CEGLÉDI SZAKKÉPZÉSI CENTRUM
2700 CEGLÉD, Malom tér 3.
Telefon: +36/53/789-934, +36/53/789-935
e-mail: ceglediszc@ceglediszc.hu, web: www.ceglediszc.hu
OM azonosító: 203068

Nyilvántartási szám: NSZFH/609/000145-1/2019

Ceglédi Szakképzési Centrum

Informatikai Biztonsági Szabályzat

Jóváhagyta:	Dr. Ferenczi Norbert
Készítette:	Szabadi Zoltán
Készült:	2019. március 1.
Hatályos:	2019. március 1.
Érvényes:	visszavonásig

I. ÁLTALÁNOS RENDELKEZÉSEK

1. A Szabályzat célja

1.1. Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja a Ceglédi Szakképzési Centrum (a továbbiakban: CSZC) által használt informatikai rendszerek/alkalmazások, továbbá az informatikai rendszerek/ alkalmazások által kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, ennek érdekében az informatikai rendszerekkel/alkalmazásokkal összefüggő tevékenységekre vonatkozó szervezeti, személyi, fizikai, informatikai és adminisztratív biztonsági követelmények meghatározása, illetve ezen követelmények teljesítésével összefüggő felelősségi előírások rögzítése.
1.2. Az IBSZ általános célja, hogy a CSZC által használt informatikai rendszerek/alkalmazások biztonságát garantáló eljárásokat és előírásokat átlátható és nyomon követhető formában egységes keretbe foglalva rögzítse az informatikai biztonság magasabb fokú kialakításának további szabályozása érdekében, továbbá dokumentumai, komplex, átfogó és széles körű informatikai biztonságot alkossanak.
1.3. Az IBSZ kiadásának célja továbbá a CSZC által használt informatikai rendszerek alkalmazásának biztonsági szempontból történő szabályozása.

2. Az IBSZ hatálya

2.1. Az IBSZ-ben meghatározott előírás, feladat, magatartási szabály – munkakörre való tekintet nélkül – kötelező érvényű, és hatálya kiterjed:

a) a CSZC szervezeti egységeinek (a továbbiakban: tagintézmények) foglalkoztatottjaira (továbbiakban: belső felhasználók);

b) a 2.1. a) pont alá nem tartozó, a CSZC-al egyéb jogviszonyban álló személyek (továbbiakban: külső felhasználók), akik feladataik teljesítése során vagy egyéb céllal, jogosultsággal, vagy annak hiányában felhatalmazással, az IBSZ tárgyi hatálya alá tartozó eszközöket, szoftvereket, informatikai rendszereket használnak, adatokat vagy dokumentumokat, információkat hoznak létre, tárolnak, használnak vagy továbbítanak, valamint azokra, akik ilyen tevékenységekkel kapcsolatosan döntéseket hoznak;

az a)–b) pont alattiak a továbbiakban együtt: a felhasználók.

2.2. A felhasználókkal kötendő valamennyi jogviszony vonatkozásában biztosítani kell az IBSZ rendelkezéseinek érvényesülését.
2.3. Az IBSZ rendelkezéseit alkalmazni kell a külső munkavégzéshez használt eszközökre is, amennyiben azok az IBSZ tárgyi hatálya alá tartoznak.
2.4. Az IBSZ-t alkalmazni kell a CSZC informatikai rendszereire, alkalmazásaira és azok moduljaira (a továbbiakban együtt: rendszer), az informatikai rendszerekhez csatlakoztatható informatikai, irodatechnikai, multimédiás eszközökre és adathordozókra, az informatikai rendszerekben kezelt, feldolgozott, tárolt adatokra, valamint az előzőekben felsoroltakkal kapcsolatos informatikai és biztonsági tevékenységre.
2.5. Az IBSZ tárgyi hatálya kiterjed:

a) a CSZC adatait feldolgozó, tároló vagy továbbító információhordozó eszközre, informatikai eszközökre és berendezésekre (ezek különösen: számítógépek, mobil eszközök, laptopok, IP telefonok, táblagépek, „okos” telefonok, nyomtatók, külső adattároló eszközök, aktív hálózati elemek, elektronikus adathordozók),

b) az a) pontban meghatározott eszközökre vonatkozó minden dokumentációra (ezek különösen: fejlesztési, szervezési, programozási, üzemeltetési dokumentumok), függetlenül azok formátumától (papír vagy elektronikus),

c) az 2.1. pontban meghatározott felhasználók által bármely okból használt információhordozó eszközökre és berendezésekre, amennyiben azok a CSZC informatikai környezetével kapcsolatot létesítenek,
d) az a) pontban felsorolt informatikai eszközökön használt vagy tárolt szoftverekre és adatokra (ezek különösen: rendszerprogramok, alkalmazások, adatbázisok), ideértve az üzemelő rendszerek adatain kívül az oktatási, teszt és egyéb célra használt adatokat is,
e) a CSZC által kezelt eszközökön tárolt adatok teljes körére, felmerülésüktől, feldolgozási és tárolási helyüktől függetlenül.

3. A Szabályzat jogi háttere és kapcsolódó belső irányítási eszközök

3.1. Az IBSZ jogi alapját az alábbi jogszabályok, közjogi szervezetszabályozó eszközök és belső irányítási eszközök
képezik:

a) 2013. évi L. törvény (a továbbiakban: Ibtv.) az állami és önkormányzati szervek elektronikus információbiztonságáról,
b) 233/2013. (VI. 30.) Korm. rendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről,
c) 301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról,
d) 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról,
e) 73/2013. (XII. 4.) NFM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről,
f) 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről,
g) a CSZC Szervezeti és Működési Szabályzata,

3.2. Az informatikai biztonságra vonatkozó CSZC rendelkezések elkészítése és előkészítése során az MSZ ISO/IEC 27000 szabványcsaládra kell figyelemmel lenni (lásd: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:v1:en).

4. Értelmező rendelkezések

4.1. Az IBSZ-ben alkalmazott, az IBSZ értelmezését, továbbá az informatikai biztonság tárgykörét érintő informatikai fogalmak az Ibtv. figyelembe vételével:

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

Adatállomány: egy nyilvántartásban kezelt adatok összessége.

Adatátvitel: elektronikus adatok informatikai rendszerek közötti továbbítása, amely lehet párbeszédre épülő (online) vagy nem párbeszédre épülő (offline) elektronikus kapcsolat.

Adatbázis: azonos minőségű (jellemzőjű), többnyire strukturált adatok összessége, amelyet a tárolására, lekérdezésére és szerkesztésére alkalmas szoftvereszköz kezel.

Adatfeldolgozás: az adatkezeléshez kapcsolódó technikai feladatok elvégzése.

Adatgazda: az a vezető, aki egy meghatározott adatcsoport tekintetében az adatok fogadásában, tárolásában, feldolgozásában, vagy továbbításában érintett szervezeti egységet képviseli és az adott adatcsoport felhasználásának kérdéseiben (például felhasználói jogosultságok engedélyezésében vagy megvonásában) elsődleges döntési jogkörrel rendelkezik.

Adathordozó: az elektronikus adatkezelő rendszerhez csatlakoztatható vagy abba beépített olyan eszköz, amelynek segítségével az elektronikus adatok tárolása, terjesztése megvalósítható. Pl. CD, DAT, DVD, floppy, merevlemez, USB-memória, cloud (felhő).

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása.

Adminisztratív biztonsági követelmények: az informatikai rendszer használata, üzemeltetése vagy fejlesztése során az adatok és a munkafolyamatok nyilvántartását, nyomon követhetőségét, továbbá az ezzel kapcsolatos feladatok ellátásának ellenőrzését lehetővé tevő segédletek és eljárásrendek meglétére, alkalmazására vonatkozó elvárások. Pl. naplók, nyilvántartások vezetése, ellenőrzése, ennek rendje.

Archiválás: a ritkán használt, meghaladottá vált, de nem selejtezhető adatok, adatbázisrészek változatlan tartalmi formában történő hosszú távú megőrzése.

Autentikáció (azonosítás): informatikai eljárás, amelynek során a felhasználó az informatikai rendszerben az autorizáció megszerzése érdekében igazolja személyazonosságát. Lehet tudás alapú (pl. jelszavas), birtoklás alapú (pl. tokenes) vagy tulajdonság alapú (pl. biometrikus), illetve ezek kombinációi.

Autorizáció (feljogosítás): azonosításra épülő informatikai eljárás, amelynek eredményeként egyértelműen azonosított személy (eszköz) a feladatai ellátásához meghatározott hozzáférési, eljárási vagy egyéb jogosultságokat kap.

Belső felhasználó: a CSZC központi szerve és a CSZC tagintézményei valamennyi foglalkoztatottja.

Belső hálózat (intranet): a CSZC saját, védett hálózata, mely belső telefonkönyvet szolgáltat, emellett, az itt található menükből strukturáltan, kereshető formában teszi elérhetővé a CSZC feladataival összefüggő adatbázisokat, CSZC belső utasításokat és nyomtatványokat.

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.

Biztonság: egy adott infrastruktúra, infrastruktúra elem, vagy elemek olyan – az érintett számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Részei a fizikai, környezeti, személyi, szervezeti, valamint az információbiztonság, az infokommunikációs infrastruktúrákban kezelt elektronikus adatok és információk biztonsága

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.

Biztonsági intézkedések: illetéktelen személyek információs infrastruktúrához, vagy információkhoz való szándékos, vagy véletlen fizikai hozzáférése elleni eszközök használatát szabályozó, valamint az illetékes személyek jogosulatlan tevékenységével szemben fellépő előírások, tervek és útmutatások összessége.

Biztonsági kockázat: az informatikai rendszerrel szembeni fenyegetés, amely a rendszer rendeltetésszerű működését és/vagy a rendszerben kezelt adatok bizalmasságát, rendelkezésre állását, sértetlenségét veszélyezteti vagy veszélyeztetheti.

Biztonsági követelmények: a kockázatelemzés eredményeként megállapított, elfogadhatatlan mértékű veszély mérséklésére, vagy megszüntetésére irányuló szükségletek együttese.

Biztonsági megfelelőség: az informatikai rendszer mennyiben, milyen mértékben felel meg az informatikai biztonsági követelményeknek.

Biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége.

Biztonsági szint: a szervezet felkészültsége az Ibtv.-ben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

Demilitarizált zóna (továbbiakban: DMZ): összekapcsolt hálózatok megbízhatatlan külső és megbízható belső részei között elhelyezkedő terület. A DMZ a benne elhelyezkedő hálózati eszközökhöz mind a megbízható belső, mind pedig a megbízhatatlan külső területről szabályozott mértékben engedélyezi a hozzáférést, de megakadályozza, hogy a külső területről bármilyen hozzáférési kísérlet eljusson a belső hálózatra.

Elektronikus információs rendszer: az adatok, információk kezelésére használt eszközök, eljárások, valamint az ezeket kezelő személyek együttese, továbbá az azonos adatkezelő és adatfeldolgozó által, egymással kapcsolatban álló eszközökön, egymással összefüggő eljárásokkal azonos célból kezelt, kiszolgált, illetve felhasznált adatok, az ezek kezelésére használt eszközök, eljárások, valamint az ezeket kezelő, kiszolgáló és felhasználó személyek együttese.

Értékelés: az infokommunikációs rendszerekkel kapcsolatos biztonsági intézkedések, eljárásrendek, Magyarországon elfogadott technológiai értékelési szabványok, követelményrendszerek és ajánlások, illetve jogszabályok szerinti megfelelőségi vizsgálata.

Fejlesztői rendszer: olyan informatikai rendszer vagy alkalmazás, amelynek felhasználói informatikusok. Célja felhasználói programok vagy alkalmazások kifejlesztésének támogatása.

Felhasználók: a 2.1. pontban meghatározott személyek.

Fizikai biztonság: illetéktelen személyek információs infrastruktúrához, vagy információkhoz való szándékos, vagy véletlen fizikai hozzáférése elleni intézkedések összessége, valamint az illetéktelen személyek, vagy illetékes személyek jogosulatlan tevékenységével szemben az adott struktúrák ellenálló képességét növelő tervek és útmutatások összessége.

Folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.
Funkcionális rendszer: a CSZC működését támogató informatikai rendszer vagy alkalmazás.
Hardver: az informatikai rendszer vagy számítógép fizikai elemei
Hálózat: számítógépek és hozzájuk kapcsolódó eszközök meghatározott szabályok szerinti összekapcsolása, amely adat- és információcserét tesz lehetővé.
Helyreállítás: valamilyen behatás következtében megsérült, eredeti funkcióját ellátni képtelen, vagy ellátni csak részben képes infrastruktúra-elem eredeti állapotának és működőképességének biztosítása, eredeti helyen.
Hitelesítés: a rendszerbe kerülő, ott lévő és onnan kikerülő adatok forrásának (az adat közlőjének), megbízható azonosítása.
Hitelesség: annak biztosítása, hogy a rendszerbe kerülő adatok és információk eredetiek, a megadott forrásból az abban tárolttal azonos, változatlan tartalommal származnak.
Hozzáférés: az infokommunikációs rendszer, vagy rendszerelem használója számára a rendszer szolgáltatásainak, vagy a szolgáltatások egy részének ellenőrzött és szabályozott biztosítása.
Illetéktelen személy: olyan személy, aki az adathoz, információhoz, az informatikai infrastruktúrához való hozzáférésre nem jogosult.
Infokommunikáció: az informatika és a telekommunikáció, mint konvergáló területek együttes neve.
Informatikai alkalmazás: számítógépen, illetve egyéb informatikai eszközön futó program.
Informatikai biztonság: az informatikai rendszer olyan állapota, amikor a rendszer rendeltetésszerűen működik és a rendszerben kezelt adatok bizalmassága, rendelkezésre állása, sértetlensége biztosított.
Informatikai biztonsági incidens: az informatikai rendszerrel szemben olyan külső, vagy belső előre tervezett, szándékos károkozású, vagy nem szándékos cselekmény, melynek célja a CSZC kezelésében lévő adatok, dokumentumok és egyéb információk jogosulatlan megismerése, megszerzése, módosítása valamint további károkozással kapcsolatos felhasználása.
Informatikai biztonsági követelmények: az informatikai rendszer használatával, üzemeltetésével és fejlesztésével kapcsolatos elvárások. Részterületei: a számítógépes biztonság, a kommunikációs biztonság, a kisugárzás biztonság és a rejtjelbiztonság.
Informatikai biztonsági politika: a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása meghatározott biztonsági feladatok irányítására és támogatására.
Informatikai biztonsági stratégia: az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere.
Informatikai infrastruktúra: a CSZC-hez kapcsolódó feladatokat ellátó, illetve a CSZC működését biztosító hálózatba kapcsolt hardverelemek, az azokon futó szoftverek és a rajtuk megtalálható adatok együttese, amely jól körülhatárolható, önmagában is működőképes, önálló szolgáltatás nyújtására képes infrastruktúra elemekből áll.
Informatikai rendszer: a számítógépek és a hozzájuk kapcsolódó eszközök (hálózat), a számítógépeken futó programok, valamint a számítógépeken kezelt, feldolgozott adatok együttese.
Informatikai vészhelyzet: a CSZC információs infrastruktúrájának leállása, szolgáltatások megszakadása, elérhetetlensége, a CSZC nemzeti információs vagyonának jelentős mértékű sérülése, illetve az ezekkel fenyegető rendellenes működés.

Információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.
Információbiztonság: az adatok és információk szándékosan, vagy gondatlanul történő jogosulatlan gyűjtése, károsítása, közlése, manipulálása, módosítása, elvesztése, felhasználása, illetve természeti vagy technológiai katasztrófák elleni védelmének koncepciói, technikái, technikai, illetve adminisztratív intézkedései. Az információbiztonság része az informatikai biztonság is, melynek alapelvei a bizalmasság, sértetlenség, rendelkezésre állás.
Információvédelem: szervezeti, személyi, fizikai, informatikai és adminisztratív előírások kidolgozása és intézkedések végrehajtása az információbiztonság érdekében.
Jogosultság: az arra felhatalmazott által adott hozzáférési lehetőség valamely információs infrastruktúrához.
Kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.
Kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.
Kockázattal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.
Következmény: valamely esemény, baleset, beavatkozás, vagy támadás hatása, amely tükrözi a belőle eredő veszteséget, valamint a hatás jellegét, szintjét és időtartamát.
Külső felhasználó: a CSZC-vel szerződéses jogviszonyban álló magánszemélyek, jogi személyek és jogi személyiséggel nem rendelkező egyéb szervezetek és ezek alkalmazottai.
Mentés (biztonsági mentés): biztonsági másolat készítése az informatikai rendszerben tárolt adatokról, adatállományokról, illetve az informatikai rendszerben használt alkalmazásokról. A másolat célja az elsődleges adattároló megsérülése esetén az adatok helyreállíthatóságának biztosítása.
Mobil eszköz: asztali munkaállomásnak nem minősülő egyes informatikai és kommunikációs feladatok ellátására használható, operációs rendszerrel, kommunikációs szolgáltatásokkal rendelkező, hordozható elektronikus eszköz. Ide tartoznak: laptopok, notebookok, táblagépek, mobiltelefonok és okostelefonok.
Munkaállomás: a felhasználó számára biztosított számítógép; lehet asztali vagy hordozható (laptop, notebook).
Napló: az informatikai rendszerben bekövetkező eseményeket, felhasználói tevékenységeket és ezek időpontját rögzítő, a rendszer által automatikusan kezelt adatállomány, amely a változások észlelését és a számon kérhetőséget biztosítja.
Naplózás: az informatikai rendszerben bekövetkező események, felhasználói tevékenységek és ezek időpontjának automatikus rögzítése a változások észlelése és a számon kérhetőség biztosítása érdekében.
Osztályozás: adatok, információk, információs infrastruktúra elemek, információs infrastruktúrák biztonsági szempontból való osztályainak kialakítása és ez alapján osztályokba sorolása.
Program: számítógépes nyelven megírt utasítássorozat. Állhat egyetlen programmodulból vagy programmodulok halmazából.

Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.
Rendszerelem: információs infrastruktúra elem.
Sebezhetőség: olyan fizikai tulajdonság, vagy működési jellemző, amely az adott információs infrastrukturális elemet egy adott veszéllyel szemben érzékennyé vagy kihasználhatóvá teszi.
Személyi biztonság: az adott rendszerrel/erőforrással kapcsolatba kerülő személyekre vonatkozó, alapvetően a hozzáférést, annak lehetőségeit és módjait szabályozó biztonsági szabályok és intézkedések összessége a kapcsolat felvétel tervezésétől, annak kivitelezésén keresztül a kapcsolat befejezéséig, valamint a kapcsolat folyamán a személy birtokába került információk vonatkozásában.
Szervezeti biztonság: egy adott szervezet strukturális felépítéséből adódó biztonsága és bevezetett biztonsági szabályainak és intézkedéseinek összessége a védendő rendszerhez/erőforráshoz való hozzáférés védelme érdekében.
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 (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.
Szoftver: a számítógép, az informatikai rendszer logikai elemei; a működtető programok (rendszerprogramok, operációs rendszerek) és a felhasználói programok (alkalmazások) összefoglaló neve.
Teljes körű védelem: azon bármilyen típusú aktív, vagy passzív védelmi intézkedések, melyek a rendszer összes elemére kiterjednek.
Tesztrendszer: olyan informatikai rendszer (környezet), amelynek célja a fejlesztés vagy bevezetés alatt álló program kipróbálásának, oktatásának támogatása.
Titkosítás: az informatikai rendszerben kezelt adatok bizalmasságának biztosítására szolgáló, nem a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet hatálya alá tartozó olyan tevékenység vagy eljárás, amelynek során az adatot úgy alakítják át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon, de a megismerésre jogosultak számára az adat az eredeti formájába visszaállítható legyen.
Veszély (fenyegetés): természeti vagy mesterséges esemény, személy, szervezet vagy tevékenység, amely potenciálisan káros a jelen szabályzatban védett tárgyakra.
Védelem: a biztonság megteremtésére fenntartására, fejlesztésére tett intézkedések, amelyek lehetnek elhárító, megelőző, ellenálló képességet fokozó tevékenységek, vagy támadás, veszély, fenyegetés által bekövetkező kár kockázatának csökkentésére tett intézkedések.
Visszaállítás: az eredeti infokommunikációs rendszer kiesése esetén a szolgáltatások további biztosítása, korábbi mentésből való visszaállítása.
Zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

II. AZ INFORMÁCIÓBIZTONSÁG SZERVEZETI STRUKTÚRÁJA, FELELŐSSÉGI KÖRÖK

5. CSZC kancellár feladatai

5.1. Felügyeli az informatikai biztonsági feladatok ellátását, felelős azok betartásáért.
5.2. Felelős a CSZC informatikai tevékenységének jogszerűségéért, beleértve az informatikai biztonsági tevékenységet is.
5.3. Kivizsgáltatja az ellenőrzések során feltárt hiányosságokat, gondoskodik a jogszabálysértő körülmények megszüntetéséről.

6. Felhasználók

6.1. Általános felhasználók a CSZC foglalkoztatottjai (ideértve a gyakornokokat is).
6.2. A kiemelt felhasználók rendelkeznek az általános felhasználókhoz kapcsolódó jogokkal, valamint azon túlmenően a feladatkörüktől és a szakmai területtől függő további egyedi jogosultságokkal is. A kiemelt felhasználókat – az elektronikus információs rendszer biztonságáért felelős személy tájékoztatása mellett – a munkáltató jogokat gyakorló vezető, a szerződéskötést kezdeményező szervezeti egység vezetője jelöli ki.
6.3. Külső felhasználók hozzáférése:

a) A CSZC igénybe vehet állományába nem tartozó külső felhasználókat általános, vagy kiemelt felhasználói jogosultságokkal időszakos, illetve folyamatos feladatok végrehajtására.
b) A CSZC külső felhasználóval való szerződéskötésével kapcsolatos eljárását a vonatkozó megállapodások szabályozzák.
c) Egyéb esetben a külső felhasználóval szerződést kötő CSZC szervezeti egység vezetője felelős a külső felhasználó bevonása által okozott informatikai, valamint az informatikai biztonsági követelmények betartásának ellenőrzéséért, szükség esetén a felelősségre vonás (illetve jogkövetkezmények bevezetésének) kezdeményezéséért, továbbá az IBSZ szerinti követelmények kommunikálásáért és a vonatkozó szerződésbe történő beépítéséért, az alábbiak szerint:
    a. a CSZC rendszereivel kapcsolatos vagy azokat érintő munkavégzés céljából érkező külső felhasználó a CSZC területén a szerződés létrejötte után kizárólag a szerződéskötést kezdeményező szervezeti egység vezetőjének tudtával és az általa kijelölt személy felügyelete mellett tartózkodhat,
    b. a külső felhasználó a munkafolyamat egyeztetése során minden olyan munkafolyamatról köteles beszámolni a szerződéskötést kezdeményező szervezeti egység vezetőjének, amely bármilyen módon érinti az informatikai rendszer biztonságát,
    c. amennyiben az a munkavégzéshez feltétlenül szükséges, a CSZC informatikai rendszereihez való hozzáféréshez ideiglenes, meghatározott időre és személyre szóló hozzáférési jogosultságot kell biztosítani, amelyről a szerződést kötő szervezeti egység vezetője gondoskodik, a CSZC személyügyekért felelőse útján bejelenti igényét,
    d. a CSZC külső felhasználóval csak olyan szerződést köthet, amely a külső felhasználó tekintetében biztosítja a vonatkozó titokvédelmi szabályok érvényesülését. A szerződéskötés során figyelembe kell venni az IBSZ előírásait, a jogszabályi előírásokat (különös tekintettel a szellemi alkotásokhoz fűződő, illetve szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő, vagy egyéb személyhez fűződő jogokra).

III. INFORMATIKAI BIZTONSÁGRA VONATKOZÓ FŐBB SZABÁLYOK

7. A felhasználókra vonatkozó szabályok

7.1. A CSZC-ben valamennyi felhasználó – jogosultságtól és állományba tartozástól függetlenül –:

a) felelős az általa használt, az IBSZ hatálya alá eső eszközök rendeltetésszerű használatáért,
b) a rá vonatkozó szabályok szerint felelős az általa elkövetett informatikai vonatkozású szabálytalanságokért, valamint a keletkező károkért és hátrányért, különös tekintettel az informatikai biztonsági incidens fogalomkörébe tartozó cselekményekért,
c) köteles az IBSZ-ben megfogalmazott szabályokat megismerni és betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni,
d) köteles a számára szervezett informatikai biztonsági oktatáson részt venni, az ismeretanyag elsajátításáról számot adni,
e) köteles a rendelkezésére bocsátott számítástechnikai eszközöket megóvni,
f) köteles a belépési jelszavát (jelszavait) az előírt időben megváltoztatni, biztonságosan kezelni,
g) felügyelet nélkül a munkahelyen (munkaállomáson) személyes adatot vagy minősített adatot tartalmazó dokumentumot, adathordozót nem hagyhat,
h) információ biztonságot érintő esemény gyanúja esetén az észlelt rendellenességekről köteles tájékoztatni a közvetlen felettesét és elektronikus információs rendszer biztonságáért felelős személyt,
i) köteles a folyó munka során nem használt hivatalos adatokat, dokumentumokat, nem nyilvános anyagokat, adathordozókat elzárni,
j) köteles a munkahelyről történő eltávozáskor az addig használt – kivéve, ha ez a rendszer(ek) más által történő használatát, vagy a karbantartást akadályozza – eszközt szabályszerűen leállítani,
k) az elektronikus levelezés és az internet használat során tartózkodik a biztonság szempontjából kockázatos tevékenységektől.

7.2. A CSZC informatikai rendszerét használó valamennyi felhasználónak tilos:

a) az általa használt eszközök biztonsági beállításait megváltoztatni,
b) a saját használatra kapott számítógép rendszerszintű beállításait módosítani (ide nem értve az irodai programok felhasználói beállításait),
c) a munkaállomására telepített aktív vírusvédelmet kikapcsolni,
d) belépési jelszavát (jelszavait), hardveres azonosító eszközét más személy rendelkezésére bocsátani, hozzáférhetővé tenni,
e) a számítógép-hálózatot fizikailag megbontani, számítástechnikai eszközöket lecsatlakoztatni, illetve bármilyen számítástechnikai eszközt rácsatlakoztatni a hálózatra az informatikai rendszert üzemeltetők jóváhagyása nélkül,
f) a számítástechnikai eszközökből összeállított konfigurációkat megbontani, átalakítani,
g) bármilyen (kivéve tanár által engedélyezett, oktatási célra használt) szoftvert installálni, internetről letölteni, külső adathordozóról merevlemezre másolni az elektronikus információs rendszer biztonságáért felelős személy engedélye, illetve az üzemeltető közreműködése nélkül, a munkaállomásokon nem a CSZC-ben rendszeresített, vagy engedélyezett szoftvereket (szórakoztató szoftverek, játékok, egyéb segédprogramok) installálni és futtatni,
h) online játékokat használni,

i) bármilyen eszközt számítástechnikai eszközökbe szerelni és használni,
j) az általa használt adathordozó (pl. CD, DVD, pendrive stb.) eszköz számítógépben hagyni a munkaállomásáról való távozás esetén,
k) ellenőrizetlen forrásból származó adatokat tartalmazó adathordozót az eszközökbe helyezni,
l) más szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő, vagy egyéb személyhez fűződő jogát vagy jogos érdekét sértő dokumentumokat, tartalmakat (zenéket, filmeket, stb.) az eszközökön tárolni, oda le-, illetve onnan a hálózatra feltölteni,
m) láncleveleket továbbítani, levélszemetet, továbbá azok mellékleteit, vagy linkjeit megnyitni,
n) rendszer biztonságáért felelős személy külön engedélye nélkül – feliratkozni, kivéve a munkavégzéshez szükséges:
    I. a CSZC által megrendelt, működtetett, vagy előfizetett szolgáltatásokat,
    II. belső információs rendszereket,
    III. közigazgatási, illetve nemzetközi, vagy uniós szervek/szervezetek által biztosított szolgáltatásokat,
    IV. közigazgatási szervek által felügyelt szervek, vagy szervezetek által biztosított szolgáltatások levelező listáit.

7.3. A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tranzakcióért a bejelentkezéstől a kijelentkezésig a bejelentkezett felhasználó a felelős. Ez a felelősség akkor is fennáll, ha a tranzakciókat harmadik személy hajtotta végre, amennyiben erre az IBSZ előírásainak felhasználó általi be nem tartása miatt kerülhetett sor.
7.4. Amennyiben a munkaállomást több személy is használhatja, a felhasználó a munkaállomást csak akkor hagyhatja el, ha minden futó programból, azonosított kapcsolatból és abban az esetben, ha nem egyedi felhasználói fiókos rendszer üzemel a számítógépen, az operációs rendszerből is kijelentkezett.
7.5. A felhasználó dokumentum nyomtatásakor köteles biztosítani, hogy az általa kinyomtatott irathoz illetéktelen személy ne férjen hozzá. Közös használatú hálózati nyomtató esetében a kinyomtatott iratot köteles a nyomtatóból eltávolítani, sikertelen nyomtatás esetén köteles meggyőződni – amennyiben szükséges, informatikus munkatárs segítségével – arról, hogy a nyomtató memóriájában nem maradt nyomtatandó dokumentum.
7.6. A felhasználó a rendelkezésére bocsátott, hordozható informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.

8. Vezetőkre vonatkozó szabályok

8.1. A CSZC szervezeti egységeinek vezetője (a továbbiakban: vezető) jogosult és köteles meghatározni az irányítása alá tartozó foglalkoztatottak munkavégzéséhez szükséges:
a) informatikai, irodatechnikai, multimédiás és kommunikációs eszközök körét,
b) a használandó informatikai rendszerek és az ahhoz szükséges jogosultságok körét.

8.2. A CSZC tagintézményeinek vezetője köteles együttműködni az elektronikus információs rendszer biztonságáért felelős személlyel annak informatikai biztonsági feladatai ellátása során.
8.3. A használatra kiadott informatikai, irodatechnikai, multimédiás vagy adathordozó eszközöknek a feladat végrehajtásra vonatkozó indokoltságát, meglétét az engedélyező vezetőnek évente felül kell vizsgálnia és az indokoltság megszűnése esetén gondoskodnia kell az eszköz visszavétele felől.

8.4. A vezető jogosult és köteles az informatikai eszközök munkavégzéshez szükséges használatának biztosítása érdekében a szükséges informatikai eszköz és jogosultság igénylési eljárásokat kezdeményezni a CSZC felé.
8.5. A vezető köteles gondoskodni az irányítása alá tartozó foglalkoztatottak informatikai biztonsági ismereteinek naprakészen tartásáról, beleértve az IBSZ és az IBSZ-el kapcsolatos CSZC rendelkezések szükséges mértékű ismeretét is.
8.6. A vezető az informatikai biztonsági előírások megsértésének észlelése esetén köteles

a) azonnal megtenni a szükséges intézkedéseket a biztonság helyreállítása érdekében,

b) kivizsgálni a biztonsági esemény körülményeit, különös tekintettel a személyes felelősség megállapítására,

c) a személyes felelősség megállapítását követően felelősségre vonást kezdeményezni.

8.7. A vezető jogosult az irányítása alá tartozó szerv vagy szervezeti egység tevékenységével kapcsolatos informatikai biztonsági feltételrendszerre vagy azok szabályozására vonatkozó javaslatot tenni a CSZC elektronikus információs rendszer biztonságáért felelős személye felé.

9. Külső felhasználókra vonatkozó szabályok

9.1. A CSZC informatikai rendszereihez és eszközeihez külső felhasználó csak érvényes szerződés alapján, dokumentáltan férhet hozzá.
9.2. A CSZC informatikai rendszereihez és eszközeihez hozzáférő külső felhasználó egyedileg köteles nyilatkozatot tenni arról, hogy az IBSZ-ben foglaltakat megismerte és az abban foglaltakat magára nézve kötelezőnek ismeri el.
9.3. A CSZC informatikai rendszereihez és eszközeihez hozzáférést biztosító szerződés csak olyan külső felhasználóval köthető, aki/amely az IBSZ-ben foglaltakat magára nézve kötelezőnek ismeri el.
9.4. Informatikai fejlesztések során a projekt teljes életciklusára nézve az egyes részeket oly módon kell dokumentálni (pl. fejlesztői dokumentáció, rendszerterv (logikai, fizikai, biztonsági), tesztelési dokumentáció, üzemeltetési dokumentáció), hogy azokból a biztonsági követelmények megvalósulása ellenőrizhető legyen.
9.5. Amennyiben a szerződés egyedi szoftverfejlesztési tevékenységre irányul, úgy csak olyan szerződés köthető, amely alapján a fejlesztett szoftver kellő mélységben kommentezett forráskódját a CSZC részére átadják, és a szerzői jogi védelem alá eső szoftver esetén a vagyoni jogokat a jogszabályok által engedélyezett legszélesebb körben átruházzák. Ettől csak különösen indokolt esetben lehet eltérni azzal, hogy a szerzői jogi védelem alá eső szoftver kizárólagos felhasználási joga a jogszabályok által engedélyezett legszélesebb körben a CSZC részére ebben az esetben is átruházásra kerül.
9.6. Az informatikai rendszerek üzemeltetése során külső felhasználó kizárólag a CSZC kijelölt munkatársának jelenlétében férhet hozzá a CSZC informatikai rendszereihez.
9.7. A CSZC központi intézményében történő helyszíni munkavégzés felügyelet mellett történhet.
9.8. Az informatikai rendszerek fejlesztése során külső felhasználó a teszt környezetben lévő, informatikai rendszerhez az elektronikus információs rendszer biztonságáért felelős személy engedélyével távoli eléréssel hozzáférhet. Az engedélyt elektronikus írásbeli formában a fejlesztést végző CSZC tagintézményének vezetője igényli a fejlesztés kezdetekor.

IV. INFORMÁCIÓBIZTONSÁGI KÖVETELMÉNYEK TELJESÜLÉSE

10. Szervezeti biztonsági követelmények

10.1. Az egyes informatikai rendszerekkel és adathordozókkal kapcsolatos fejlesztési, üzemeltetési és biztonsági tevékenységet úgy kell megtervezni és végrehajtani, a fejlesztési, működtetési és védelmi terveket, dokumentumokat, előírásokat úgy kell elkészíteni, hogy azok a biztonsági osztályozási előírások figyelembevételével garantálják az információbiztonság szükséges és elégséges szintjét. Ezen elvek alapján kockázatarányos, differenciált, többszintű informatikai védelmi rendszert kell kialakítani és működtetni.
10.2. A 2.3. pontban említettek felügyelete és üzemeltetése vonatkozásában érvényesíteni kell az összeférhetetlenség elvét oly módon, hogy a feladategyesítésből eredő hibák és rosszindulatú tevékenységek kockázatát kizárják, vagy elfogadható szintre csökkentsék.
10.3. Minimális összeférhetetlenségi szabályok különösen:

a) Az CSZC informatikáért felelős személye az informatikával összefüggő feladatain kívül nem láthat el más szakmai (például köznevelés-igazgatási, szakképzés-szervezési stb.) feladatokat.
b) Szakmai és funkcionális informatikai alkalmazás szakmai felügyeletét kizárólag a CSZC központi egysége láthatja el.
c) A fejlesztési, a minőségbiztosítási és az üzemeltetési feladatokat ellátó egységeket a visszaélések megelőzése érdekében szervezeti szinten el kell különíteni egymástól.
d) Az informatikai szerepkörök/feladatok személyre (véglegesen vagy átmeneti időszakra történő) telepítését belső felhasználók esetében úgy kell végrehajtani, hogy az üzemeltetési, fejlesztési, változáskezelési, minőségbiztosítási, információbiztonság felügyeleti feladatok ellátásának egymástól való függetlensége biztosított legyen.
e) Az informatikai szerepkörök/feladatok személyre telepítésekor kötelező gondoskodni a helyettesítésről oly módon, hogy e feladatokat is CSZC foglalkoztatott tudja ellátni.
f) A feladatok és felelősségek személyekhez rendelésekor biztosítani kell a felelősségi viszonyok egyértelmű megállapíthatóságát.

11. Személyi biztonsági követelmények, oktatás, jogosultságkezelés

11.1. A foglalkoztatottakat a CSZC-ben végzendő tevékenység megkezdése előtt informatikai biztonsági képzésben kell részesíteni.
11.2. Az informatikai biztonságra vonatkozó jogszabályi környezet megváltozásakor, továbbá ha a CSZC informatikai biztonságát, illetve az IBSZ tartalmát érintő jelentős változás következik be, az IBSZ hatályba lépését, illetve a jelentős változását követő 60 napon belül a felhasználókat informatikai biztonsági továbbképzésben, a külső felhasználókat informatikai biztonsági tájékoztatásban kell részesíteni (a továbbiakban együtt: oktatás).
11.3. Az oktatás tematikájának összeállításáért a CSZC információs rendszer biztonságáért felelős személye, az oktatás megszervezéséért, végrehajtásáért a CSZC vezetője a felelős.
11.4. Az oktatáson történt részvételt a megjelent személyek az IBSZ oktatásán való részvételről szóló nyilatkozat aláírásával igazolják. Az IBSZ oktatásán való részvételről szóló nyilatkozatban az oktatáson történt részvétel igazolása mellett kötelesek nyilatkozni arról, hogy az informatikai biztonsági előírásokat megismerték és azok betartását magukra nézve kötelezőnek fogadják el. Az IBSZ oktatásán való részvételről szóló nyilatkozatot

foglalkoztatottak esetében a személyügyi anyaggal együtt, külső felhasználó esetében a polgári jogi szerződéssel együtt kell őrizni.
11.5. Az oktatást végző személy az oktatáson részt vett személyekről olvashatóan kitöltött Jelenléti ívet készít, melyet a CSZC vezetőjének átad.
11.6. A CSZC informatikai rendszereihez, a rendszerekben tárolt adatokhoz kizárólag az IBSZ oktatásában részesült személyek férhetnek hozzá. Az oktatás hiányában hozzáférési jogosultság nem kérhető.
11.7. A külső felhasználók IBSZ-szel való megismertetése a szerződéskötést kezdeményező szervezeti egység vezetőjének feladata és felelőssége.
11.8. Új felhasználó hozzáférési rendszerbe való illesztését a CSZC tagintézmény információs rendszer biztonságáért felelős személye végzi. Az új felhasználói jogosultság létrehozása a Kinevezési dokumentumok aláírását követően történik.
11.9. A jogosultságok kiosztása előtt, amennyiben az adott munkakör, tevékenység megköveteli a tipikus jogoktól – ide nem értve a munkavégzéshez szükséges adatbázisok elérését – történő eltérést a tagintézmény vezetőjének hatásköre eldönteni.
11.10. A hozzáférési jogosultság zárolásra, megszüntetésre kerül a felhasználó hozzáférést megalapozó jogviszonyának azonnali hatályú megszüntetésekor. A jogviszony más jogcím alapján történő megszüntetése, illetve megszűnése esetén a hozzáférési jogosultság a jogviszony megszűnése – vagy amennyiben előbb bekövetkezik a munkavégzési kötelezettség alóli mentesítés – napjától kerül zárolásra.
11.11. A hozzáférési jogosultság a foglalkoztatotti jogviszony fennállása alatt zárolásra, megszüntetésre vagy módosításra kerül.
11.12. A felhasználó hozzáférést megalapozó jogviszonyának megszűnésekor a munkáltatói jogkör gyakorlója, illetve a szerződéskötést kezdeményező vezető a felhasználó tájékoztatása mellett köteles rendelkezni a felhasználó adatainak, munkavégzéssel kapcsolatos dokumentumainak további kezeléséről (archiválás, törlés, harmadik személy általi hozzáférhetőség).
11.13. Amennyiben a felhasználó hozzáférést megalapozó jogviszonya megszűnik, de a hozzáférés más formában továbbra is indokolt (valamely új jogviszony a felhasználót továbbra is a CSZC-hez köti pl. távoli hozzáférést használó külsős dolgozó, tanácsadó, egyéb jogviszony) a felhasználói jogosultságokat meg kell szüntetni és a felhasználót új felhasználóként kell kezelni, az új jogviszonyra irányadó eljárásrend alapján.

12. Fizikai biztonsági követelmények

12.1. Az informatikai eszközöket úgy kell telepíteni és tárolni, hogy azokhoz a foglalkoztatottakon, külső felhasználókon kívüli más személy hozzáférése kizárt legyen.
12.2. A CSZC tulajdonát képező vagy az általa használt informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót a CSZC objektumaiból kivinni csak hivatali feladat ellátására, a közvetlen vezető elektronikus írásbeli engedélyével (e-mail) lehet.

13. Informatikai biztonsági követelmények

13.1. Az informatikai rendszerekben csak jogtiszta szoftver telepíthető.
13.2. A hivatali feladatok ellátásához szükséges felhasználáson kívül informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót az informatikai rendszerekhez csatlakoztatni tilos.
13.3. Nem a CSZC tulajdonát képező informatikai, irodatechnikai, multimédiás eszközt az informatikai rendszerekhez vagy azok elemeihez csatlakoztatni tilos. Kivételt képeznek a

CSZC alap- vagy funkcionális tevékenységével összefüggésben az együttműködő partnerektől hivatalos tevékenységük során átvett eszközök.
13.4. A CSZC területén a CSZC által kezelt adatok védelmére vonatkozó rendelkezéseket vagy személyiségi jogokat sértő, továbbá a CSZC működésére vonatkozó magáncélú adatrögzítés – beleértve a hang- és képfelvétel készítését is – tilos.
13.5. Az informatikai rendszerekben végrehajtott műveleteket a felhasználó azonosítását lehetővé tevő módon naplózni kell.

14. Adminisztratív biztonsági követelmények

14.1. Az informatikai rendszerek teljes életciklusát dokumentálni kell, így a tervezés, a fejlesztés és továbbfejlesztés, a tesztelés és ellenőrzés, az üzemeltetés és karbantartás, valamint a megszüntetés fázisait is.
14.2. A dokumentáció teljességéért és naprakészségéért az informatikai rendszert fejlesztő, a rendszer üzemeltetésének megkezdésétől a szakmai felügyeletet ellátó szervezeti egység vezetője felel.
14.3. Az informatikai rendszer dokumentációja akkor teljes, ha tartalmazza mind a funkcionális, mind a biztonsági megfelelőségre vonatkozó valamennyi lényeges adatot.
14.4. Az elektronikus adatokat tároló eszközöket a rajtuk tárolt vagy tárolandó adatokat a jogszabályi előírásoknak megfelelően kell kezelni.
14.5. Az elektronikus adatokat tároló eszközök azonosítását, mozgásuk nyomon követhetőségét az átadás-átvétel, továbbítás, selejtezés, megsemmisítés dokumentálásával biztosítani kell.
14.6. Az elektronikus adathordozók kezelése vonatkozásában az IBSZ-ben nem szabályozott kérdésekben az Iratkezelési Szabályzat előírásai értelemszerűen irányadóak.
14.7. A papír alapú dokumentumok előállítására alkalmas eszközök (nyomtató, plotter, fax) használatára az informatikai eszközökre vonatkozó szabályozások érvényesek. A felhasználók számára tiltott tevékenységek a CSZC adatait nyomtatott formában megjelenítő eszközök esetén is irányadóak.

V. AZ INFORMÁCIÓBIZTONSÁG MŰKÖDTETÉSE

15. Megfelelés az IBSZ-nek, fenyegetettségek

15.1. A CSZC információbiztonsági fenyegetettségének elemzését és a kockázatok meghatározását évente el kell végezni.
15.2. Az IBSZ-nek megfelelő működést igény szerint, de legalább évente teljes körűen ellenőrizni kell.
15.3. A fenyegetettségek elemzését és a kockázatok meghatározását az elektronikus információs rendszer biztonságáért felelős személy hajtja végre, szükség szerint független külső szakértő bevonásával.

16. Az IBSZ felülvizsgálata, aktualizálása

16.1. Az IBSZ-t szükség szerint – de legalább évente – felül kell vizsgálni és aktualizálni kell, így különösen:

– súlyos informatikai biztonsági eseményeket (incidensek) követően, az esemény tanulságaira figyelemmel,

– a szabályozási környezet változása esetén, amennyiben az az IBSZ-ben foglaltakat érinti.

16.2. Amennyiben az IBSZ rendkívüli módosítása szükséges – a szükséges módosítás jellegétől vagy terjedelmétől függetlenül – az információs rendszer biztonságáért felelős személy közvetlenül jelzi ezt a CSZC vezetőjének.

17. Az informatikai biztonsági események felismerése, jelentése

17.1. Minden felhasználó kötelessége – amennyiben kellő gondossággal eljárva azt felismerhette – a lehetséges legrövidebb időn belül közvetlen vezetőjének bejelenteni minden olyan veszélyforrást, amely az elektronikus információbiztonságra nézve érdemi fenyegetést jelent vagy jelenthet.

17.2. A felhasználó részéről különösen a következő veszélyforrások jelzése kötelező:

a) az IBSZ-ben, a vonatkozó jogszabályokban előírt elektronikus információbiztonsági rendszabályok lényeges megszegése, illetve ennek gyanúja,

b) a felismert vagy felismerni vélt, az elektronikus információbiztonságot lényegesen veszélyeztető esemény, ezen belül különösen:

I. nem nyilvános adat illetéktelen személy általi megismerése,

II. informatikai rendszerekben tárolt adatok illetéktelen személyek általi megváltoztatása, törlése vagy hozzáférhetetlenné tétele,

III. informatikai rendszer működésének, használatának jogosulatlan akadályozása,

IV. nem engedélyezett vagy licenc-szel nem rendelkező szoftver telepítése,

V. felhasználói jelszavak egymás közötti megosztása, hozzáférhetővé tétele,

VI. vírusfertőzés, kémprogramok, billentyűzetleütést figyelő alkalmazások megjelenése,

VII. mobil eszköz elvesztése, ellopása esetén,

VIII. fentiek bármelyikére tett kísérlet (a továbbiakban együtt: biztonsági események).

17.3. Nem számít informatikai biztonsági eseménynek az informatikai hiba, meghibásodás vagy rendszeresemény, amely nem érinti az informatikai szolgáltatások minőségét és azt az üzemeltetők képesek megoldani.

17.4. A bejelentés során minimálisan megadandó információk:

a) az informatikai biztonsági esemény pontos leírása,

b) érintett informatikai szolgáltatás pontos megnevezése,

c) érintett informatikai eszköz gyári száma, leltári száma, típusa,

d) tagintézmény neve, pontos címe (emelet, ajtó),

e) észlelő neve, elérhetősége (opcionális),

f) A vezető által kijelölt helyszíni kapcsolattartó neve, elérhetősége.

18. Biztonsági események kivizsgálása

18.1. A biztonsági eseményeket soron kívül ki kell vizsgálni. A vizsgálatot az elektronikus információs rendszer biztonságáért felelős személy folytatja le, szükség szerinti mértékben bevonva a CSZC központi szervezetét.

18.2. A vizsgálat eredményét az elektronikus információs rendszer biztonságáért felelős személy írásban dokumentálja, amelyből 1-1 példányt kap az elektronikus információs rendszer biztonságáért felelős személy, illetve a biztonsági eseményben közvetlenül érintett(ek).

19. Biztonsági események nyilvántartása

19.1. A biztonsági események kapcsán tett bejelentések, a lefolytatott vizsgálatok, valamint a végrehajtott intézkedések adatait külön nyilvántartás, a Biztonsági Nyilvántartás tartalmazza, amelyet az elektronikus információs rendszer biztonságáért felelős személy és a biztonsági vezető közösen vezet.
19.2. A Biztonsági Nyilvántartás adatait fel kell használni:

a) a bekövetkezett biztonsági esemény következményeinek enyhítésére,

b) a jövőben várható hasonló biztonsági események megelőzésére, bekövetkezési gyakoriságának csökkentésére,

20. A biztonsági szabályok megszegésének következményei

20.1. Az informatikai biztonsággal kapcsolatos szabályok megszegése esetén a szabályszegőkkel szemben érvényesítendő jogkövetkezmények tekintetében elsősorban annak súlyosságára tekintettel vagy etikai, vagy munkáltatói fegyelmi jogkörben kell eljárni.
20.2. Az információbiztonsággal kapcsolatos szabályok súlyos megszegése vagy annak gyanúja esetén az elektronikus információs rendszer biztonságáért felelős személy javaslatára – érintett foglalkoztatott közvetlen vezetője, illetve az utasítási joggal rendelkező vezető véleményének kikérésével – az elnök jogosult a megfelelő jogkövetkezmények érvényesítése érdekében eljárást indítani, illetőleg eljárás megindítását kezdeményezni.

21. Azonosítás és feljogosítás az informatikai rendszer használatára

21.1. A felhasználó az informatikai rendszert csak egyértelmű azonosítást követően, a számára meghatározott és biztosított jogosultságok keretei között használhatja.
21.2. Az informatikai rendszer használata során a felhasználók egyértelmű azonosítását folyamatosan biztosítani kell.
21.3. Minden felhasználót kizárólagos személyi használatú egyedi azonosítóval kell ellátni, amelyhez minimálisan egyedi jelszót kell rendelni. További azonosítási lehetőségek is elfogadottak, melyek az elektronikus információs rendszer biztonságáért felelős személy engedélyével vezethetők be.
21.4. A felhasználók azonosítójának a felhasználói nevet tartalmaznia kell. Kivételt képeznek az operációs rendszerek különleges, előre rögzített azonosítói és a különleges informatikai feladatkört ellátók által használt speciális és teszt felhasználói nevek. A felhasználói névben törekedni kell a családi és utónév használatára, névazonosság esetén a felhasználónevek megkülönböztetésére.
21.5. A felhasználói jelszónak legalább az alábbi követelményeket teljesítenie kell:

a) legalább 6 karakter hosszú,

b) kis- és nagybetűket és számokat vegyesen tartalmaz,

c) nem tartalmazhat könnyen kitalálható, ismétlődő karaktersorozatot,

d) nem utalhat a felhasználó személyére,

e) érvényességi ideje legfeljebb 90 nap,

f) az utolsó négy jelszó használata tiltott

g) maximum 5 téves próbálkozás után a fiók/munkaállomás zárolási ideje 15 perc.

21.6. A jelszó megváltoztatása kötelező:

a) a felhasználói azonosító informatikai rendszerbe történt felvételét követő első bejelentkezéskor,

b) az informatikai üzemeltető szervezeti egység munkatársa általi újbóli jelszóbeállítást, felülírást követően,

c) ha a jelszó illetéktelen személy tudomására juthatott vagy bármilyen módon nyilvánosságra kerülhetett,

d) az érvényességi idő lejártakor.

21.7. A felhasználó köteles a jelszót bizalmasan őrizni, illetéktelenek általi megismerését kizárni.

21.8. Tilos a jelszót más által megismerhető módon feljegyezni, azt mással bármilyen formában közölni.

22. Szoftverek telepítése, internethasználat

22.1. A hálózathoz csatlakozó munkaállomásra csak a munkavégzéshez szükséges adatállományok, programok tölthetők le, illetve telepíthetők.

22.2. A hálózathoz csatlakozó munkaállomásra nem telepíthető, nem másolható – ideiglenesen sem –, illetve a belső hálózaton nem tehető közzé olyan adatállomány, információ, amely

a) jogszabályt sért, így különösen adatvédelmi, szerzői jogvédelmi, személyiségvédelmi előírásba ütközik,

b) a hálózat rendeltetésszerű működését, biztonságát veszélyezteti vagy veszélyeztetheti, így különösen annak erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon veszi igénybe.

22.3. Az internet felhasználása csak a CSZC ügymenete érdekének megfelelően kialakított és betartott szabályok alapján történhet.

22.4. Az internet-szolgáltatás minőségének szinten tartása és a CSZC érdekeinek biztosítása céljából a CSZC – az elektronikus információs rendszer biztonságáért felelős személy javaslatára vagy engedélyével – korlátozásokkal élhet. A korlátozások a következőkre terjedhetnek ki:

a) bizonyos fájl-típusok letöltésének korlátozása,

b) az alapvető etikai normákat sértő oldalak látogatásának tiltása,

c) a látogatható weboldalak körének behatárolása és a maximális fájl-letöltési méret korlátozása.

22.5. Felhasználók internet használatára vonatkozó általános szabályok:

a) csak a munkavégzéshez, szakmai tájékozottság bővítéséhez szükséges vagy általános tájékozottságot biztosító információt, segítséget nyújtó oldalak látogathatók,

b) tilos a jó ízlést, közerkölcsöt sértő, rasszista, uszító és más, a véleménynyilvánítás kereteit meghaladó oldalak szándékos látogatása, online játékok, fogadási oldalak felkeresése, bármely tartalommal kapcsolatos magánvélemény kinyilvánítása (pl. privát blog és chat),

c) a felhasználók nem tölthetnek fel egyénileg – a felelős jóváhagyása nélkül – a CSZC-val kapcsolatos adatot az internetre,

d) az internetről csak a munkavégzéshez szükséges adatállományok, táblázatok, tölthetők le, alkalmazások, programok nem,

e) a látogatott oldal nem szokványos működése (pl.: folyamatos újratöltődés, kilépés megtagadása, ismeretlen oldalak látogatására történő kényszerítés, ismeretlen program futásának észlelése, stb.) esetén a közvetlen technikai támogató segítségét kell kérni.

23. Elektronikus levelezőrendszer használata a központi munkaegységben

23.1. A CSZC központi feladatainak végrehajtásához alkalmazott elektronikus levelezésben kizárólag a cegledіszc.hu végződésű, hivatali levelezési cím használható. Magán e-mail

címről hivatali információt továbbítani tilos. A CSZC tevékenységével össze nem függő célra a hivatali postafiók, levelezési cím nem használható.
23.2. A CSZC-al közszolgálati jogviszonyban vagy munkaviszonyban álló személy kaphat levelezési címet, személyes postafiókot. Külsős munkavállaló esetén a kancellár egyedi elbírálás alapján postafiók beállítást igényelhet.
23.3. A levelezőrendszerek használata során a vírusvédelmi előírásokat folyamatosan érvényesíteni kell.
23.4. A hivatali levelezőrendszeren kizárólag hivatali célú üzenetek továbbíthatók. Magáncélú üzenetet nem nevesített felhasználóknak (pl. csoport, mindenki) küldeni tilos.

24. Vírusvédelem

24.1. A vírusvédelmi eljárásokat, a vírusvédelemre vonatkozó szabályozást, beleértve az intézkedési rendet, úgy kell kialakítani, hogy az

a) a folyamatos vírusvédelmi felügyelet ellátását lehetővé tegye,
b) támogassa a valós riasztások kiszűrését,
c) alkalmas legyen a súlyos gondatlanságot, szándékosságot jelentő esetek felismerésére,
d) tegye lehetővé az általános vírusbiztonsági helyzet értékelését,
e) biztosítsa az új fenyegetések időben történő felismerését.

24.2. A hálózat esetében a vírusvédelem központilag biztosított.
24.4. A vírusvédelmi előírások súlyos, szándékos vagy sorozatos megsértése rendkívüli információbiztonsági eseménynek (incidens) minősül.

VI. INFORMÁCIÓBIZTONSÁGI ELJÁRÁSOK

25. Általános irányelvek

25.1. Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakör, feladat ellátásához szükséges minimális funkcióelérést biztosíthatják.
25.2. A hozzáférési jogosultságok kezelését, a jogosultságigénylés folyamatának részleteit – annak kiadását követően – a jogosultságkezelési szabályzat tartalmazza.
25.3. A felhasználók a hozzáférésüket megalapozó jogviszonyuk létrejöttét követően (a lehető legrövidebb időn belül) megkapják felhasználói azonosítójukat.
25.4. A kiosztott felhasználói azonosítót haladéktalanul használatba kell venni. Ennek első lépéseként az induló (alapértelmezett) jelszót meg kell változtatni.
25.5. Amennyiben a felhasználó jogviszonya előreláthatólag három hónapot meghaladóan szünetel, vagy a felhasználó a munkavégzésben előreláthatóan ennyi ideig nem vesz részt, a hozzáférést megalapozó jogviszonyából eredő feladatát tartósan nem látja el, a felhasználói azonosítóját fel kell függeszteni (inaktiválni kell) a munkába állás, az adott tevékenység folytatása napjáig. Az inaktiválást a közvetlen vezető, illetve a szerződéskötést kezdeményező tagintézmény vezetőjének hatásköre. A felhasználói azonosító újraaktiválási igényének felmerülésekor a hozzáférés helyreállítását szintén a közvetlen vezető, illetve a szerződéskötést kezdeményező vezetőjének hatásköre.
25.6. A felhasználók szervezeten belüli áthelyezése kapcsán felmerülő jogosultsági változásokat a felhasználó vezetője intézi.
25.7. Gyakornokok esetén a hozzáférési jogosultságok – hasonlóan a külső felhasználók számára létrehozott azonosítókhoz –, csak bizonyos, a munkavégzésükhöz feltétlenül szükséges területekhez való hozzáférést tehetnek lehetővé. A hozzáférési jogosultság megadását a gyakornokot alkalmazó vezetője intézi.

26. Munkaállomások hozzáférésére vonatkozó minimális előírások

26.1. A számítógépes munkaállomások képernyőit (monitor) úgy kell elhelyezni, hogy az azon megjelenő információkat illetéktelen személy ne láthassa.
26.2. A munkaállomás beállításait adminisztrátori jelszóval kell védeni módosítás ellen.
26.3. Szenzitív adatbázisokat és programokat – amennyiben megoldható – hardveres azonosítást biztosító eszközzel kell védeni.

27. Szoftvereszközök használatának szabályozása

27.1. Az informatikai biztonság teljes körű megvalósításához hozzájárul a jogtiszta szoftverek és a szoftvereszközök jogszerű használata, valamint a szoftverek biztonságos kezelése.
27.2. A CSZC által használt szoftvereket az elektronikus információs rendszer biztonságáért felelős személy ellenőrizheti.
27.3. A rendszeres szoftvervizsgálat során ellenőrizni kell:

a) a használatban lévő szoftverek rendelkeznek-e licence-szel (ide nem értve az engedélyezett freeware szoftvereket),
b) a megvásárolt licencek száma arányos-e a használt szoftverek mennyiségével,
c) a használt szoftverek verziószámát,
d) a ténylegesen használt szoftverek megegyeznek-e az engedélyezett szoftverek listájával.

27.4. A szoftvereszközök telepítésére és használatára vonatkozó általános szabályok:

a) a CSZC munkaállomásaira csak eredményesen tesztelt szoftverek telepíthetők,
b) tilos a munkaállomásokra licence-szel nem rendelkező vagy a kereskedelmi forgalomban beszerezhető nem engedélyezett vagy nem a CSZC által fejlesztett szoftvert telepíteni,
c) a CSZC által vásárolt és kifejlesztett szoftverek (és a hozzájuk tartozó dokumentumok) másolása és átadása harmadik fél részére tilos, kivéve, ha a licencszerződés ezt külön szabályozza és lehetővé teszi,
d) a felhasználók csak a CSZC által telepített szoftvereket, ide értve az engedélyezett freeware szoftvereket is használhatják
e) a felhasználók rendelkezésére bocsátott hardver és szoftver eszközök ellenőrzését az elektronikus információs rendszer biztonságáért felelős személy bejelentés nélkül bármikor kezdeményezheti.

28. Mobil IT tevékenység, hordozható informatikai eszközök használata

28.1. A mobil eszközök használatával kapcsolatban a következő biztonsági eljárásokat kell alkalmazni:

a) a mobil eszközök átvételéhez átadás-átvételi dokumentumokat kell készíteni;
b) mobiltelefonok, tabletek esetén legalább PIN kód beállítása a feloldáshoz;
c) valamennyi hordozható személyi számítógépet rendszeres szoftver-, adat- és biztonsági ellenőrzéseknek kell alávetni. Rendszeres időközönként (lehetőleg havi 1 alkalommal) a munkahelyi hálózatához kell csatlakoztatni az eszközt az operációs rendszer biztonsági és vírusvédelmi frissítéseinek végrehajtása érdekében. A mobil eszközt szállító felhasználók:

I. kötelesek azt a szállítás idejére lehetőleg minél kevésbé szem előtt lévő módon elhelyezni,
II. nem hagyhatják őrizetlenül gépjárműben,

II. repülés vagy vonatút, valamint autóbuszon történő utazás ideje alatt kézipoggyászként kötelesek szállítani.

28.2. Azokban az esetekben, amikor az eszközök nem a CSZC épületeiben (szálloda, lakás) találhatók, fokozott figyelmet kell szentelni a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása vagy ellopása elleni védelemnek.

28.3. Tilos a mobil eszközök:

a) engedély nélküli átruházása vagy adatainak közlése, lementése,

b) megfelelő védelem nélkül nem biztonságos hálózathoz csatlakoztatása,

c) bármilyen indokolatlan veszélynek történő kitétele vagy nem rendeltetésszerű használata.

28.4. A CSZC adataiból csak azon adatokat szabad mobil eszközön tárolni:

a) amely adatokról központi biztonsági mentés készül,

b) amelyekkel kapcsolatban biztosítani lehet a jogszabályban vagy belső szabályban előírt adatbiztonságot és adatvédelmet.

VII. ELLENŐRZÉSEK, RENDSZERES FELÜLVIZSGÁLATOK

29. Ellenőrzésekre vonatkozó szabályok

29.1. Az információbiztonságot folyamatosan kontrollálni kell. A kontroll eljárások kialakításánál elsődlegesen azt kell figyelembe venni, hogy azok által az információbiztonság szintje mérhető legyen.

29.2. Ennek érdekében meg kell határozni az ellenőrzések területeit, és minden területhez külön-külön meg kell fogalmazni az ellenőrzési célkitűzéseket. Az ellenőrzési célkitűzések ismeretében meg kell jelölni az ellenőrzés eszközeit (dokumentumok, naplók, szoftverek, adatok, amelyek a biztonsági rendszerről hiteles képet tudnak adni), azok tartalmi követelményeit.

29.3. Az ellenőrzés eredményét minden esetben ki kell értékelni és a megfelelő következtetéseket le kell vonni, illetve vissza kell csatolni a biztonsági folyamatra. Szükség esetén felelősségre vonási eljárást kell kezdeményezni.

29.4. Az ellenőrzéseket dokumentumok, dokumentációk, személyes beszámoltatás és helyszíni szemlék alapján lehet végrehajtani.

29.5. Az informatikai biztonsággal kapcsolatos ellenőrzések területei az alábbiak lehetnek:

a) megfelelőségi vizsgálat – célja felderíteni, hogy a CSZC rendelkezik-e az elégséges személyi, eljárási, tárgyi feltételekkel és azok megfelelően dokumentáltak-e,

b) információbiztonság szintjére vonatkozó vizsgálat – célja felderíteni, hogy az információbiztonság szintje megfelel-e a meghatározott védelmi szintnek,

c) információbiztonsági szabályok betartásának ellenőrzése – célja felderíteni, hogy a CSZC információbiztonsági szabályait a felhasználók ismerik-e, illetve betartják-e,- ez az ellenőrzés az informatikai biztonság egy-egy területére is leszűkíthető,

d) biztonsági dokumentumrendszer felülvizsgálata – célja a CSZC belső szabályrendszerét képező hatályos eljárások felülvizsgálata, hogy azok megfelelnek-e az elvárt jogi, informatikai, szakmai elvárásoknak és az általuk szabályozott területen megfelelő szabályok betartására alkalmazhatóak.

29.6. Az ellenőrzések során elsősorban az alábbiakat kell vizsgálni:

a) az IT biztonsági rendszer működése megfelel-e a biztonsági követelményeknek, az IT-rendszer előírt dokumentumai léteznek-e, illetve naprakészek-e,

b) az IT biztonsági rendszer felépítése, tartalma megfelel-e a vonatkozó szabványnak,

c) az IT biztonsági szabályok érvényesülnek-e a folyamatokban;

d) az IT-személyzet, illetve a felhasználók rendelkeznek-e a megfelelő IT-biztonsági ismeretekkel,

e) az adatokra és a rendszerekre vonatkozó kezelési szabályok betartását,
f) a naplózási rendszer megfelelő alkalmazását,
g) a biztonsági események kezelésének, a szükséges mértékű felelősségre vonás gyakorlatát,
h) a mentési rendszer megfelelő alkalmazását,
i) a hozzáférési jogosultságok naprakészségét, a kiadott jogosultságok szükségességét,
j) a dokumentációk pontosságát, naprakészségét, a változások követését, megfelelő kezelését, nyilvántartását,
k) az alkalmazott szoftverek jogtisztaságát,
l) a szerződések megfelelőségét,
m) a fizikai biztonsági előírások betartását.

VIII. ZÁRÓ RENDELKEZÉSEK

A szabályzat 2019. március 1-jén lép hatályba.

2019. március 1.

Dr. Ferenczi Norbert
kancellár

Megismerési záradék
az Informatikai Biztonsági Szabályzathoz

Alulírottak, nyilatkozunk arról, hogy a centrum és tagintézményei az Informatikai Biztonsági Szabályzatban foglaltakat megismertük, azokat a saját feladatunk vonatkozásában magunkra nézve kötelezőnek ismerjük el.

Egyúttal nyilatkozom arról, hogy a centrum/tagintézmények érintett dolgozóival a szabályzatot ismertetni fogjuk.

Név	*Munkakör, feladat ellátó*	*Aláírás*	*Megjegyzés*
Buncsák Gábor	főigazgató		a szabályzat egy példányát átvettem
Hegedűsné Homoki Mária	gazdasági vezető		a szabályzat egy példányát átvettem
Szabadi Zoltán	szakmai főigazgató-helyettes		a szabályzat egy példányát átvettem
Fernengel Katalin	tagintézmény-vezető		a szabályzat egy példányát átvettem
Imréné Lukácsi Ildikó	tagintézmény-vezető		a szabályzat egy példányát átvettem
Fehérvári Károly	tagintézmény-vezető		a szabályzat egy példányát átvettem
Sápi Viktória	megbízott tagintézmény-vezető		a szabályzat egy példányát átvettem
Baranyi Tibor	tagintézmény-vezető		a szabályzat egy példányát átvettem
Fekete József	tagintézmény-vezető		a szabályzat egy példányát átvettem

A megismertetési feladatokat a mai napon elláttam.

Cegléd, 2019. március 1.

Cegléd Szakképzési Centrum 3.

Szabadi Zoltán
szakmai főigazgató-helyettes