmas rendszer működik, a 90 naponkénti jelszócserét automatikusan ki kell kényszeríteni, a jelszó lejártát követő 2 hetes türelmi idővel.

6.10.4 Jogosultság változása

Jogosultság változását a jogosultság létrehozásával azonos elvek szerint kell végezni.

6.10.5 Jogosultság megszüntetése

A távozó munkatársak és diákok jogosultságát a távozás napján meg kell szüntetni. A megszüntetési igényt a szervezeti vezetője, diákok esetén osztályfőnöke kezdeményezi az igényléssel megegyező felületen (Intranet, ennek hiányában nyomtatvány).

6.11 Munkaállomások és más informatikai eszközök használata

Az informatikai eszközök csak rendeltetésszerűen használhatók, munkavégzés és/vagy tanulási célokra. az informatikai eszközök magáncélú használata tilos.

A felhasználó az informatikai eszközökre szoftvereket nem tölthet le és nem installálhat.

A használat során tilos tudatosan kihasználni az esetleges előforduló szoftverhibákat, védelmi hiányosságokat

6.12 Elektronikus levelezés és internethasználat

A hálózati munkaállomások az internethez kizárólag az ESZC hivatalos internetkijáratán (központi határvédelmi rendszerén) keresztül csatlakozhatnak a világhálóhoz. Kivételt képezhetnek ez alól azon mobil munkaállomások és más mobil eszközök, amelyek mobilinternetet használhatnak. Mobilinternet használat során a felhasználó köteles gondoskodni arról, hogy eközben ne kapcsolódjon másik hálózati interfészen az ESZC hálózatához, mert így, amennyiben mindkét hálózati kapcsolat él, a támadók az ESZC hálózatába be tudnak hatolni a határvédelmi rendszer megkerülésével. A használat során tilos tudatosan kihasználni az esetleges előforduló szoftverhibákat, védelmi hiányosságokat.

Az elektronikus levelezésre vonatkozó szabályok:

- Az ESZC levelezőrendszerének rendeltetése a hivatali és oktatási feladatok ellátása, ezért a felhasználók magán vagy egyéb célra nem használhatják.
- Tilos a felhasználónak olyan tartalmat az ESZC informatikai rendszeréből kiküldeni, ami az ESZC érdekeivel ellentétes.
- A küldhető és fogadható levél maximális mérete 25 MB.
- Egy levélben a címzettek száma nem lehet több mint 150 e-mail cím.

Az ESZC az e-mailt használja a legfontosabb kommunikációs eszközként, ezért az egyes e-mail fiókokban megjelenhetnek – az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti – nem nyilvános adatok, egyéb bizalmas információk. Tehát a teljes e-mail adatbázist védendő adatállományként kell kezelni. Ezt a szempontot figyelembe kell venni a mentések tárolásának kialakításakor. Továbbá a felhasználóknak a tudomására kell hozni, hogy

nem nyilvános adatot, vagy bizalmas információt csak személyhez kötött e-mail címről küldjenek, vagy fogadjanak.

Az ESZC korlátozza a munkahelyen internetről letölthető tartalmakat, és széles körű védelmet (ideértve tartalomszűrést is) alkalmaz. Az internet csak munka vagy általános érdeklődés kielégítése céljából használható. Amennyiben a felhasználó nem megengedett tartalmat tölt le, a rendszergazda vagy az IBF felszólíthatja e tevékenység felhagyására.

Az ESZC informatikai rendszerében a felhasználóknak kerülni kell az ismeretlen eredetű fájlokkal történő műveleteket. Ennek megvalósítása érdekében az ESZC működése során kerülni kell az olyan eljárásokat, amelyek eredményeképpen mások számára félreértésre okot adó, ezáltal veszélyes, azonosíthatatlan eredetű és rendeltetésű fájl jön létre. Ezért:

- A felhasználóknak az elektronikus levelezés során ismeretlen forrásból származó gyanús csatolt állományokat megnyitnia tilos, és azonnal jeleznie kell az informatikának.
- Az internet használata közben a kiugró ablakokon felajánlott telepítéseket a kiugró ablak jobb felső sarkában található kilépés gombbal (vagy az ablak bezárását eredményező billentyűkombinációval, pl. Alt+F4) el kell utasítani. A felajánlott telepítés engedélyezése tilos.

6.13 Rendszerüzemeltetés

Az üzemeltetési, működtetési folyamatokban – a kockázatokkal arányosan – szét kell választani a felhasználó/igénylő/megrendelő, a szolgáltató/végrehajtó és az ellenőrző/felügyeleti funkciókat. A kötelességek és a felelősségek meghatározását a munkaköri leírásoknak kell tartalmaznia.

Az informatikai infrastruktúra üzemeltetésével foglalkozó dolgozók (rendszergazdák) saját munkájának megtervezése során tekintetbe veszi az ESZC működését, és az üzleti kritikus rendszereknél a karbantartási feladatokat az operatív működési időn kívülre teszi. A rendszerek eléréséhez szükséges adminisztrátori jelszavakat csak a kijelölt üzemeltetők ismerhetik, de biztonsági okokból e jelszavak borítékban elzárva megtalálhatóak az ESZC telephelyén is.

A szükséges javítócsomagok telepítése, illetve a telepítés előtti biztonsági mentés operációs rendszer és üzleti alkalmazás esetében az üzemeltetés feladata. E javító csomagok telepítése automatizáltan történik.

Az egyes szervezeti egységekhez tartozó gyökérkönyvtárakat az üzemeltetés hozza létre. E gyökérkönyvtárak tulajdonosa és alapértelmezett adatgazdája a szervezeti egység vezetője.

Az adminisztrátori jelszavak kiemelten védendő információnak minősülnek. Ezért csak kódoltan tárolhatók, vagy papíron rögzítve borítékban lezárva és páncélszekrényben tárolva.

Az egyedi fejlesztésű rendszereket a fejlesztés vagy build lezárultával külön szabályozásban meghatározott módon a fejlesztési vezetőnek át kell adnia az üzemeltetési vezető számára. Ez

garantálja, hogy az üzemeltetés a feladatait magas színvonalon tudja ellátni a rendszer tekintetében.

Az üzemeltetett rendszerek tekintetében gondoskodni kell arról, hogy rendelkezésre álljon külső vagy belső erőforrás formájában az üzemeltetéshez szükséges kompetencia és humán erőforrás.

Az üzemeltetett rendszerek tekintetében gondoskodni kell arról, hogy rendelkezésre álljon minden szükséges hardver- és szoftvererőforrás (pl.: tárhely, szerver, licenc stb.), amely szükséges a folyamatos, magas szolgáltatási színvonal fenntartásához.

Az üzemeltetett rendszereknél, amennyiben lehetséges, automatikus és folyamatos patchelést kell alkalmazni.

6.14 Informatikai üzletmenet folytonosság és katasztrófaelhárítás

Kiemelten fontos cél az informatikai üzletmenet-folytonosság biztosítása katasztrófa esetén is, mivel az üzleti folyamatok jelentősen függnek az IT támogatástól. A szabályozásélja, hogy katasztrófahelyzet esetén is felkészüljünk a visszaállításra, lehetőleg a legkisebb kieséssel.

Katasztrófának tekintjük azon hirtelen, nem tervezett eseményt, amely nagy kárt vagy veszteséget okoz. Üzleti szempontból katasztrófának tekintjük, ha a szervezet meghatározott időn túl nem képes kritikus üzleti funkcióit működtetni. A katasztrófa jellemzője továbbá, hogy normál problémakezeléssel nem megoldható, illetve a belső IT szervezet nem képes önerőből elhárítani rövid idő alatt.

Az informatikai üzletmenet-folytonossági tervezésnek illeszkednie kell a teljes szervezetre vonatkozó üzletmenet-folytonossági tervezésbe.

Az egyes rendszereket csoportokba kell sorolni a szerint, hogy mennyire kritikusak a szervezet működésének szempontjából. Ezek a csoportok egyben prioritást is felállítanak a szolgáltatások helyreállításának menetében. A csoportosítás elsődlegesen a felhasználók által használt szolgáltatásokra vonatkozik, nem az ennek működéséhez szükséges háttér- infrastruktúrára.

Katasztrófahelyzetben a helyreállítást az IBF irányítja, aki jogosult az előző pontban ismertetett általános prioritási lista felülbírálatára.

Katasztrófahelyzetben az Informatikai vezető engedélyével lehetőség van külső erőforrások bevonására, a gazdasági főigazgató-helyettes haladéktalan tájékoztatása mellett.

Az üzletmenet folytonossága számos komponensből épül fel (biztonsági mentés, dokumentáció, szabályozottság stb.), amelyet az egyes fejezeteknél tárgyalunk.

6.15 Biztonsági események kezelése

Biztonsági eseményt minden esetben dokumentált formában ki kell vizsgálni, és ennek megállapításai alapján, amennyiben szükséges, védelmi intézkedéseket tenni.

Amennyiben a biztonsági esemény előidézője vagy aktív résztvevője az ESZC-vel foglalkoztatásra irányuló vagy egyéb jogviszonyban álló személy vagy cég, a felelősség vagy a nem szerződésszerű teljesítés megállapítása érdekében vizsgálatot kell lefolytatni az adott munkavégzésre irányuló jogviszonyt szabályozó normák rendelkezései alapján.

6.16 Változáskezelés

Új rendszer vagy a meglévő rendszereket érintő bármilyen módosítás csakis ellenőrzött módon vezethető be. Elsődleges fontosságú, hogy minden érintett félnek jóvá kell hagynia a változásokat azok bevezetése előtt.

Új rendszereket vagy a meglévő rendszereket érintő változásokat formális átvételi eljárások végrehajtása után lehet üzembe helyezni. Az üzembe helyeztetést az üzemeltetés végzi. Ezeknek biztosítania kell az alábbiakat:

- Az IBF az implementálást, amennyiben a változás a felhasználók számára is érzékelhető változással jár. Az IBF jóváhagyásnak vissza kell tükröznie egy általa vagy számára végrehatott átvételi teszt eredményeit. A tesztnek egyebek között igazolnia kell, hogy a biztonsági intézkedések a felhasználó szempontjából hatásosan működnek.
- A rendszer megfelelően kezelhető és szervezhető (a leendő felhasználó képviselője és az üzemeltetés/rendszergazdák véleménye alapján), elfogadható mértékű biztonsági kockázatot jelent más rendszerek számára (az információbiztonsági felelős véleménye alapján).
- A rendszer üzemeltetésre való átadása során a kijelölt üzemeltetők számára – az üzemeltetési és felhasználói dokumentációval együtt – át kell adni a rendszer biztonsági dokumentációját. Az üzemelő rendszer konfigurációjáról, a működő rendszerek verzióiról nyilvántartást vezet az információbiztonsági felelős. Továbbá megőrzi a változásról, a jóváhagyásokról és tesztekről készült feljegyzéseket.

6.17 Monitorozás és naplózás

Az üzemeltetés a teljes informatikai rendszer működést monitorozza. A monitorozás lehetőséget teremt arra, hogy az üzemeltetés már akkor beavatkozhasson, amikor felhasználói hibabejelentés még nem történt meg. Az alkalmazott monitorozó eszközt az üzembiztonság fokozása érdekében folyamatosan továbbfejlesztjük.

Az informatikai üzemeltetés (rendszergazdák) kialakítja a központi naplózást és archiválást. Ezen archívum célja, hogy bizonyíthatóvá váljanak a később felfedezett biztonsági szabályszegések, valamint valós idejű detekciós lehetőségeket biztosít.

6.18 Biztonsági alrendszerek

6.18.1 Biztonsági események észlelése és kezelése

A felhasználók felelőssége az alábbiak jelentése az információbiztonsági felelősnek (IBF):

- felismert vagy felismerni vélt biztonsági esemény,
- felismert vagy felismerni vélt védelmi gyengeség, biztonsági rés, sérülékenység, ac) információbiztonsági szempontból nem megfelelő magtartás tapasztalása,
- bármilyen bizalmas információ kiszivárgása.

Az információbiztonsági felelős felelőssége az esetet a megfelelő hatóságoknak jelenteni, amennyiben azt jogi előírások megkívánják, továbbá a tudomására jutott biztonsági események kivizsgálását haladéktalanul meg kell kezdenie. A kivizsgálás kapcsán vizsgálni kell:

- a biztonsági esemény bekövetkezésének okát,
- az esemény személyi felelősségét,
- az okozott kár mértékét.

Az összegyűjtött bizonyítékokat az információbiztonsági felelős írásba foglalja, amelyben pontosan felsorolásra kerülnek az összegyűjtött bizonyítékok és azok biztonsági eseménnyel kapcsolatos tartalmi pontjai. Az elkészült dokumentumot fel kell használni hasonló biztonsági események megelőzésére, valamint a biztonsági dokumentációs rendszer felülvizsgálatakor.

6.18.2 Malware- és tartalomszűrés, végpontvédelem

Az ESZC gateway szintű malware-védelmet, spam- és tartalomszűrést használ.

Az a felhasználó, aki az adatait és adathordozóit a malware-ellenőrzés vagy malware-védelmi intézkedés (vírusirtás) alól bármilyen indokból kivonja, az abból eredő károkért teljes felelősséggel tartozik. Az üzemeltetésnek figyelemmel kell kísérnie a legfrissebb malwarek megjelenésével kapcsolatos híreket, amelyek alapján tájékoztatásokat küldhet a felhasználóknak.

Az üzemeltetés feladata, hogy a munkaállomásokra telepített malware-védelmi rendszereket karbantartása, a felhasználóknak támogatást nyújtson, továbbá a definíciós állományok és a keresőmotorok szükséges frissítéseiről gondoskodjon. A definíciós állományok legalább napi rendszerességgel központilag kerülnek frissítésre.

Az ESZC rendszerében komplex végpontvédelmet alkalmaz. Ez kiterjed többek között:

- malware-védelemre
- az informatikai eszközökhöz csatlakoztatható eszközök kontrolljára,
- adattitkosításra, és
- a futtatható programok kontrolljára.

6.19 Oktatás, képzés, és a biztonsági tudatosság fokozása

Az információbiztonsági felelősnek az információbiztonság-tudatossága érdekében oktatásokat, képzéseket köteles szervezni a következő témakörökben:aa) általános információbiztonsági oktatás (az információbiztonsági rendszer elemeinek bemutatása) minden új és hasonló oktatáson eddig részt nem vett felhasználó részére,

- új, bevezetésre kerülő rendszerekkel kapcsolatos biztonsági oktatás minden, a rendszer bevezetésében érintett felhasználónak,
- rendszeres, az információbiztonsági tudatosság fenntartását biztosító oktatás.

Az információbiztonsági tudatosság fenntartását biztosító oktatás az információbiztonsági felelős feladata. Az oktatások végrehajtásához külső fél igénybe vehető. Az oktatásoknak a saját munkatársakon felül ki kell terjednie a szerződés keretében dolgozó munkatársakra is. Az információvédelmi képzések kiterjednek

- a biztonsági követelményekre,
- a szükséges szakmai, informatikai, technológiai, jogi ismeretekre,
- a védelemmel kapcsolatos feladatokra,
- a munkatársak szerepére, fontosságára, be) a be nem tartás következményeire,
- a szabályozásokra.

Az információbiztonsági felelősnek az alábbi esetekben kell gondoskodnia az információvédelmi ismeretek oktatásáról az érintett kör részére:

- új dolgozó belépése,
- jelentősebb változásokat követően,
- az információvédelmi feladatok és felelősségek változása (pl. új szolgáltatás, információs rendszer, szervezet, működés változása),
- információvédelmi fenyegetettség változása vagy incidens bekövetkezése esetén, valamint
- minden esetben, ha azt az informatikai vezető kezdeményezi.

Külső képzésekről a javaslat alapján az információ biztonsági felelős felettese dönt.

Az információbiztonsági felelős a képzésről jegyzőkönyvet készít, külső képzés esetén a kapott igazolás, bizonyítvány másolatát összegyűjti. A feljegyzéseket a képzés tartalmának érvényességének lejárta után megőrzi.

6.20 Fizikai biztonság

Az ESZC székhelyén/telephelyein beléptető rendszert alakított ki. Az épületbe bejutás élőerős biztonsági személyzet vagy beléptetőrendszer felügyelete mellett lehetséges, azaz illetéktelen személyeknek belopódzásra nincsen lehetőségük. Az ESZC valamennyi foglalkoztatottja és tanulója, rendelkezik belépőkártyával, amelynek segítségével mozogni tud az ESZC épületeiben. A kártya

elvesztését azonnal jelenteni kell a kártya kiadásáért felelős vezetőnek, aki gondoskodik annak pótlásáról, valamint az elveszett kártya letiltásról.

Az elkerített irodaterületen belül szigorúbb biztonsági zóna a szerverek üzemeltetésére szolgáló helységek, ahova csak a megbízott üzemeltető vagy az információbiztonsági felelős engedélyével, illetve jelenlétében lehet belépni.

Az adatátvitelt bonyolító és az információs szolgáltatásokat támogató elektromos és távközlési kábeleket kábelcsatornával kell védeni a károsodástól, véletlen elszakítástól és szabotázstól. Az elhelyezésből és a tevékenység jellegéből fakadóan a kockázatok mértéke nem indokolja speciális árnyékolású kábelezés általános alkalmazását. A kábelhálózat karbantartása az üzemeltető feladata

7. Kapcsolódó külső és belső szabályozó dokumentumok

7.1 Külső szabályozó dokumentumok

2024. évi LXIX. törvény Magyarország kiberbiztonságáról

7.2 Belső szabályozó dokumentumok