Békéscsabai Szakképzési Centrum
OM azonosító: 203029
E/2020/000209
5600 Békéscsaba, Gyulai út 32/1.
Tel.: +36 66/441-314
Fax: +36 66/441-314
www.bszc.hu
E-mail: centrum@bszc.hu

Ikt.szám:

NSZFH/602/
000054-4/2026

BÉKÉSCSABAI SZAKKÉPZÉSI CENTRUM INFORMÁCIÓBIZTONSÁGI SZABÁLYZAT

Készült: 2026. augusztus 12.

Hatályos: 2026. szeptember 01.

Érvényes: visszavonásig

Jóváhagyta:

Mucsi Balázs Sándor
főigazgató

Békéscsabai Szakképzési Centrum 5.

Uhljár Erik Róbert
kancellár

Tartalomjegyzék

1. Általános rendelkezések

1.1. Preambulum

A Békéscsabai Szakképzési Centrum (a továbbiakban: **BSZC**) kiemelt jelentőséget tulajdonít az általa kezelt információk, elektronikus információs rendszerek, informatikai infrastruktúra, valamint a személyes és egyéb védendő adatok biztonságának.

A BSZC alapfeladata a szakképzésről szóló jogszabályokban meghatározott feladatok magas színvonalú ellátása. E feladatok biztonságos, folyamatos és jogszerű végrehajtásának elengedhetetlen feltétele az információk megfelelő védelme, az informatikai rendszerek megbízható működése, valamint az információbiztonsági követelmények következetes érvényesítése.

A BSZC vezetése elkötelezett amellett, hogy:

- biztosítsa az információbiztonsági és adatvédelmi követelmények folyamatos érvényesülését;
- elősegítse a biztonságtudatos szervezeti kultúra kialakítását;
- támogassa az informatikai infrastruktúra biztonságos fejlesztését és üzemeltetését;
- biztosítsa a jogszabályoknak megfelelő szervezeti és technikai védelmi intézkedések alkalmazását;
- előmozdítsa a kiberbiztonsági kockázatok megelőzését, felismerését és kezelését.

Az információbiztonság a BSZC valamennyi szervezeti egységének közös felelőssége. A vezetés fontosnak tartja, hogy a BSZC valamennyi munkavállalója, valamint minden olyan személy, aki a BSZC elektronikus információs rendszereit használja, a Szabályzat rendelkezéseit megismerje, betartsa és munkavégzése során következetesen alkalmazza.

1.2. A Szabályzat rendeltetése és alkalmazásának alapelvei

Az Információbiztonsági Szabályzat (a továbbiakban: **Szabályzat**) a BSZC belső normatív szabályozó dokumentuma. Rendelkezéseit a hatályos jogszabályokkal, a BSZC Szervezeti és Működési Szabályzatával, valamint egyéb belső szabályzataival összhangban kell alkalmazni.

A Szabályzat meghatározza:

- az információbiztonság alapelveit;
- az informatikai és elektronikus információs rendszerek biztonságos használatának követelményeit;
- a vezetők, munkavállalók és egyéb felhasználók jogait és kötelezettségeit;
- az információbiztonsági irányítás szervezeti rendjét;
- az informatikai rendszerek üzemeltetésére és használatára vonatkozó alapvető szabályokat;
- a biztonsági események kezelésének rendjét;
- az ellenőrzési és felülvizsgálati követelményeket.

A Szabályzat megalkotásának célja egy olyan egységes szabályozási környezet kialakítása, amely elősegíti a BSZC elektronikus információs rendszereinek biztonságos működését, támogatja a jogszabályi megfelelést és hozzájárul az oktatási, igazgatási, gazdálkodási és egyéb feladatok zavartalan ellátásához. A Szabályzatban meghatározott követelmények valamennyi szervezeti egységre kötelezők, így alkalmazása során minden szervezeti egység köteles együttműködni az információbiztonsági követelmények teljesítése érdekében.

1.3. Az információbiztonság célkitűzései

A korszerű információbiztonság nem kizárólag informatikai feladat. Az információbiztonság olyan tevékenység, amely magában foglalja:

- a jogszabályi megfelelőség biztosítását;
- a szervezeti és működési folyamatok szabályozását;
- az informatikai rendszerek biztonságos üzemeltetését;
- a fizikai biztonság követelményeit;
- a személyi biztonságot;
- a rendszeres oktatást és tudatosságnövelést;
- a folyamatos ellenőrzést és fejlesztést.

A BSZC minden munkavállalójától elvárja, hogy munkavégzése során az információbiztonság követelményeit saját feladatkörének megfelelően alkalmazza, és a tudomására jutott biztonsági eseményeket késedelem nélkül jelentse.

A BSZC az információbiztonság területén az alábbi célokat határozza meg:

- az elektronikus információk bizalmasságának, sértetlenségének, hitelességének és rendelkezésre állásának biztosítása;
- az oktatási, tanügyi, gazdasági és igazgatási folyamatokat támogató informatikai rendszerek folyamatos működésének biztosítása;
- a személyes adatok jogszerű kezelésének elősegítése;
- a biztonsági események megelőzése, illetve azok hatásainak csökkentése;
- a munkavállalók információbiztonsági tudatosságának folyamatos fejlesztése;
- az informatikai kockázatok folyamatos értékelése és kezelése;
- a biztonsági események gyors felismerése, bejelentése és kivizsgálása;
- a belső szabályozási rendszer folyamatos fejlesztése;
- a BSZC információs vagyonának megőrzése és védelme.

2. Jogszabályi háttér, alapelvek és fogalommeghatározások

2.1. Jogszabályi háttér

A Szabályzat az alábbi jogszabályok figyelembevételével készült:

- Magyarország Alaptörvénye;
- 2019. évi LXXX. törvény a szakképzésről;
- 12/2020. (II. 7.) Korm. rendelet a szakképzésről szóló törvény végrehajtásáról;
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: **Infotv.**);
- az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR);
- 2012. évi I. törvény a munka törvénykönyvéről;
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról;
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról;
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről;
- a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH), valamint a kiberbiztonsági hatóság iránymutatásai, amennyiben azok a Szakképzési Centrum működésére irányadók.

A BSZC a kiberbiztonsági jogszabályok rendelkezéseit a rá irányadó körben alkalmazza. A Szabályzat nem értelmezhető úgy, hogy a 2024. évi LXIX. törvény valamennyi kötelezettsége automatikusan alkalmazandó lenne a Békéscsabai Szakképzési Centrumra.

Amennyiben valamely elektronikus információs rendszer tekintetében jogszabály alapján biztonsági osztályba sorolási kötelezettség áll fenn, a BSZC a rendszert a vonatkozó jogszabályok szerint sorolja be, illetve biztosítja a meghatározott védelmi intézkedések alkalmazását.

2.2. Az információbiztonság alapelvei

A BSZC információbiztonsági tevékenysége az alábbi alapelvekre épül:

- **Jogszerűség:** az információk és elektronikus információs rendszerek kezelése kizárólag jogszabályoknak és belső szabályzatoknak megfelelően történhet.
- **Bizalmasság:** az információhoz kizárólag az arra jogosult személy férhet hozzá.
- **Sértetlenség:** biztosítani kell, hogy az adatok illetéktelenül ne módosuljanak, ne semmisüljenek meg és ne sérüljenek.
- **Rendelkezésre állás:** az elektronikus információs rendszereknek a működéshez szükséges mértékben folyamatosan elérhetőnek kell lenniük.
- **Elszámoltathatóság:** minden felhasználói tevékenységnek visszakövethetőnek kell lennie naplózás vagy egyéb ellenőrzési mechanizmus útján.
- **Legkisebb jogosultság elve:** a felhasználó kizárólag azon jogosultságokkal rendelkezhet, amelyek munkaköri feladatai ellátásához szükségesek.
- **Biztonságtudatosság:** a BSZC valamennyi munkatársa köteles az információbiztonsági szabályokat megismerni és betartani.

2.3. A BSZC információbiztonsági környezete

A BSZC feladatainak ellátása során több, országos működésű elektronikus információs rendszert használ: KRÉTA; VIR; FAR; SZIR; OSAP; KIRA; SAP.

A VIR rendszer használatának feltétele érvényes dolgozói jogviszony, valamint egyedi felhasználónév–jelszó alapú hitelesítés.

A KRÉTA rendszer használatára – jogszabályban és szerződésben meghatározott körben – a duális képzőhelyek képviselői is jogosultak.

A BSZC felhőszolgáltatást nem alkalmaz.

Az intézményi levelezés hivatalos rendszere a **mail.bszc.hu**. Munkavégzéssel összefüggő elektronikus levelezés kizárólag ezen a rendszeren keresztül folytatható.

A BSZC a bizalmas elektronikus állományok továbbítására elsődlegesen jelszóval védett tömörített állományokat alkalmaz.

A munkavállalók saját tulajdonú informatikai eszközeik használatára (BYOD) a BSZC engedélyével jogosultak. A belső hálózathoz történő csatlakozás kizárólag nyilvántartott MAC-cím alapján engedélyezhető.

Tanulók saját eszközzel a belső munkahelyi hálózathoz nem csatlakozhatnak.

2.4. Fogalommeghatározások

A jelen Szabályzat alkalmazásában:

- **Információbiztonság:** azon szervezési, személyi, fizikai és technikai intézkedések összessége, amelyek biztosítják az információk bizalmasságát, sértetlenségét és rendelkezésre állását.
- **Kiberbiztonság:** az elektronikus információs rendszereket érő kibertámadások, jogosulatlan hozzáférések és egyéb biztonsági események megelőzésére, felismerésére és kezelésére irányuló intézkedések összessége.
- **Elektronikus információs rendszer:** minden olyan informatikai rendszer, alkalmazás, hálózat vagy szolgáltatás, amelyet a BSZC feladatainak ellátására használ.
- **Felhasználó:** minden olyan személy, aki a BSZC elektronikus információs rendszerét jogosultan használja.
- **Jogosultság:** valamely elektronikus információs rendszerhez vagy adatállományhoz biztosított hozzáférési lehetőség.
- **Rendszergazda:** a BSZC által kijelölt szakember, aki az informatikai infrastruktúra üzemeltetését, karbantartását és biztonságos működését biztosítja.
- **Információbiztonsági felelős (IBF):** a BSZC munkavállalója, aki koordinálja az információbiztonsági követelmények érvényesülését és figyelemmel kíséri a Szabályzat végrehajtását.
- **Biztonsági esemény (incidens):** minden olyan esemény, amely veszélyezteti vagy veszélyeztetheti az elektronikus információs rendszer biztonságát, az adatok bizalmasságát, sértetlenségét vagy rendelkezésre állását.
- **Naplózás:** a rendszerben végzett műveletek rögzítése a visszakövethetőség és az ellenőrizhetőség biztosítása érdekében.
- **Hitelesítés:** annak ellenőrzése, hogy a rendszerhez hozzáférni kívánó személy jogosult-e az adott rendszer használatára.
- **Távoli hozzáférés:** a BSZC informatikai rendszerének helyszínen kívüli elérése. Távoli rendszergazdai hozzáférés kizárólag üzemeltetési, karbantartási, hibaelhárítási vagy biztonsági célból alkalmazható, a célhoz kötöttség és a személyiségi jogok tiszteletben tartása mellett.

3. A Szabályzat célja, hatálya és kapcsolódása más belső szabályzatokhoz

3.1. A Szabályzat célja

A BSZC Információbiztonsági Szabályzatának célja, hogy meghatározza az információbiztonság és a kiberbiztonság szervezeti, személyi, fizikai és technikai követelményeit, valamint biztosítsa a BSZC által kezelt információk és elektronikus információs rendszerek biztonságos, jogszerű és folyamatos működését.

A Szabályzat célja:

- az elektronikus információs rendszerek bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása;
- a személyes adatok és egyéb védendő információk jogszerű kezelésének elősegítése;
- az informatikai rendszerek biztonságos használatának egységes szabályozása;
- az információbiztonsági kockázatok megelőzése, csökkentése és kezelése;
- a biztonsági események megelőzésének, felismerésének és kezelésének támogatása;

- a munkavállalók és egyéb felhasználók információbiztonsági kötelezettségeinek meghatározása;
- a jogszabályi megfelelőség biztosítása,
- valamint a BSZC működésének támogatása.

3.2. A Szabályzat személyi hatálya

A Szabályzat személyi hatálya kiterjed:

- a BSZC valamennyi munkavállalójára;
- a főigazgatóra;
- a kancellárra;
- a főigazgató-helyettesre;
- a gazdasági vezetőre;
- a tagintézmények igazgatóira és igazgatóhelyetteseire;
- az oktatókra;
- az ügyviteli és gazdasági munkatársakra;
- az információbiztonsági felelősre;
- a rendszergazdákra;
- a megbízási vagy vállalkozási jogviszonyban informatikai szolgáltatást nyújtó személyekre, amennyiben a BSZC informatikai rendszereihez hozzáférnek;
- minden olyan természetes személyre, aki jogosultság alapján a BSZC elektronikus információs rendszereit használja.

A tanulókra a Szabályzat azon rendelkezései alkalmazandók, amelyek az általuk használt elektronikus információs rendszerek, digitális szolgáltatások és informatikai eszközök rendeltetésszerű használatára vonatkoznak.

3.3. A Szabályzat tárgyi hatálya

A Szabályzat tárgyi hatálya kiterjed:

- a BSZC tulajdonában vagy kezelésében lévő informatikai eszközökre;
- a vezetékes és vezeték nélküli hálózatokra;
- a szerverekre és hálózati aktív eszközökre;
- a munkaállomásokra;
- a mobil informatikai eszközökre;
- az elektronikus adathordozókra;
- a papíralapú és elektronikus információkra;
- a biztonsági mentésekre;
- a naplóállományokra;
- az elektronikus levelezési rendszerre;
- a kamerarendszer működéséhez kapcsolódó informatikai eszközökre és digitális felvételekre;
- a BSZC által használt elektronikus információs rendszerekre (KRÉTA, VIR, FAR, SZIR, OSAP, KIRA és SAP).

3.4. Területi hatály

A Szabályzat rendelkezéseit kell alkalmazni:

- a BSZC központi szervezeti egységében;
- a BSZC valamennyi tagintézményében;

- minden olyan helyszínen, ahol a BSZC tulajdonában vagy kezelésében álló informatikai eszközöket használják;
- a munkavégzés helyétől függetlenül, amennyiben a felhasználó a BSZC informatikai rendszereihez jogosultan hozzáfér.

3.5. Időbeli hatály

A Szabályzat a kiadásáról rendelkező vezetői döntésben meghatározott napon lép hatályba. Rendelkezéseit a hatálybalépést követően valamennyi érintett köteles megismerni és alkalmazni.

3.6. Kapcsolódás más belső szabályzatokhoz

A Szabályzat a BSZC belső szabályozási rendszerének része. A Szabályzat rendelkezéseit különösen az alábbi belső szabályzatokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat;
- Adatvédelmi és Adatbiztonsági Szabályzat;
- Adatkezelési Szabályzat;
- Iratkezelési Szabályzat;
- Mesterséges Intelligencia Használatának Szabályzata;
- Kameraszabályzat;
- Munkavédelmi Szabályzat;
- Tűzvédelmi Szabályzat;
- Anyag- és Eszközgazdálkodási Szabályzat;
- Leltárkezelési és Leltározási Szabályzat;
- Belső Ellenőrzési Szabályzat;
- egyéb, az informatikai rendszerek működését érintő belső szabályzatok és vezetői utasítások.

4.Információbiztonsági irányítás és felelősségi rendszer

A BSZC információbiztonsági tevékenysége a vezetői felelősség, a szervezeti együttműködés, a jogszabályi megfelelőség és a folyamatos fejlesztés elvére épül.

A BSZC vezetése biztosítja az információbiztonsági követelmények végrehajtásához szükséges szervezeti, személyi és technikai feltételeket.

4.1. A kancellár feladatai

A kancellár az információbiztonság megvalósításával összefüggésben:

- biztosítja az információbiztonság szervezeti és gazdasági feltételeit;
- gondoskodik a szükséges pénzügyi és tárgyi erőforrások rendelkezésre állásáról;
- támogatja az információbiztonsági fejlesztéseket;
- együttműködik a főigazgatóval és az információbiztonsági felelőssel;
- dönt az informatikai fejlesztésekhez kapcsolódó gazdasági kérdésekben.

4.2. A főigazgató feladatai

A főigazgató:

- felel a Szabályzat kiadásáért, végrehajtásáért és rendszeres felülvizsgálatáért;
- gondoskodik az információbiztonsági követelmények érvényesítéséről;

- kijelöli az információbiztonsági felelőst;
- elrendeli a szükséges intézkedéseket jelentős biztonsági esemény esetén;
- biztosítja a munkavállalók rendszeres információbiztonsági tájékoztatását és oktatását.

4.3. A főigazgató-helyettes és a gazdasági vezető feladatai

A főigazgató-helyettes és a gazdasági vezető saját feladatkörükben:

- közreműködnek a Szabályzat végrehajtásában;
- gondoskodnak az irányításuk alá tartozó szervezeti egységek szabálykövető működéséről;
- jelzik az információbiztonságot érintő kockázatokat;
- együttműködnek az információbiztonsági felelőssel és a rendszergazdákkal.

4.4. A tagintézmények igazgatóinak feladatai

A tagintézmények igazgatói:

- biztosítják a Szabályzat helyi végrehajtását;
- gondoskodnak a munkavállalók tájékoztatásáról;
- együttműködnek a központi szervezeti egységgel;
- haladéktalanul jelzik az információbiztonsági eseményeket;
- támogatják a tagintézményi rendszergazda munkáját.

4.5. Az információbiztonsági felelős (IBF) feladatai

A BSZC saját munkavállalójaként kijelölt információbiztonsági felelős (továbbiakban: **IBF**) koordinálja a Szabályzat végrehajtását.

Feladata:

- figyelemmel kíséri az információbiztonsági követelmények teljesülését;
- közreműködik a Szabályzat elkészítésében és felülvizsgálatában;
- koordinálja az információbiztonsági fejlesztéseket;
- nyilvántartja és értékeli a biztonsági eseményeket;
- közreműködik a kockázatok kezelésében;
- kapcsolatot tart a vezetőkkel és a rendszergazdákkal;
- javaslatot tesz a szükséges biztonsági intézkedésekre;
- közreműködik az információbiztonsági oktatások szervezésében.

Az IBF feladatait a személyes adatok kezelésére vonatkozó szabályok tiszteletben tartásával, a szükségesség és arányosság elvének megfelelően látja el.

4.6. A tagintézményi rendszergazdák feladatai

Minden tagintézményben tagintézményi rendszergazda tevékenykedik.

Feladataik:

- szerverek, hálózatok, valamint az informatikai rendszerek és eszközök üzemeltetése;
- jogosultságok technikai kezelése;
- biztonsági mentések végrehajtása;
- naplózási rendszerek működtetése;
- biztonsági frissítések telepítése;
- biztonsági intézkedések végrehajtása;
- informatikai hibák kezelése;

- vírusvédelem biztosítása;
- a biztonsági események haladéktalan jelzése.

4.7. A felhasználók feladatai

Valamennyi felhasználó köteles:

- a Szabályzat rendelkezéseit megismerni és betartani;
- a részére biztosított felhasználói azonosítót és jelszót bizalmasan kezelni;
- kizárólag a részére biztosított jogosultságokat használni;
- a munkavégzés során a BSZC hivatalos informatikai rendszereit alkalmazni;
- az informatikai eszközöket rendeltetésszerűen használni;
- haladéktalanul bejelenteni minden biztonsági eseményt vagy annak gyanúját;
- együttműködni az információbiztonsági ellenőrzések során.

4.8. Együttműködés

A vezetők, az információbiztonsági felelős, a rendszergazdák és a felhasználók kötelesek együttműködni annak érdekében, hogy a BSZC elektronikus információs rendszerei biztonságosan, folyamatosan és jogszerűen működjenek.

Az információbiztonsági feladatok végrehajtása során minden érintett köteles a tudomására jutott információkat kizárólag a feladatai ellátásához szükséges mértékben kezelni.

4.9. Az adatvédelmi feladatokat ellátó személy feladatai

A BSZC-ben a személyes adatok kezelésével összefüggő szakmai feladatok ellátásáról a mindenkor kijelölt adatvédelmi feladatokat ellátó személy gondoskodik.

Az adatvédelmi feladatokat ellátó személy:

- figyelemmel kíséri az adatvédelmi jogszabályok alkalmazását;
- szakmai támogatást nyújt az adatkezelések megfelelőségéhez;
- közreműködik az adatvédelmi incidensek kivizsgálásában;
- együttműködik az információbiztonsági felelőssel;
- szükség szerint javaslatot tesz a belső szabályzatok módosítására.

5. Informatikai eszközök és elektronikus információs rendszerek használata

Jelen fejezet meghatározza a BSZC tulajdonában, kezelésében vagy használatában álló informatikai eszközök és elektronikus információs rendszerek biztonságos, jogszerű és rendeltetésszerű használatának szabályait.

Az előírások célja az információbiztonság fenntartása, az elektronikus információs rendszerek zavartalan működésének biztosítása, valamint a jogosulatlan hozzáférések, adatvesztések és egyéb biztonsági események megelőzése.

5.1. Az informatikai eszközök használatának általános szabályai

- A BSZC informatikai eszközeit kizárólag a munkavégzéshez, oktatási, ügyviteli vagy egyéb engedélyezett feladatok ellátásához szabad használni.
- Az informatikai eszközöket minden felhasználó köteles rendeltetésszerűen használni, állapotukat megóvni és a biztonságos működés feltételeit biztosítani.

- Az eszközökön kizárólag jogszerűen beszerzett és engedélyezett szoftver használható.
- Jogosulatlan program telepítése, licenc nélküli szoftver használata vagy az informatikai rendszer működésének szándékos módosítása tilos.
- Az informatikai eszközök más részére történő átadása csak az arra jogosult vezető vagy rendszergazda tudtával történhet.

5.2. Elektronikus információs rendszerek használata

A BSZC feladatainak ellátása során az alábbi központi elektronikus információs rendszereket használja:

- KRÉTA;
- VIR;
- FAR;
- SZIR;
- OSAP;
- KIRA;
- SAP.

A rendszerek használata kizárólag a felhasználó részére biztosított jogosultság keretei között történhet.
A VIR rendszer használatának feltétele fennálló dolgozói jogviszony, valamint egyedi felhasználónév és jelszó alkalmazása.
A KRÉTA rendszer használatára – jogszabályban vagy együttműködési megállapodásban meghatározott körben – a duális képzőhelyek képviselői is jogosultak.

5.3. Munkaállomások és mobil eszközök használata

A felhasználó köteles:

- a munkaállomást használaton kívül zárolni;
- az informatikai eszközt illetéktelen személy számára hozzáférhetetlenné tenni;
- az eszközt fizikai sérüléstől megóvni;
- az adatvesztés megelőzése érdekében a kijelölt adattárolási helyeket használni.

Az informatikai eszközök elvesztését, eltulajdonítását vagy sérülését haladéktalanul jelezni kell a közvetlen vezetőnek és a rendszergazdának.

5.4. Saját tulajdonú informatikai eszközök (BYOD) használata

A BSZC a munkavállalók számára engedélyezi saját tulajdonú informatikai eszköz használatát.

A saját tulajdonú eszköz kizárólag akkor csatlakozhat a BSZC informatikai hálózatához, ha:az eszköz megfelel az információbiztonsági követelményeknek.

A saját tulajdonú eszköz használata nem eredményezheti a BSZC elektronikus információs rendszereinek biztonsági kockázatát.

Tanulók saját tulajdonú informatikai eszközzel a BSZC belső munkahelyi hálózatához nem csatlakozhatnak.

5.5. Oktatási célokra történő eszközhasználat

Az iskolai eszközök fő célja az oktatás és a tanulás támogatása. A felhasználók kötelesek az eszközöket kizárólag erre a célra használni.

- **Digitális tananyagok használata**

- ✓ Az iskolai eszközökön tárolt tananyagokat csak az oktatási célok érdekében lehet felhasználni. Azok engedély nélküli másolása, terjesztése vagy módosítása szigorúan tilos.
- ✓ A tanulók számára kiadott feladatokat és anyagokat az iskolai platformokon kell megosztani. Más adatmegosztási módszerek, például privát csoportok használata, csak akkor megengedett, ha azok megfelelnek a GDPR követelményeinek.

- **Online tanórák és távoktatás eszközei**
  - ✓ A távoktatáshoz használt eszközöket és platformokat biztonságosan kell beállítani. Az online tanórákhoz való csatlakozás csak az iskola által jóváhagyott rendszeren keresztül végezhető.
  - ✓ Az online órák során tilos a tanórákat engedély nélkül rögzíteni, illetve azokat harmadik fél számára hozzáférhetővé tenni.

Az intézmény fenntartja a jogot, hogy az iskolai eszközök használatát monitorozza a biztonság érdekében. A rendszergazda köteles havi rendszerességgel ellenőrizni az eszközök állapotát, a telepített szoftverek listáját és a biztonsági naplókat.

A rendszeres ellenőrzések célja az, hogy kiszűrjék az illetéktelen használatot, a vírusfertőzéseket és az egyéb fenyegetéseket.

5.6. Elektronikus levelezés

A BSZC hivatalos elektronikus levelezési rendszere a **mail.bszc.hu**. A munkavégzéssel összefüggő elektronikus levelezést kizárólag ezen a rendszeren keresztül kell folytatni.

Tilos:

- hivatalos ügyintézéshez magán e-mail cím használata;
- bizalmas adatok illetéktelen címzett részére történő továbbítása;
- kéretlen vagy rosszindulatú elektronikus üzenetek továbbküldése.

A felhasználó köteles fokozott körültekintéssel eljárni ismeretlen feladótól érkező elektronikus levelek, csatolmányok és hivatkozások megnyitása során.

5.7. Adattárolás és fájlkezelés

A munkavégzés során keletkező elektronikus dokumentumokat a BSZC által kijelölt adattárolási helyeken kell tárolni. Helyi adattárolás kizárólag indokolt esetben alkalmazható.

Bizalmas vagy védett elektronikus állomány külső továbbítása esetén a BSZC által rendszeresített jelszóval védett tömörített állomány alkalmazandó.

A jelszót az állománytól eltérő kommunikációs csatornán kell megküldeni a címzett részére.

5.8. Internet- és hálózathasználat

A BSZC internetkapcsolata elsődlegesen a munkavégzés és az oktatási feladatok ellátását szolgálja.

Tilos:

- jogellenes tartalmak letöltése vagy terjesztése;
- az informatikai rendszer biztonságát veszélyeztető weboldalak használata;
- jogosulatlan hálózati eszköz csatlakoztatása;

- a hálózati biztonsági beállítások megkerülése.

A belső hálózathoz történő csatlakozás kizárólag a BSZC által jóváhagyott eszközzel történhet.

5.9. Tiltott felhasználói magatartások

Tilos:

- más felhasználó azonosítóját használni;
- más jogosultságával visszaélni;
- jelszót megosztani;
- jogosulatlanul adatot másolni, módosítani vagy törölni;
- informatikai védelmi intézkedéseket megkerülni;
- a rendszergazdai jogosultságokat jogosulatlanul használni;
- a naplózási folyamatokat befolyásolni vagy azok működését akadályozni.

5.10. A felhasználók kötelezettségei

A BSZC elektronikus információs rendszerei kizárólag a Szabályzat által meghatározott követelmények figyelembevételével létrehozott felhasználói fiókkal vehetők igénybe. Minden felhasználói tevékenységnek egyértelműen visszavezethetőnek kell lennie az adott felhasználóra.

Valamennyi felhasználó köteles:

- az informatikai eszközöket a Szabályzatban meghatározottak szerint használni;
- a biztonsági előírásokat betartani;
- a rendszergazda utasításait követni az informatikai biztonságot érintő kérdésekben;
- az észlelt rendellenességet vagy biztonsági eseményt haladéktalanul bejelenteni;
- részt venni az előírt információbiztonsági oktatásokon.

5.11. Mesterséges intelligencián alapuló alkalmazások használata

A BSZC támogatja a mesterséges intelligencián (MI) alapuló alkalmazások felelős és jogszerű használatát a munkavégzés, az oktatás és a tanulás támogatása érdekében.

Az MI-alapú alkalmazások használata során a felhasználók kötelesek betartani az adatvédelmi, információbiztonsági és titoktartási előírásokat, valamint az intézmény külön MI-használati szabályzatában foglaltakat.

Nyilvánosan elérhető mesterséges intelligencia szolgáltatásba **nem tölthető fel**:

- bizalmas és személyes adat;
- KRÉTA, VIR, KIRA, SAP rendszerből származó adat, export, riport vagy kimutatás;
- belső pénzügyi adat;
- szerződések és belső bizalmas dokumentumok;
- felhasználónév, jelszó vagy egyéb hitelesítési adat;
- minden olyan információ, amelynek nyilvánosságra kerülése a BSZC vagy valamely érintett személy jogos érdekét sértheti.

Az MI-eszközök kizárólag olyan célokra használhatók, amelyek nem veszélyeztetik az intézmény információbiztonságát és adatvédelmi kötelezettségeinek teljesítését.

6. Jogosultságkezelés és hozzáférés-kezelés

A jogosultságkezelés során érvényesíteni kell a **legkisebb jogosultság**, a **szükségesség, az arányosság**, valamint a **visszakövethetőség** elvét.

6.1. A jogosultságkezelés alapelvei

A jogosultságok kezelésének alapelvei:

- minden felhasználó egyedi azonosítóval rendelkezik;
- a jogosultság kizárólag munkaköri feladat ellátásához adható;
- egy jogosultság csak a szükséges időtartamra biztosítható;
- a jogosultságokat rendszeresen felül kell vizsgálni;
- a megszűnt vagy indokolatlanná vált jogosultságokat haladéktalanul vissza kell vonni;
- a jogosultságok kiadásának, módosításának és megszüntetésének dokumentálhatónak kell lennie.

6.2. Szerepkör alapú hozzáférés-kezelés

A BSZC elektronikus információs rendszereihez és hálózati erőforrásaihoz történő hozzáférés kizárólag egyedi felhasználói azonosítóval rendelkező, regisztrált felhasználók számára biztosítható.

A felhasználó kizárólag azokhoz az információkhoz, alkalmazásokhoz és informatikai erőforrásokhoz férhet hozzá, amelyek munkaköri feladatainak, tanulmányi jogviszonyának vagy szerződéses kötelezettségeinek ellátásához szükségesek.

A jogosultságok meghatározása során az alábbi felhasználói csoportokat kell figyelembe venni:

- vezetők;
- oktatók;
- nem oktató munkavállalók;
- rendszergazdák;
- informatikai biztonsági felelős;
- tanulók;
- duális képzőhelyek jogosult felhasználói (különösen a KRÉTA rendszer tekintetében);
- külső szolgáltatók és egyéb szerződéses partnerek.

Emelt jogosultság kizárólag dokumentált vezetői jóváhagyással, meghatározott feladat ellátására és a szükséges időtartamra biztosítható

6.3. Jogosultságok igénylése

Új hozzáférési jogosultság kizárólag:

- munkaviszony vagy egyéb jogviszony létesítését követően,
- munkaköri feladat indokoltsága alapján,
- a közvetlen vezető jóváhagyásával,
- valamint a rendszergazda technikai végrehajtásával adható ki.

Az információbiztonsági felelős szükség esetén jogosult a jogosultság kiadásának információbiztonsági szempontú felülvizsgálatára.

6.4. Jogosultságok módosítása és megszüntetése

A jogosultságot módosítani kell:

- munkakör változása esetén;
- szervezeti egység változása esetén;
- új feladatkör ellátása esetén;
- ideiglenes helyettesítés esetén.

A jogosultságot haladéktalanul meg kell szüntetni:

- a jogviszony megszűnésekor;
- a munkakör megszűnésekor;
- a hozzáférés indokának megszűnésekor;
- biztonsági okból elrendelt intézkedés esetén.

A vezető köteles a jogosultság megszüntetését haladéktalanul kezdeményezni.

6.5. Felhasználói azonosítók és hitelesítés

Valamennyi felhasználó részére egyedi felhasználói azonosítót kell biztosítani.

A hitelesítési adatoknak (jelszó) meg kell felelniük az adott informatikai rendszer által meghatározott, illetve a Centrum által előírt biztonsági követelményeknek.

A VIR rendszer használata kizárólag érvényes dolgozói jogviszony és egyedi felhasználónév–jelszó alapú hitelesítés mellett engedélyezett.

A felhasználó köteles:

- felhasználói azonosítóját és jelszavát bizalmasan kezelni;
- a jelszó illetéktelen megismerésének gyanúja esetén azt haladéktalanul megváltoztatni,
- illetve a rendszergazdát értesíteni.

6.6. Emelet szintű jogosultság – többtényezős hitelesítés

Emelt szintű jogosultság kizárólag azon személy részére biztosítható, akinek ez munkaköri feladatai ellátásához elengedhetetlen.

Az emelt jogosultság:

- személyhez kötött;
- nem ruházható át;
- kizárólag a szükséges feladat végrehajtására használható;
- használata naplózható.

Az emelt jogosultsággal rendelkező személy köteles különös gondossággal eljárni az elektronikus információs rendszerek használata során.

Az adminisztrátori, rendszergazdai, valamint egyéb emelt jogosultságot biztosító hozzáférések esetében – amennyiben azt az alkalmazott informatikai rendszer műszaki lehetősége támogatja – többtényezős hitelesítést kell alkalmazni.

A többtényezős hitelesítés történhet:

- hitelesítő alkalmazással;
- egyszer használatos hitelesítési kóddal
- hardveres hitelesítő eszközzel;
- vagy más, a BSZC által jóváhagyott hitelesítési módszerrel.

6.7. Távoli hozzáférés

A rendszergazdai jogosultság kiemelt jogosultságnak minősül. Rendszergazdai távoli hozzáférés kizárólag meghatározott informatikai feladat ellátása érdekében, a szükséges mértékben és a Centrum által engedélyezett technikai megoldással alkalmazható.

A BSZC informatikai hálózatának és eszközeinek üzembiztonsága, folyamatos karbantartása, a technikai hibák gyors elhárítása, valamint a biztonsági események kezelése érdekében a rendszergazda jogosult a BSZC tulajdonában lévő bármely munkahelyi számítógépre távoli asztalkapcsolat kialakítására alkalmas szoftvert (pl. távoli elérést, képernyőmegosztást biztosító kliensprogramokat) telepíteni és futtatni

A távoli hozzáférés:

- kizárólag engedélyezett felhasználó részére biztosítható;
- célhoz kötött;
- időben korlátozható;
- naplózható.

A távoli hozzáférés nem használható a munkavállalók indokolatlan ellenőrzésére vagy személyes adataik jogellenes megismerésére.

6.8. Jogosultságok felülvizsgálata

A jogosultságokat rendszeresen, de legalább évente egy alkalommal felül kell vizsgálni.

A felülvizsgálat célja különösen:

- a szükségtelen jogosultságok megszüntetése;
- a jogosultságok aktualizálása;
- a biztonsági kockázatok csökkentése.

A felülvizsgálatban a szervezeti egység vezetője, az információbiztonsági felelős és a rendszergazda működik együtt.

6.9. Naplózás

A jogosultságok létrehozását, módosítását és megszüntetését dokumentálni kell.

Ahol azt az alkalmazott rendszer műszakilag lehetővé teszi, a jogosultságokkal kapcsolatos rendszergazdai műveleteket naplózni kell.

A naplóállományokhoz kizárólag az arra jogosult személyek férhetnek hozzá.

A naplóadatok kizárólag:

- informatikai üzemeltetési;
- információbiztonsági;
- ellenőrzési;
- jogszabályban meghatározott célból használhatók fel.

6.10. A felhasználók kötelezettségei

A felhasználó köteles:

- kizárólag a saját felhasználói azonosítóját használni;
- jogosultságát rendeltetésszerűen használni;
- minden olyan körülményt jelezni, amely jogosulatlan hozzáférésre vagy jogosultsággal való visszaélésre utalhat.

6.11. Rendkívüli intézkedések

Információbiztonsági esemény vagy annak megalapozott gyanúja esetén a rendszergazda – az információbiztonsági felelős vagy az illetékes vezető értesítése mellett – jogosult a hozzáférés ideiglenes korlátozására vagy felfüggesztésére, ha ez a további károk megelőzéséhez szükséges. Az intézkedésről dokumentált feljegyzést kell készíteni.

7. Adatvédelem és adatbiztonság

Az adatvédelem és az adatbiztonság biztosítása valamennyi vezető, munkavállaló és a BSZC elektronikus információs rendszereit használó személy közös felelőssége.

Az adatkezelés során biztosítani kell az adatok bizalmasságát, sértetlenségét, rendelkezésre állását és szükség szerinti helyreállíthatóságát.

7.1. Az adatkezelés alapelvei

A BSZC a személyes adatok kezelése során az alábbi alapelveket érvényesíti:

- jogszerűség, tisztességes eljárás és átláthatóság;
- célhoz kötött adatkezelés;
- pontosság;
- korlátozott tárolhatóság;
- integritás és bizalmas jelleg;
- elszámoltathatóság.

A személyes adatok kizárólag jogszabályban vagy belső szabályzatban meghatározott célból kezelhetők.

7.2. A személyes adatok védelme

A személyes adatok kezelése során biztosítani kell, hogy azokhoz kizárólag az arra jogosult személyek férjenek hozzá.

A személyes adatokat:

- jogosulatlan hozzáféréstől;
- jogosulatlan módosítástól;
- jogosulatlan továbbítástól;
- véletlen vagy jogellenes törléstől;
- megsemmisüléstől;
- elvesztéstől megfelelő szervezési és technikai intézkedésekkel védeni kell.

A személyes adatok kezelésére vonatkozó részletes szabályokat a BSZC **Adatkezelési**, valamint az **Adatvédelmi és Adatbiztonsági Szabályzata** tartalmazza.

7.3. Az elektronikus adatok biztonsága

Az elektronikus információkat olyan módon kell kezelni, hogy azok:

- hitelessége;
- sértetlensége;
- rendelkezésre állása;
- bizalmassága biztosított legyen.

Az elektronikus adatok kezelése során a BSZC:

- jogosultságkezelést alkalmaz;
- naplózza az arra alkalmas rendszerek biztonsági eseményeit;
- rendszeresen telepíti a biztonsági frissítéseket;
- vírusvédelmi megoldásokat alkalmaz;
- napi rendszerességgel biztonsági mentést készít.

A biztonsági mentések a BSZC központi szerverére történnek.

7.4. Papíralapú dokumentumok védelme

A papíralapú dokumentumokat úgy kell kezelni, hogy azokhoz illetéktelen személy ne férhessen hozzá.

A Békéscsabai Szakképzési Centrumban központi irattár működik, illetve valamennyi tagintézmény saját irattárral rendelkezik.

A már nem szükséges, selejtezhető, személyes adatot tartalmazó dokumentumokat kizárólag az iratkezelési szabályoknak megfelelően, iratmegsemmisítő alkalmazásával vagy azzal egyenértékű biztonságos módon lehet megsemmisíteni.

7.5. Adathordozók kezelése

A hordozható adathordozók használata kizárólag munkavégzési célból engedélyezett.

Pendrive használata megengedett, azonban a felhasználó köteles gondoskodni arról, hogy az azon tárolt adatok ne váljanak illetéktelen személy számára hozzáférhetővé.

Bizalmas vagy védett adat külső adathordozóra történő másolása kizárólag indokolt esetben történhet.

Amennyiben bizalmas adat elektronikus úton kerül továbbításra, a BSZC által rendszeresített jelszóval védett tömörített állomány alkalmazása kötelező.

7.6. Adattovábbítás

Adat kizárólag:

- jogszabály alapján;
- az érintett hozzájárulása alapján, ha az szükséges;
- vagy megfelelő vezetői felhatalmazás alapján továbbítható.

Elektronikus adattovábbítás során biztosítani kell az adatok bizalmasságát és sértetlenségét.

A jelszóval védett állomány jelszavát az állománytól eltérő kommunikációs csatornán kell közölni a címzettel.

7.7. Adatmegőrzés és adattörlés

Az adatokat kizárólag a jogszabályban vagy belső szabályzatban meghatározott ideig lehet megőrizni.

Az adatkezelési cél megszűnését követően az adatokat a vonatkozó jogszabályok és belső szabályzatok szerint törölni, selejtezni vagy archiválni kell.

Az elektronikus adatok törlését úgy kell végrehajtani, hogy azok jogosulatlan személy számára ne legyenek helyreállíthatók.

7.8. Kamerafelvételek kezelése

A BSZC és tagintézményei területén működő elektronikus megfigyelőrendszer által rögzített felvételek kezelése során biztosítani kell a személyes adatok védelmét.

A kamerarendszer működtetésére, a felvételek megőrzési idejére, a hozzáférési jogosultságokra és az érintetti jogok gyakorlására vonatkozó részletes szabályokat a BSZC **Adatvédelmi és Adatbiztonsági Szabályzata**, valamint a **Kameraszabályzata** tartalmazza.

7.9. A munkavállalók adatvédelmi kötelezettségei

Valamennyi munkavállaló köteles:

- a tudomására jutott személyes és egyéb védett adatokat bizalmasan kezelni;
- a munkaköréhez szükséges mértékben adatot kezelni;
- az adatvédelmi és információbiztonsági szabályokat betartani;
- az adatvédelmet vagy adatbiztonságot veszélyeztető eseményt haladéktalanul bejelenteni;
- részt venni az előírt adatvédelmi és információbiztonsági oktatásokon.

7.10. Kapcsolódás a biztonsági események kezeléséhez

Amennyiben a személyes adatok biztonságát érintő esemény következik be, az eseményt a jelen Szabályzat **„Biztonsági események"** című fejezetében meghatározott eljárás szerint kell kezelni.

Szükség esetén az adatvédelmi incidensek kezelésére a GDPR és az Infotv. rendelkezéseit is alkalmazni kell.

8. Fizikai és környezeti biztonság

A fizikai és környezeti biztonsági intézkedések célja:

- az illetéktelen hozzáférések megelőzése;
- az informatikai eszközök sérülésének, elvesztésének vagy eltulajdonításának megakadályozása;
- az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának fenntartása;
- a működés folyamatosságának támogatása.

8.1. Az épületek és helyiségek védelme

A BSZC központi szervezeti egységében és valamennyi tagintézményében biztosítani kell az informatikai eszközök elhelyezésére szolgáló helyiségek megfelelő fizikai védelmét.

Ennek érdekében:

- az informatikai helyiségekhez kizárólag az arra jogosult személyek férhetnek hozzá;
- a munkahelyiségeket használaton kívül zárva kell tartani;
- a kulcsok és belépési jogosultságok kezeléséről az intézmény vezetése gondoskodik;
- az informatikai berendezéseket olyan módon kell elhelyezni, hogy azokhoz illetéktelen személy ne férhessen hozzá.

8.2. Informatikai eszközök fizikai védelme

A BSZC tulajdonában vagy használatában lévő informatikai eszközöket rendeltetésszerűen kell használni és meg kell óvni a sérüléstől, eltulajdonítástól, jogosulatlan használattól és megsemmisüléstől.

A felhasználó köteles:

- a felügyelet nélkül hagyott informatikai eszközt megfelelő védelemmel ellátni;
- hordozható eszközét biztonságosan tárolni;
- az eszköz elvesztését vagy sérülését haladéktalanul jelenteni.

8.3. Szerverek és hálózati eszközök védelme

A BSZC szervereit, hálózati aktív eszközeit és egyéb központi informatikai infrastruktúráját fokozott fizikai védelem mellett kell üzemeltetni.

A központi szerverhelyiség kizárólag az arra feljogosított személyek – különösen a rendszergazda és az információbiztonsági felelős – számára hozzáférhető.

A szerverhelyiség biztonságos üzemeltetését szolgáló műszaki védelem részei:

- **szünetmentes tápegység (UPS)** biztosítja az elektromos energiaellátás átmeneti kiesése esetén az informatikai rendszerek szabályos leállításának, illetve folyamatos működésének lehetőségét;
- **klímaberendezés** gondoskodik a berendezések üzemszerű működéséhez szükséges környezeti feltételek fenntartásáról;
- **mozgásérzékelő rendszer** támogatja a helyiség fizikai védelmét és az illetéktelen behatolás észlelését.

Az épület tűzjelző rendszere a szerverhelyiséghez kapcsolódó közlekedő/folyosó területén érzékelőt tartalmaz, ami hozzájárul az informatikai infrastruktúra biztonságához.

Az informatikai infrastruktúrán végzett karbantartási, konfigurációs vagy egyéb rendszergazdai beavatkozásokat – amennyiben azt a vonatkozó belső eljárásrend előírja – dokumentálni kell.

8.4. Hordozható informatikai eszközök és adathordozók védelme

Laptopok, hordozható adattárolók és egyéb mobil informatikai eszközök használata során különös gondossággal kell eljárni.

A felhasználó köteles:

- megakadályozni az illetéktelen hozzáférést;
- az adathordozó elvesztését vagy eltulajdonítását haladéktalanul jelenteni;
- bizalmas adatot kizárólag a Szabályzatban meghatározott módon továbbítani.

A pendrive használata munkavégzési célból engedélyezett, azonban kizárólag a jelen Szabályzat adatbiztonsági előírásainak betartásával.

8.5. Beléptetési rendszer

A BSZC fizikai biztonságának erősítése érdekében a tagintézmények közül **két intézményben elektronikus beléptetési rendszer működik**.

A beléptetési rendszer elsődleges célja:

- az intézmény területére történő belépések és kilépések szabályozása;
- a tanulók intézményből történő kilépésének ellenőrzése;

- az intézményi vagyon és az elektronikus információs rendszerek fizikai védelmének támogatása.

A beléptetési rendszer a nyári időszakban – az igazgató döntése alapján – az oktatók jelenlétének nyilvántartására is alkalmazható. A jelenléti adatok kezelése során a BSZC biztosítja a vonatkozó adatvédelmi és munkaügyi jogszabályok, valamint a belső adatkezelési és adatvédelmi szabályzatok betartását.

A beléptetési rendszer működtetése során keletkező adatokhoz kizárólag az arra jogosult személyek férhetnek hozzá, felhasználásuk kizárólag a működtetéshez, a biztonsági célok érvényesítéséhez, illetve a jogszabályban vagy belső szabályzatban meghatározott célokhoz szükséges mértékben történhet.

A beléptetési rendszer alkalmazása nem érinti a kamerarendszer működtetésére, illetve a személyes adatok kezelésére vonatkozó külön belső szabályzatok rendelkezéseit.

8.6. Környezeti védelem

Az informatikai eszközök működtetése során törekedni kell arra, hogy azok megfelelő környezeti feltételek között működjenek.

Ennek érdekében biztosítani kell:

- az elektromos hálózat biztonságos használatát;
- a berendezések megfelelő szellőzését;
- a túlzott hőhatás, nedvesség és por elleni védelmet;
- az eszközök rendeltetésszerű elhelyezését.

Az informatikai eszközöket úgy kell elhelyezni, hogy azok ne akadályozzák a biztonságos közlekedést, valamint ne jelentsenek balesetveszélyt.

8.7. Kamerarendszer és fizikai védelem

A BSZC központi épületében és tagintézményeiben elektronikus megfigyelőrendszer működik a személy- és vagyonvédelem, valamint az intézményi vagyon megóvása érdekében.

A kamerarendszer működtetése nem irányulhat a munkavállalók folyamatos ellenőrzésére.

A kamerafelvételek kezelésére, megőrzési idejére, a hozzáférési jogosultságokra és az érintettek jogaira vonatkozó részletes szabályokat a BSZC **Adatvédelmi és Adatbiztonsági Szabályzata**, valamint **Kameraszabályzata** tartalmazza.

8.8. Látogatók és külső személyek belépése

Az informatikai infrastruktúrát érintő helyiségekbe külső személy kizárólag indokolt esetben és az illetékes munkatárs tudtával és kíséretében léphet be. Amennyiben a külső személy az informatikai rendszereken munkát végez, tevékenységét a megbízásának megfelelő keretek között, a szükséges felügyelet mellett kell ellátnia.

8.9. Selejtezés és eszközök kivonása

Az informatikai eszközök selejtezése vagy végleges kivonása előtt gondoskodni kell az azokon található adatok biztonságos törléséről vagy – szükség szerint – az adathordozó fizikai megsemmisítéséről. A selejtezést a BSZC hatályos Anyag- és Eszközgazdálkodási Szabályzata szerint kell végrehajtani.

8.10. A munkavállalók kötelezettségei

Valamennyi munkavállaló köteles:

- megóvni a rábízott informatikai eszközöket;
- betartani a fizikai biztonságra vonatkozó előírásokat;
- rendellenességet vagy vagyonvédelmi eseményt haladéktalanul jelenteni.

9. Kommunikáció- és hálózatbiztonság

A kommunikáció- és hálózatbiztonsági intézkedések célja:

- az elektronikus információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása;
- a jogosulatlan hálózati hozzáférések megelőzése;
- a kibertámadásokkal szembeni védelem erősítése;
- a biztonságos elektronikus kommunikáció feltételeinek megteremtése.

9.1. Hálózati infrastruktúra védelme

A BSZC informatikai hálózatát úgy kell kialakítani és üzemeltetni, hogy biztosítsa az elektronikus információs rendszerek biztonságos működését.

Ennek érdekében:

- a központi informatikai hálózat hardveres tűzfallal védett;
- valamennyi tagintézmény önálló tűzfallal rendelkezik;
- a hálózati eszközök konfigurációját kizárólag arra feljogosított rendszergazda módosíthatja;
- a hálózati konfiguráció módosítását – szükség szerint – dokumentálni kell.

A hálózati védelmi megoldásokat rendszeresen felül kell vizsgálni, és szükség esetén aktualizálni kell.

9.2. Elektronikus levelezés és kommunikáció

A BSZC hivatalos elektronikus levelezési rendszere a **mail.bszc.hu** webmail szolgáltatás.

A munkavállalók szolgálati célú elektronikus levelezésre kizárólag a BSZC által biztosított levelezési szolgáltatást használhatják.

A levelezőrendszer használata során:

- a felhasználó köteles a hozzáférési adatait bizalmasan kezelni;
- bizalmas vagy személyes adatot tartalmazó elektronikus mellékletet a Szabályzatban meghatározott módon kell védeni;
- a hivatalos levelezés során kizárólag a munkavégzéshez kapcsolódó célból kezelhető személyes adat.

A BSZC levelezőprogramként elsősorban **Thunderbird** alkalmazható.

9.3. Internet- és hálózathasználat

Az internet-hozzáférés a munkavégzés, az oktatási feladatok és a BSZC feladatellátásának támogatását szolgálja.

A hálózat használata során tilos:

- jogszabályba ütköző tevékenység végzése;
- a hálózat biztonságát veszélyeztető programok használata;
- jogosulatlan hálózati vizsgálatok vagy behatolási kísérletek végrehajtása;
- a biztonsági védelmi intézkedések megkerülése.

A BSZC hálózatán webszűrés, URL-szűrés és tartalomszűrés működik a biztonsági kockázatok csökkentése érdekében.

9.4. Vezeték nélküli hálózatok

A BSZC vezeték nélküli hálózatait elkülönített jogosultsági szinteken kell működtetni.

Ennek megfelelően:

- külön dolgozói vezeték nélküli hálózat működik;
- külön vendég vezeték nélküli hálózat áll rendelkezésre;
- a tanulók számára biztosított vezeték nélküli hálózat a belső intézményi hálózattól elkülönítetten működik.

A vezeték nélküli hálózatokhoz történő hozzáférést kizárólag az arra jogosult személyek részére lehet biztosítani.

9.5. Távoli hozzáférés

Távoli munkavégzés kizárólag biztonságos kapcsolat alkalmazásával engedélyezhető. A BSZC-ben a távoli hálózati kapcsolódás **VPN-kapcsolaton keresztül** történik.

A VPN-hozzáférés:

- kizárólag engedélyezett felhasználó részére biztosítható;
- személyhez kötött;
- megfelelő hitelesítéshez kapcsolódik;
- használata naplózható.

A kizárólag Távoli Asztal (RDP) alapú közvetlen internetes hozzáférés nem alkalmazható.

9.6. Külső kapcsolatok és elektronikus információs rendszerek

A BSZC által használt elektronikus információs rendszerek – különösen a KRÉTA, VIR, FAR, SZIR, OSAP, KIRA és SAP – kizárólag a meghatározott jogosultságok alapján használhatók.

A KRÉTA rendszerhez a duális képzőhelyek részére biztosított hozzáférések kezelését a rendszer saját jogosultsági rendje és a vonatkozó belső eljárásrend szerint kell biztosítani.

A VIR rendszer használata kizárólag érvényes dolgozói jogviszony fennállása mellett, egyedi felhasználónévvel és jelszóval történhet.

9.7. Kártékony programok elleni védelem

A BSZC elektronikus információs rendszereinek védelme érdekében központilag menedzselt vírusvédelmi rendszer működik.

Az informatikai munkaállomások elsődleges vírusvédelmét az **ESET Endpoint Antivirus** biztosítja.

A felhasználó nem jogosult a vírusvédelmi rendszer kikapcsolására, módosítására vagy működésének akadályozására.

9.8. Hálózati események naplózása

A hálózat biztonságos működésének biztosítása érdekében a BSZC az alkalmazott rendszerek műszaki lehetőségeinek megfelelően naplózza a biztonsági szempontból jelentős hálózati eseményeket.

A naplóállományok kizárólag:

- üzemeltetési;
- információbiztonsági;
- ellenőrzési;
- jogszabályban meghatározott célból használhatók fel.

A naplóadatokhoz kizárólag az arra jogosult személyek férhetnek hozzá.

9.9. A felhasználók kötelezettségei

A hálózat használata során a felhasználó köteles:

- kizárólag a számára engedélyezett hálózati szolgáltatásokat használni;
- a hozzáférési adatait bizalmasan kezelni;
- a hálózat biztonságát veszélyeztető eseményt haladéktalanul bejelenteni;
- a biztonsági frissítések és informatikai intézkedések végrehajtását támogatni;
- a belső hálózatra kizárólag engedélyezett eszközzel csatlakozni.

9.10. Kapcsolódás a biztonsági események kezeléséhez

A kommunikációs vagy hálózati biztonságot érintő eseményeket a jelen Szabályzat **„Biztonsági események"** című fejezete szerint kell kezelni.

A hálózat biztonságát veszélyeztető esemény észlelése esetén a felhasználó köteles haladéktalanul értesíteni a rendszergazdát vagy az információbiztonsági felelőst.

10. Mobil eszközök és saját tulajdonú eszközök (BYOD)

A szabályozás célja, hogy a mobil eszközök használata ne veszélyeztesse a BSZC elektronikus információs rendszereinek, személyes adatainak és egyéb védendő információinak biztonságát.

10.1. Mobil eszközök használata

Mobil informatikai eszköznek minősül:

- notebook;
- okostelefon;
- tablet;
- egyéb hordozható elektronikus eszköz.

A mobil eszközöket kizárólag rendeltetésszerűen és a jelen Szabályzat előírásainak megfelelően lehet használni.

A felhasználó köteles gondoskodni arról, hogy a használatában lévő eszköz ne kerülhessen illetéktelen személy birtokába vagy felügyelet nélküli használatába.

10.2. Saját tulajdonú eszközök (BYOD) használata

A BSZC a munkavállalók saját tulajdonú informatikai eszközeinek használatát munkavégzés céljából engedélyezi.

Ennek feltételei:

- a rendszergazda előzetes engedélye;
- a MAC-cím rögzítése;
- megfelelő vírusvédelmi megoldás alkalmazása;
- a biztonsági beállítások elfogadása.

A saját tulajdonú eszköz használata nem eredményezheti a BSZC elektronikus információs rendszereinek biztonsági kockázatát.

A saját eszköz használata nem mentesíti a munkavállalót a jelen Szabályzatban meghatározott kötelezettségek alól.

10.3. A tanulók saját eszközei

A tanulók saját tulajdonú informatikai eszközei a BSZC belső intézményi hálózatához nem csatlakoztathatók.

A tanulók részére biztosított vezeték nélküli hálózat a belső informatikai hálózattól elkülönítetten működik.

10.4. Távoli munkavégzés mobil eszközzel

A mobil eszközről történő távoli munkavégzés kizárólag biztonságos kapcsolaton keresztül történhet.

A BSZC-ben a távoli hozzáférés VPN-kapcsolat alkalmazásával biztosított.

A felhasználó köteles gondoskodni arról, hogy a VPN-hozzáféréshez használt hitelesítési adatok illetéktelen személy birtokába ne kerüljenek.

10.5. Elektronikus levelezés mobil eszközről

Mobil eszközről történő hivatalos elektronikus levelezés során kizárólag a BSZC hivatalos levelezési rendszere használható.

A szolgálati célú elektronikus levelezés során a felhasználó köteles betartani a jelen Szabályzat elektronikus kommunikációra és adatvédelemre vonatkozó rendelkezéseit.

Bizalmas vagy személyes adatot tartalmazó dokumentum mobil eszközről történő továbbítása során a BSZC által rendszeresített adatvédelmi intézkedéseket kell alkalmazni.

10.6. Mobil adathordozók használata

Mobil adathordozó – különösen pendrive – használata munkavégzési célból megengedett.

A felhasználó köteles:

- az adathordozót biztonságos módon kezelni;
- megakadályozni annak illetéktelen használatát;
- elvesztését vagy eltulajdonítását haladéktalanul bejelenteni.

Bizalmas adat elektronikus adathordozón történő továbbítása során jelszóval védett tömörített állomány alkalmazása kötelező.

10.7. Elveszett vagy eltulajdonított eszközök

Amennyiben a mobil eszköz vagy adathordozó elveszik, eltulajdonítják vagy illetéktelen személy birtokába kerülhetett, a felhasználó köteles azt haladéktalanul bejelenteni:

- közvetlen vezetőjének;
- a rendszergazdának;
- szükség esetén az információbiztonsági felelősnek.

Az eseményt a Szabályzat **„Biztonsági események"** című fejezete szerint kell kezelni.

10.8. A felhasználók kötelezettségei

A mobil eszközt vagy saját tulajdonú eszközt használó munkavállaló köteles:

- az eszközt megfelelő fizikai védelem mellett használni;
- a hozzáférési adatokat bizalmasan kezelni;
- a biztonsági beállítások sértetlenségét megőrizni;
- az operációs rendszer és az alkalmazások biztonsági frissítéseinek telepítését támogatni;
- az információbiztonságot veszélyeztető eseményt haladéktalanul bejelenteni.

11. Mentési és helyreállítási rend

A mentési és helyreállítási intézkedések célja:

- az elektronikus adatok elvesztésének megelőzése;
- a rendszerek működésének mielőbbi helyreállítása;
- a feladatellátás folyamatosságának biztosítása;
- az információbiztonsági kockázatok csökkentése.

11.1. A biztonsági mentések alapelvei

A BSZC gondoskodik az elektronikus információs rendszerek működéséhez szükséges adatok rendszeres biztonsági mentéséről.

A biztonsági mentéseknek biztosítaniuk kell, hogy indokolt esetben a működéshez szükséges adatok helyreállíthatók legyenek.

A mentések készítését úgy kell megszervezni, hogy azok a működés folyamatosságát a lehető legkisebb mértékben befolyásolják.

11.2. A biztonsági mentések rendje

A BSZC rendszeres, legalább napi gyakoriságú biztonsági mentést végez a kijelölt rendszerekről és adatokról. A mentések központi szerverre történnek. Az offline mentés jelenleg nem része a BSZC mentési gyakorlatának

A mentési folyamatot kizárólag az arra feljogosított rendszergazdák kezelhetik és felügyelhetik.

A biztonsági mentésekhez való hozzáférés kizárólag a feladat ellátásához szükséges mértékben biztosítható.

11.3. A mentések védelme

A biztonsági mentéseket úgy kell kezelni, hogy azok:

- illetéktelen személy számára ne legyenek hozzáférhetők;
- sértetlenségük biztosított legyen;
- szükség esetén helyreállítás céljára felhasználhatók legyenek.

A mentések kezelésére ugyanazon adatbiztonsági követelmények irányadók, mint az eredeti adatok kezelésére.

11.4. Helyreállítási eljárás

Adatvesztés, rendszerhiba vagy egyéb rendkívüli esemény bekövetkezése esetén a rendszergazda megvizsgálja a helyreállítás szükségességét és végrehajtja a rendelkezésre álló mentésekből történő adat-visszaállítást.

A helyreállítás során biztosítani kell, hogy:

- kizárólag hiteles mentés kerüljön felhasználásra;
- a helyreállított adatok sértetlensége ellenőrizhető legyen;
- a helyreállítás a lehető legkisebb adatvesztéssel történjen.

Szükség esetén a helyreállításról és annak eredményéről dokumentáció készül.

11.5. Felelősségi rend

A mentési rendszer működtetéséért és felügyeletéért a rendszergazdák felelősek.

Az információbiztonsági felelős jogosult a mentési rend megfelelőségének ellenőrzésére, valamint javaslatot tehet annak fejlesztésére.

A felhasználók kötelesek az általuk észlelt adatvesztést vagy rendellenességet haladéktalanul bejelenteni.

11.6. Rendkívüli események kezelése

Amennyiben az adatvesztés vagy rendszerhiba információbiztonsági eseménnyel, vagy kibertámadással függ össze, a helyreállítási eljárást a jelen Szabályzat **„Biztonsági események kezelése"** című fejezete szerint kell lefolytatni.

A helyreállítás során elsődleges szempont az elektronikus információs rendszerek biztonságának helyreállítása és az esemény további következményeinek megelőzése.

11.7. A mentési rend felülvizsgálata

A BSZC a mentési rendet rendszeresen, valamint jelentősebb informatikai változás vagy biztonsági esemény bekövetkezését követően felülvizsgálja.

A felülvizsgálat során különösen értékelni kell:

- a mentések rendszerességét;
- a helyreállítás eredményességét;
- a mentési folyamat biztonságát;
- a szükséges fejlesztési intézkedéseket.

12. Biztonsági események

A biztonsági esemény kezelésének célja:

- az információbiztonsági kockázatok csökkentése;
- a biztonsági események hatásának mérséklése;
- az elektronikus információs rendszerek működésének mielőbbi helyreállítása;
- a hasonló események jövőbeni megelőzése.

12.1. Biztonsági esemény fogalma

Biztonsági eseménynek minősül minden olyan esemény vagy körülmény, amely veszélyezteti vagy veszélyeztetheti a BSZC elektronikus információs rendszereinek, adatainak vagy informatikai szolgáltatásainak bizalmasságát, sértetlenségét vagy rendelkezésre állását.

Biztonsági eseménynek tekintendő:

- jogosulatlan hozzáférési kísérlet;
- felhasználói fiók illetéktelen használata;
- vírusfertőzés vagy egyéb kártékony program észlelése;
- adathordozó vagy informatikai eszköz elvesztése, vagy eltulajdonítása;
- személyes adat jogosulatlan megismerése, módosítása vagy törlése;
- szolgáltatáskimaradás vagy rendszerhiba, amely információbiztonsági kockázatot jelent;
- informatikai rendszer elleni kibertámadás gyanúja;
- a jelen Szabályzat előírásainak súlyos megsértése.

12.2. Bejelentési kötelezettség

A BSZC valamennyi munkavállalója köteles a tudomására jutott vagy általa észlelt biztonsági eseményt haladéktalanul bejelenteni.

A bejelentést elsősorban:

- a közvetlen vezető részére;
- a rendszergazda részére;
- szükség szerint az információbiztonsági felelős részére kell megtenni.

A bejelentés elmulasztása vagy indokolatlan késedelme a Szabályzat megsértésének minősülhet.

12.3. A biztonsági esemény kivizsgálása

A bejelentést követően a rendszergazda és – szükség szerint – az információbiztonsági felelős megvizsgálja:

- az esemény jellegét;
- az érintett informatikai rendszereket;
- az érintett adatok körét;
- a bekövetkezett vagy várható következményeket;
- a szükséges azonnali intézkedéseket.

A vizsgálat során biztosítani kell, hogy az esemény kivizsgálása során keletkező információk kizárólag az arra jogosult személyek számára legyenek hozzáférhetők.

12.4. A biztonsági esemény kezelése

A biztonsági esemény jellegétől függően az alábbi intézkedések alkalmazhatók:

- az érintett felhasználói jogosultság ideiglenes korlátozása vagy felfüggesztése;
- az érintett eszköz vagy rendszer elkülönítése;
- jelszó módosítása;
- vírusmentesítés;
- adat-visszaállítás biztonsági mentésből;
- a sérülékenység megszüntetése;
- a szolgáltatás biztonságos helyreállítása.

A szükséges intézkedéseket a lehető legrövidebb időn belül végre kell hajtani.

12.5. Dokumentálás

A jelentősebb biztonsági eseményekről dokumentációt kell készíteni. A dokumentáció tartalmazza:

- az esemény időpontját;
- a bejelentés időpontját;
- az esemény rövid leírását;
- az érintett rendszereket;
- a megtett intézkedéseket;
- a helyreállítás időpontját;
- szükség esetén a megelőző intézkedésekre vonatkozó javaslatokat.

Az incidensdokumentációt az információbiztonsági nyilvántartás részeként kell kezelni.

12.6. Személyes adatokat érintő események

Amennyiben a biztonsági esemény személyes adatokat érint vagy érinthet, az eseményt haladéktalanul jelezni kell az adatvédelmi feladatokat ellátó személy részére.

A személyes adatok megsértésével járó eseményeket a GDPR, az Infotv., valamint a BSZC **Adatvédelmi és Adatbiztonsági Szabályzata** szerint kell kezelni.

Szükség esetén meg kell vizsgálni, hogy fennáll-e hatósági bejelentési vagy érintetti tájékoztatási kötelezettség.

12.7. A biztonsági esemény lezárása és megelőző intézkedések

Az incidens lezárását követően értékelni kell:

- az esemény kiváltó okát;
- az alkalmazott intézkedések eredményességét;
- a hasonló események megelőzésének lehetőségeit.

Szükség esetén kezdeményezni kell:

- a Szabályzat módosítását;
- a technikai védelem fejlesztését;
- a felhasználók tájékoztatását vagy oktatását;
- az informatikai eljárásrend módosítását.

13. Ellenőrzés, képzés és szankciók

Az ellenőrzések célja annak vizsgálata, hogy a Szabályzat rendelkezései a gyakorlatban megfelelően érvényesülnek-e, valamint, hogy az esetleges hiányosságok feltárása és megszüntetése megtörténjen.

13.1. Belső ellenőrzés

A BSZC jogosult a Szabályzat rendelkezéseinek betartását rendszeresen vagy szükség szerint ellenőrizni. Az ellenőrzés kiterjedhet:

- az informatikai eszközök rendeltetésszerű használatára;
- a felhasználói jogosultságok jogszerűségére;
- a hozzáférés-kezelési szabályok betartására;

- a biztonsági mentések végrehajtására;
- a naplózási és incidenskezelési eljárások alkalmazására;
- az adatvédelmi és információbiztonsági előírások teljesülésére.

Az ellenőrzéseket a feladat- és hatáskörrel rendelkező vezetők, az információbiztonsági felelős, a rendszergazdák, valamint – feladatkörének megfelelően – a belső ellenőrzés végezheti.

13.2. Információbiztonsági oktatás és tudatosítás

A BSZC kiemelt feladatának tekinti a munkavállalók információbiztonsági tudatosságának fejlesztését.

Ennek érdekében:

- minden új munkavállaló részére a munkába állást követően információbiztonsági tájékoztatást kell biztosítani;
- a munkavállalók részére rendszeres információbiztonsági oktatást kell szervezni;
- jelentős jogszabályi vagy informatikai változás esetén soron kívüli tájékoztatás tartható;
- szükség esetén célzott oktatás rendelhető el egyes szervezeti egységek vagy felhasználói csoportok részére.

Az oktatás megtörténtét dokumentálni kell.

13.3. A munkavállalók kötelezettségei

A munkavállaló köteles:

- a Szabályzat rendelkezéseit megismerni és betartani;
- az előírt oktatáson részt venni;
- az információbiztonságot veszélyeztető eseményt haladéktalanul bejelenteni;
- az ellenőrzések során együttműködni.

13.4. Szabályszegések és jogkövetkezmények

A Szabályzat megsértése esetén – a jogsértés jellegétől és súlyától függően – a munkáltató a hatályos jogszabályok, különösen a **Munka Törvénykönyve**, a **szakképzésről szóló jogszabályok**, valamint a BSZC belső szabályzatai alapján intézkedést alkalmazhat.

Az intézkedés lehet:

- figyelemfelhívás vagy szóbeli tájékoztatás;
- írásbeli figyelmeztetés;
- a jogosultság ideiglenes korlátozása vagy visszavonása;
- ismételt információbiztonsági oktatás elrendelése;
- munkajogi következmények alkalmazása;
- szükség esetén polgári jogi, szabálysértési vagy büntetőeljárás kezdeményezése.

Az alkalmazott intézkedésnek minden esetben arányban kell állnia a szabályszegés jellegével, súlyával és következményeivel.

13.5. Adatvédelmi és információbiztonsági együttműködés

Amennyiben az ellenőrzés során személyes adatokat érintő hiányosság vagy adatvédelmi incidens gyanúja merül fel, az információbiztonsági felelős együttműködik az adatvédelmi feladatokat ellátó személlyel.

Szükség esetén közösen tesznek javaslatot a szükséges szervezési, technikai vagy szabályozási intézkedésekre.

13.6. Nyilvántartás és dokumentálás

Az ellenőrzésekről, oktatásokról és jelentősebb intézkedésekről dokumentációt kell vezetni. A dokumentáció tartalmazza:

- az ellenőrzés vagy oktatás időpontját;
- a résztvevők körét;
- az ellenőrzés megállapításait;
- a szükséges intézkedéseket;
- az intézkedések végrehajtásának felelősét és határidejét.

A dokumentációt a vonatkozó iratkezelési és adatvédelmi szabályok szerint kell megőrizni.

14. Záró rendelkezések

14.1. A Szabályzat jóváhagyása

Az **Információbiztonsági Szabályzatot** a Békéscsabai Szakképzési Centrum a vonatkozó jogszabályok és belső szabályzatok alapján adja ki.

A Szabályzat kiadására és módosítására a BSZC hatályos szervezeti és működési szabályai szerint jogosult vezető rendelkezése alapján kerül sor.

14.2. Hatálybalépés

Jelen Szabályzat **2026 év szeptember hó 01. napján** lép hatályba.

A Szabályzat hatálybalépésével egyidejűleg hatályát veszti a Békéscsabai Szakképzési Centrum korábbi Informatikai Biztonsági Szabályzata, valamint minden olyan belső rendelkezés, amely jelen Szabályzattal ellentétes.

A jelen Szabályzat nem érinti azon belső szabályzatok hatályát, amelyekre e Szabályzat kifejezetten hivatkozik.

14.3. A Szabályzat megismerése

A Szabályzatot a BSZC valamennyi érintett munkavállalója számára hozzáférhetővé kell tenni.

Az érintett munkavállalók kötelesek a Szabályzat rendelkezéseit megismerni és munkavégzésük során betartani.

A Szabályzat megismerésének tényét a munkáltató által meghatározott módon dokumentálni kell.

14.4. Felülvizsgálat

Jelen Szabályzatot rendszeresen, de legalább az alábbi esetekben felül kell vizsgálni:

- jogszabályváltozás esetén;
- szervezeti átalakulás esetén;
- új informatikai rendszer bevezetésekor;
- súlyos vagy ismétlődő biztonsági eseményt követően;
- belső vagy külső ellenőrzés megállapításai alapján.

A felülvizsgálat során gondoskodni kell arról, hogy a Szabályzat megfeleljen a hatályos jogszabályoknak, a BSZC működésének és az információbiztonsági kockázatoknak.

14.5. Mellékletek kezelése

A jelen Szabályzat mellékletei a Szabályzat elválaszthatatlan részét képezik.

A mellékletek célja, hogy egységes eljárásrendet, nyomtatványokat és dokumentációs mintákat biztosítsanak a BSZC információbiztonsági követelményeinek gyakorlati végrehajtásához.

A mellékletek alkalmazása – eltérő rendelkezés hiányában – a Szabályzat hatálya alá tartozó valamennyi szervezeti egységre és érintett személyre kötelező.

A mellékletek tartalma jogszabályváltozás, szervezeti változás vagy informatikai fejlesztés esetén – a Szabályzat rendelkezéseivel összhangban – felülvizsgálható és aktualizálható.

A mellékletek kitöltött példányait a vonatkozó iratkezelési, adatvédelmi és adatbiztonsági szabályok szerint kell kezelni és megőrizni.

1.számú melléklet: Információbiztonsági esemény/incidens bejelentő lap

1. A bejelentés alapadatai

Megnevezés	Kitöltendő adat
Bejelentés dátuma/időpontja	
Bejelentő neve	
Munkakör	
Szervezeti egység/tagintézmény	
Elérhetőség (telefon, e-mail)	

2. Az esemény adatai

Megnevezés	Kitöltendő adat
Az esemény észlelésének időpontja	
Az esemény helye	
Az esemény rövid megnevezése	

3. Az esemény részletes leírása

Kérjük röviden ismertesse:

- mi történt;
- hogyan észlelte az eseményt;
- milyen rendszereket vagy adatokat érinthet.

.....

.....

.....

.....

.....

.....

4. Érintett informatikai rendszerek

Jelölje az érintett rendszereket:

☐ KRÉTA
☐ VIR
☐ FAR
☐ SZIR
☐ OSAP
☐ KIRA
☐ SAP
☐ mail.bszc.hu
☐ Munkaállomás
☐ Laptop
☐ Mobiltelefon
☐ Hálózati eszköz
☐ Szerver
☐ Egyéb:

5. Az esemény jellege

☐ Jogosulatlan hozzáférési kísérlet
☐ Jelszóval kapcsolatos esemény
☐ Vírusfertőzés
☐ Adathalász e-mail
☐ Eszköz elvesztése
☐ Eszköz eltulajdonítása
☐ Rendszerleállás
☐ Adatvesztés
☐ Személyes adatot érintő esemény
☐ Egyéb:

6. Azonnali intézkedések

Milyen intézkedések történtek?
☐ Eszköz leválasztása a hálózatról
☐ Jelszó módosítása
☐ Rendszergazda értesítése
☐ Információbiztonsági felelős értesítése
☐ Adatvédelmi tisztviselő / adatvédelmi feladatokat ellátó személy értesítése
☐ Egyéb:
.....

7. Az esemény várható hatása

☐ Nem okozott működési zavart
☐ Kisebb működési zavar
☐ Jelentős működési zavar
☐ Adatvesztés
☐ Személyes adat érintett
☐ Nem ismert

8. Intézkedő személy

Név	Beosztás	Intézkedés

9. Az esemény kivizsgálásának eredménye

(A rendszergazda / információbiztonsági felelős tölti ki.)

Az esemény oka:

.....

.....

A megtett intézkedések:

.....

.....

.....

Szükséges további intézkedések:

.....

.....

10. Az esemény lezárása

Megnevezés	Kitöltendő adat
Az esemény lezárásának időpontja	
A helyreállítás megtörtént	☐ Igen ☐ Nem
További intézkedés szükséges	☐ Igen ☐ Nem

11. Jóváhagyás

Név	Beosztás	Aláírás	Dátum
Rendszergazda			
Információbiztonsági felelős			
Szükség esetén adatvédelmi feladatokat ellátó személy			

2.számú melléklet: Titoktartási és információbiztonsági nyilatkozat

1. A nyilatkozattevő adatai

Név: .....

Munkakör / beosztás: .....

Szervezeti egység / tagintézmény: .....

Jogviszony típusa

☐ munkaviszony
☐ megbízási jogviszony
☐ vállalkozási jogviszony
☐ egyéb:
.....

2. Nyilatkozat

Alulírott kijelentem, hogy munkám során tudomásomra juthatnak olyan adatok, információk és dokumentumok, amelyek a Békéscsabai Szakképzési Centrum működésével, munkavállalóival, tanulóival, partnereivel, valamint elektronikus információs rendszereivel kapcsolatosak.

Kötelezettséget vállalok arra, hogy

1. a tudomásomra jutott személyes adatokat, üzemi, gazdasági, szervezeti, oktatási és informatikai információkat kizárólag a munkaköri feladataim ellátásához szükséges mértékben használom fel;
2. a tudomásomra jutott adatokat jogosulatlan személy részére nem adom át, nem teszem hozzáférhetővé, és azokat kizárólag jogszerű célból kezelem;
3. betartom a BSZC Információbiztonsági Szabályzatának, Adatvédelmi és Adatbiztonsági Szabályzatának, valamint egyéb kapcsolódó belső szabályzatainak rendelkezéseit;
4. a részemre biztosított felhasználói azonosítókat, jelszavakat és hozzáférési jogosultságokat kizárólag saját magam használom;
5. gondoskodom arról, hogy munkavégzésem során illetéktelen személy intézményi adatokhoz vagy információkhoz ne férhessen hozzá;
6. a papíralapú és elektronikus dokumentumokat a vonatkozó belső szabályzatoknak megfelelően kezelem és tárolom;
7. biztonsági esemény vagy adatvédelmi incidens észlelése esetén haladéktalanul értesítem közvetlen vezetőmet, az informatikai biztonsági felelőst vagy a rendszergazdát;
8. tudomásul veszem, hogy a titoktartási kötelezettség a jogviszony megszűnését követően is fennmarad mindaddig, amíg az érintett információ nyilvánosságra nem kerül vagy jogszabály eltérően nem rendelkezik.

3. Információbiztonsági kötelezettségvállalás

Kijelentem, hogy

- az intézményi informatikai eszközöket kizárólag rendeltetésszerűen használom;

- az elektronikus információs rendszerek használata során betartom a jogosultságkezelési és hozzáférés-kezelési szabályokat;
- kizárólag engedélyezett informatikai eszközt és szoftvert használok;
- saját tulajdonú eszközt kizárólag a vonatkozó BYOD szabályok betartásával csatlakoztatok az intézményi hálózathoz;
- adathordozót csak a Szabályzat rendelkezéseinek megfelelően használok;
- az intézményi elektronikus levelezés során a kötelező levelezési rendszert (mail.bszc.hu) használom;
- gondoskodom a rám bízott informatikai eszközök fizikai védelméről.

4. Tudomásul veszem

Tudomásul veszem, hogy

- a titoktartási kötelezettség megszegése munkajogi, polgári jogi, adatvédelmi vagy büntetőjogi következményeket vonhat maga után;
- a személyes adatok jogosulatlan kezelése a hatályos jogszabályok alapján jogkövetkezménnyel járhat;
- a Szabályzat megsértése fegyelmi vagy munkáltatói intézkedést eredményezhet;
- a BSZC jogosult a belső szabályzatok betartását ellenőrizni.

5. Nyilatkozat

Kelt: .....

Aláírás: .....

6. Munkáltatói igazolás

Igazolom, hogy a munkavállaló részére a szükséges információbiztonsági tájékoztatás megtörtént.

Vezető neve: .....

Beosztása: .....

Dátum: .....

Aláírás: .....

3.számú melléklet: Informatikai eszköz átadás-átvétel jegyzőkönyv

1. Az átadás-átvétel adatai

Átadás dátuma: .....

Átvétel helye: .....

2. Az átadó adatai

Név: .....

Beosztás: .....

Szervezeti egység: .....

3. Az átvevő adatai

Név: .....

Munkakör: .....

Szervezeti egység / tagintézmény: .....

Telefonszám: .....

E-mail cím: .....

4. Átadott informatikai eszköz(ök)

Eszköz pontos megnevezése	Eszköz szám (SAP)	Gyári szám	Mennyiség	Mennyiségi egység

5. Telepített intézményi szoftverek

☐ Windows
☐ Microsoft Office
☐ Thunderbird
☐ ESET Endpoint Antivirus
☐ VPN kliens
☐ Távoli adminisztrációhoz szükséges program
☐ Egyéb

6. Az eszköz állapota átadáskor

☐ Hibátlan

☐ Rendeltetésszerű használatra alkalmas

☐ Használatot nem akadályozó esztétikai sérülés

☐ Javítást igényel

Leírás:

.....

.....

7. Az átvevő nyilatkozata

Alulírott kijelentem, hogy

1. az informatikai eszközt rendeltetésszerű használatra alkalmas állapotban vettem át;
2. az eszközt kizárólag munkaköri feladataim ellátására használom;
3. az eszközt harmadik személy részére nem adom át a munkáltató előzetes engedélye nélkül;
4. az intézményi felhasználóneveket és jelszavakat bizalmasan kezelem;
5. gondoskodom az eszköz fizikai védelméről;
6. elvesztés, lopás vagy biztonsági esemény esetén haladéktalanul értesítem közvetlen vezetőmet és a rendszergazdát;
7. az eszköz meghibásodását vagy sérülését késedelem nélkül bejelentem;
8. munkaviszonyom megszűnésekor vagy a munkáltató rendelkezésére az eszközt hiánytalanul visszaszolgáltatom;
9. megismertem és magamra nézve kötelezőnek ismerem el a Békéscsabai Szakképzési Centrum Információbiztonsági Szabályzatának rendelkezéseit

Átadó	**Átvevő**
Név:	Név: .....
Aláírás:	Aláírás: .....
Dátum:	Dátum: .....

8. Visszavétel

Visszavétel időpontja:

.....

Az eszköz állapota:

☐ Hibátlan

☐ Rendeltetésszerű használatra alkalmas

☐ Sérült

☐ Hiányos

Hiányzó tartozék:

.....

Sérülés leírása:

.....

Adatok törlése megtörtént:

☐ Igen
☐ Nem

Rendszergazda neve: .....

Aláírás: .....

Átadó

Név: .....

Aláírás: .....

Dátum: .....

Átvevő

Név: .....

Aláírás: .....

Dátum: .....

4.számú melléklet: Mentési és helyreállítási ellenőrzési jegyzőkönyv

1. Az ellenőrzés adatai

A jegyzőkönyv száma: .....

Az ellenőrzés időpontja: .....

Az ellenőrzés helye: .....

Ellenőrzést végző személy: .....

Beosztása: .....

2. Az ellenőrzés tárgya

Érintett informatikai rendszer(ek)

☐ KRÉTA
☐ VIR
☐ FAR
☐ SZIR
☐ OSAP
☐ KIRA
☐ SAP
☐ Levelezőrendszer (mail.bszc.hu)
☐ Fájlszerver
☐ Egyéb: .....

3. A mentés adatai

Mentés dátuma: .....

Mentés típusa:
☐ Teljes mentés
☐ Növekményes mentés
☐ Egyéb: .....

Mentési hely:
☐ Központi szerver
☐ Egyéb: .....

Mentés sikeresen lefutott:
☐ Igen
☐ Nem
Amennyiben nem: .....

4. Helyreállítási próba

Helyreállítás célja:

☐ Tervezett ellenőrzés
☐ Rendszerteszt
☐ Incidens utáni visszaállítás
☐ Egyéb .....

A visszaállítás során ellenőrzött adatok:

☐ Dokumentumok
☐ Adatbázis
☐ Levelezés
☐ Konfigurációs állományok
☐ Felhasználói adatok
☐ Egyéb .....

5. A helyreállítás eredménye

A helyreállítás
☐ teljes mértékben sikeres volt.
☐ részben sikeres volt.
☐ sikertelen volt.

Helyreállítás időtartama: .....

Visszaállított adatok teljessége:

☐ Teljes
☐ Részleges
☐ Nem megfelelő

Az adatok sértetlensége ellenőrizve:

☐ Igen
☐ Nem

A rendszer rendeltetésszerű működése helyreállt:

☐ Igen
☐ Nem

6. Megállapítások

.....

.....

.....

7. Feltárt hibák

☐ Nem került feltárásra hiba.
☐ Az alábbi hibák kerültek megállapításra:

.....

.....

8. Szükséges intézkedések

Intézkedés	Felelős	Határidő	Teljesítés

9. Nyilatkozat

Alulírott kijelentem, hogy

- a mentési folyamat ellenőrzését a vonatkozó belső szabályzat szerint végeztem el;
- a helyreállítási próbát dokumentált módon végrehajtottam;
- a jegyzőkönyvben szereplő adatok a valóságnak megfelelnek.

Ellenőrzést végző

Név: .....

Aláírás: .....

Dátum: .....

Informatikai biztonsági felelős (amennyiben érintett)

Név: .....

Aláírás: .....

Dátum: .....

5.számú melléklet: Információbiztonsági oktatás jelenléti íve és nyilatkozata

1. Az oktatás adatai

Oktatás megnevezése:

☐ Belépő munkavállalók információbiztonsági oktatása
☐ Éves ismétlő oktatás
☐ Rendkívüli oktatás
☐ Informatikai rendszer változásához kapcsolódó oktatás
☐ Egyéb: .....

Oktatás időpontja: .....

Oktatás helyszíne: .....

Oktatás időtartama: .....

Oktató neve: .....

Beosztása: .....

2. Az oktatás témakörei

Az oktatás során ismertetésre kerültek különösen az alábbi témák:

☐ Információbiztonsági Szabályzat
☐ Jogosultságkezelés
☐ Jelszókezelés
☐ Elektronikus levelezés biztonsága
☐ KRÉTA, VIR, FAR, SZIR, OSAP, KIRA, SAP rendszerek biztonságos használata
☐ mail.bszc.hu levelező rendszer használata
☐ VPN használata
☐ Mobil eszközök és BYOD szabályai
☐ Adathordozók használata
☐ Biztonsági mentések
☐ Fizikai biztonság
☐ Adatvédelmi incidensek
☐ Információbiztonsági események bejelentése
☐ Egyéb: .....

3. Jelenléti ív

Sor-szám	Név	Munkakör	Taginézmény/szervezeti egység	Aláírás

(szükség esetén bővíthető)

4. A résztvevő nyilatkozata

Alulírott kijelentem, hogy

- részt vettem a Békéscsabai Szakképzési Centrum információbiztonsági oktatásán;
- megismertem az **Információbiztonsági Szabályzat** rám vonatkozó rendelkezéseit;
- megismertem a felhasználói kötelezettségeket, különösen a jogosultságkezelésre, jelszóhasználatra, elektronikus levelezésre, adatvédelemre és incidens-bejelentésre vonatkozó szabályokat;
- vállalom, hogy munkám során az intézményi informatikai rendszereket kizárólag rendeltetésszerűen használom;
- tudomásul veszem, hogy a Szabályzat megszegése munkajogi, adatvédelmi vagy egyéb jogkövetkezményekkel járhat;
- vállalom, hogy információbiztonsági esemény vagy adatvédelmi incidens észlelése esetén azt haladéktalanul bejelentem.

5. Az oktató nyilatkozata

Igazolom, hogy a jelenléti íven szereplő személyek részére az oktatást megtartottam, az oktatás során a fenti témakörök ismertetésre kerültek, és a résztvevők részére lehetőséget biztosítottam kérdések feltevésére.

Oktató neve: .....

Beosztása: .....

Aláírás: .....

Dátum: .....

6.számú melléklet: Nyilatkozat az Információbiztonsági Szabályzat megismeréséről

Kijelentem, hogy a Békéscsabai Szakképzési Centrum Információbiztonsági Szabályzatát megismertem, annak rendelkezéseit megértettem, azokat magamra nézve kötelezőnek ismerem el, vállalom azok maradéktalan betartását.

Dátum: .....

Intézmény: .....

NÉV	BEOSZTÁS	ALÁÍRÁS