Adatbiztonsági Szabályzat

2018.

1. Bevezetés

A szervezet neve: **Szegedi Közlekedési Kft.**
Székhelye: **6720 Szeged, Zrínyi u. 4-8.**

Ez az Adatbiztonsági Szabályzat (a továbbiakban: Szabályzat) a Szegedi Közlekedési Kft. (a továbbiakban: SZKT) ügyvezető igazgatója által, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény alapján; és a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló az **Európai Parlament és a Tanács (EU) 2016/679 Rendeletének (GDPR)** rendelkezéseire figyelemmel került kiadásra.

A szabályozás alapvető célja az informatikai rendszerek és a tárolt adatok biztonságának megőrzéséhez szükséges intézkedések rögzítése. Ez alapvető feltétele az intézkedések végrehajthatóságának, ellenőrizhetőségének, és szükség esetén a szankcionálhatóságnak.

A Szabályzat egy olyan intézkedés együttes, amely az SZKT szervezetén belül működtetett informatikai rendszerekre vonatkozóan tartalmazza:

- a biztonsági intézkedéseket, a biztonságos számítógépes adatkezeléshez szükséges tevékenységeket és előírásokat,
- a munkatársak részéről a számítógépes adatkezelési rendszer üzemeltetésével kapcsolatos tevékenységeket, biztonsági előírásokat és személyi elvárásokat,
- szervesen illeszkedik a hatályos jogszabályokhoz és az SZKT egyéb működési és ügyrendi előírásaihoz.

Az eljárási utasítás részét képezi az adat és dokumentumkezelés, a jogosultságkezelés, a mentési eljárások és az adatvédelem.

A munkaköri feladatokat és a munkafolyamatok pontos ismertetését a munkavállalók munkaköri leírásai tartalmazzák. Az SZKT informatikai üzemeltetési feladatait a Számítástechnikai Üzemeltetési Szabályzat tartalmazza.

2. A szabályzat minősítése

A Szabályzat minősítését az informatikai rendszerek biztonsági osztályba sorolásának figyelembe vételével az SZKT ügyvezető igazgatója határozza meg. Az SZKT által működtetett informatikai rendszerek globális minősítése: **IV – F (Fokozott biztonsági osztály).**

3. A Szabályzat elérhetővé tétele

Jelen Szabályzatot az SZKT Dolgozói Információs Rendszerében (a továbbiakban: DIR), valamint az SZKT honlapján (www.szkt.hu) az „Adatvédelmi politika és tájékoztatók” menüpontban elérhetővé kell tenni.

A Szabályzat törzspéldányát, amely nyomtatott formában, eredeti aláírásokkal van ellátva, minden esetben az Ügyvezetői Titkárságon kell őrizni, ahol szerkeszthető formátumban, elektronikusan is rendelkezésre áll.

4. A Szabályzat hatálya

Területi hatály: **6720 Szeged, Zrínyi u. 4-8.**
6724 Szeged, Bakay N. u. 35. egyben Pulcz u. 48.
6720 Szeged, Deák F u. 31.
6724 Szeged, Körtöltés u. 35. egyben Csáky u. 5-6.
6720 Szeged, Arany János u. 5.
6728 Szeged, Bajai út, Regionális Repülőtér

A Szabályzat területi hatálya kiterjed továbbá a Szegedi Közlekedési Kft. üzemeltetésében lévő minden egyéb szolgáltatási helyszínre.

Időbeli hatály: jelen Szabályzat a kiadás napján lép hatályba és visszavonásig alkalmazandó.

Személyi hatály: jelen Szabályzat hatálya kiterjed az SZKT-val munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban álló valamennyi természetes személyre, jogi személyre, és jogi személyiséggel nem rendelkező szervezetre.

Tárgyi hatály: jelen Szabályzat hatálya kiterjed az SZKT által üzemeltetett valamennyi informatikai rendszerre, a rendszerekkel kapcsolatos teljes adatkezelési és informatikai folyamatra, valamint a kapcsolódó informatikai eszközre és szoftverre.

5. Fogalmi meghatározások

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

2) **Adatállomány:** valamely informatikai rendszerben lévő, logikailag összetartozó adatok csoportja, amelyet egy névvel jelölnek.

3) **Adatátvitel:** bitek vagy bájtok sorozatának küldése egy helyről egy másik helyre, számos technológia, többek között a rézhuzal, optikai szál, lézer, rádió vagy az infravörös fény igénybe vételével.

4) **Adatbiztonság:** az adatokhoz való jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás elleni intézkedések együttes rendszere.

5) **Adatmentés:** azon intézkedések összessége, amelyek eredményeként a számítógépes adatokról meghatározott időszakonként (naponta, hetente, havonta, …stb.) biztonsági másolat készül.

6) **Adatfeldolgozás:** az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve, hogy a technikai feladatot az adatokon végzik.

7) **Adatsértetlenség**: 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.

8) **Adatszármazás hitelesítése**: annak megerősítése, hogy a kapott adatok forrása a kívánt forrás.

9) **Adatvédelem:** a személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

10) **Aktív fenyegetés**: olyan szabad, jogosulatlan hozzáférés veszélye, amely megváltoztathatja a rendszer állapotát.

11) **Alapfenyegetettség:** a fenyegető tényezők olyan csoportosítása, amely a biztonsági alapfunkciók valamelyikének kiesését okozza.

12) **Alkalmazói program:** olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be.

13) **Archiválás:** az a mentési művelet, amikor az adathordozóra mentett állományok a későbbiekben már nem módosíthatók.

14) **Bejelentkezés:** a felhasználó által olyan kapcsolat kezdeményezése, amelynek során számára az informatikai rendszer funkcióinak használata lehetővé válik.

15) **Bizonyítható azonosítás**: a hozzáférési jogosultság ellenőrzése során olyan azonosítási eljárás, amelynek segítségével kétséget kizáróan, utólag is bizonyítható a felhasználó kiléte.

16) **Biztonság:** az informatikai rendszerekben olyan előírások és szabványok betartása, amelyek a rendszer működőképességét, az adatok rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.

17) **Biztonsági auditálás:** a biztonsági előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés.

18) **Elérhetőség:** az adatfeldolgozás során valamely informatikai alkalmazás szolgáltatásai az adott helyen és időben igénybe vehetők.

19) **Felelősségre vonhatóság:** olyan tulajdonság, amely lehetővé teszi, hogy az adott entitás tevékenységei egyértelműen az adott entitásra legyenek visszavezethetők.
20) **Felhasználó:** az informatikai rendszereket használó személy vagy szervezet.

21) **Feljogosítás:** teljes vagy korlátozott hozzáférési jogok megadása.

22) **Fenyegető tényező:** olyan lehetséges művelet vagy esemény, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemeinek védettségét, biztonságát.

23) **Fizikai védelem:** a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.

24) **Gyenge pont:** az informatikai rendszerelemek olyan tulajdonságai, amelyek révén a fenyegető tényezők hatásainak ki vannak téve.

25) **Hálózat:** informatikai rendszerek fizikai és logikai összekapcsolása, amely az összekapcsolt rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé, egymás erőforrásait képesek használni.

26) **Hálózatvezérlő adatok:** a hálózati kommunikáció vezérléséhez, irányításához, ellenőrzéséhez szükséges adatok.

27) **Hardver:** az informatikai rendszer eszközei, fizikai elemeit alkotó részei.

28) **Háromgenerációs elv:** az adatbiztosításhoz és az adatmentéshez szükséges olyan eljárás, amely időben egymást követően három mentést biztosít, és ebből a három mentésből állítja vissza az informatikai rendszer működőképességét.

29) **Hitelesítés:** olyan eljárás, amelynek segítségével egy informatikai rendszeren belüli kapcsolatban a partnerek kölcsönösen kétségtelenül felismerhetik egymást, és ez az állapot a kapcsolat egész idejére változatlanul fennmarad.

30) **Hozzáférés:** olyan eljárás, amely az informatikai rendszer használója számára elérhetővé teszi a rendszerben tárolt adatokat, információkat.

31) **Hozzáférés-ellenőrzés:** az erőforrásokhoz való jogosulatlan hozzáférés elhárítása, beleértve az erőforrás jogosulatlan használatának megakadályozását.

32) **Hozzáférés-ellenőrzési lista:** az erőforráshoz való hozzáférésre jogosult személyek és hozzáférési jogaik jegyzéke.

33) **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.

34) **Elektronikus információs rendszer:** az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók) eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese.

35) **Elektronikus információs rendszer biztonsága:** az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

36) **Jelszó (password):** meghatározott karaktersorozatból álló bizalmas hitelesítési információ.

37) **Kár:** azon érték csökkenése, amelyet valamely objektum jelent egy informatikai rendszer alkalmazásában, és amely akkor következik be, ha valamely fenyegető tényező kifejti hatását.

38) **Kockázat:** a fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat két részből, a kárnagyságból és a bekövetkezés gyakoriságából tevődik össze.

39) **Kiberbiztonság:** a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés működtetéséhez.

40) **Helyi (lokális) számítógép:** személyi számítógép, laptop, vagy munkaállomás a munkahelyre telepítve.

41) **Működőképesség:** az informatikai rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való fennmaradása.

42) **Papíralapú adathordozó:** az adatok minden olyan változatának meghatározására szolgál, amelyek papíron állnak rendelkezésre.

43) **Passzív fenyegetés:** az információ jogosulatlan nyilvánosságra hozatalának veszélye a rendszer állapotának változása nélkül.

44) **Program:** eljárási leírás, amely valamely informatikai rendszer által közvetlenül vagy átalakítást követően végrehajtható.

45) **Rendelkezésre állás:** annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

46) **Rendszerprogram (rendszerszoftver):** olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk, és alkalmazói programokat működtessünk. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

47) **Személyiségi jog:** az egyének joga arra, hogy ellenőrizzék és befolyásolják azt, hogy ki és milyen velük kapcsolatos adatot vagy információt gyűjthet és tárolhat, és ez az adat vagy információ kinek hozható tudomására.

48) **Szerver (Kiszolgáló):** azok a speciális felépítésű számítógépek, amelyeken közös adatbázisok, programok vannak elhelyezve, és ezeket egy időben több felhasználó elérheti, azokon feladatot végezhet.

49) **Szoftver:** valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges.

50) **Szolgáltatás megtagadása:** az erőforrásokhoz való feljogosított hozzáférés megakadályozása vagy az időkritikus műveletek késleltetése.

51) **Támadás:** valamely személy vagy alkalmazás akciója azzal a szándékkal, hogy valamely informatikai rendszert veszélyeztessen, és károkat okozzon.

52) **Titkosság, bizalmasság:** olyan tulajdonság, amely lehetővé teszi, hogy az információ jogosulatlan egyének, entitások vagy folyamatok számára ne legyen elérhető, vagy ne kerüljön nyilvánosságra.

53) **Védelmi mechanizmusok:** olyan intézkedések, amelyeket a biztonsági szabványok határoznak meg a hardver és szoftver gyártó cégek pedig termékeik előállítása során építik be és szolgáltatják a felhasználók részére.

54) **Vírus:** olyan programok vagy programrészek, amelyek a számítógépes adatkezelésben súlyos károkat okozhatnak, számítógépre kerülésük kiszámíthatatlan. Ezek rendszerbe kerülése ellen védekezni kell, elsősorban vírusirtó (víruskereső) programok segítségével.

6. Biztonsági osztályba sorolás

Az adatbiztonsági intézkedések kiadása és bevezetése előtt fel kell térképezni azokat az adatállományokat, adatbázis-csoportokat, valamint a hozzájuk kapcsolódó alkalmazásokat, amelyek az információvédelem és a megbízható működés szempontjából az alábbi biztonsági osztályokba sorolhatók:

Információvédelmi alap biztonsági osztály (IV-A): személyes adatok, üzleti titkok, pénzügyi adatok, illetve a szervezet belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya

Információvédelmi fokozott biztonsági osztály (IV-F): szolgálati titok, valamint a nem minősített adatok közül a különleges személyes adatok, nagy tömegű személyes adatok, banktitkok, közepes értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya

Információvédelmi kiemelt biztonsági osztály (IV-K): az államtitok, a katonai szolgálati titok, valamint a nem minősített adatok közül a nagy tömegű különleges személyes adatok, valamint a nagy értékű üzleti titkok feldolgozására, tárolására alkalmas rendszer biztonsági osztálya

Az SZKT által működtetett informatikai rendszerek biztonsági osztályba sorolása az alábbiak szerint alakul:

Informatikai Rendszer	Biztonsági Kategória
ügyviteli szoftverek	IV-F

A biztonsági osztályba sorolást legalább háromévenként vagy szükség esetén soron kívül, dokumentált módon felül kell vizsgálni.

7. Figyelembe vett szabályozók

Az informatikai rendszerre vonatkozóan a következő szintű szabályozókat kell figyelembe venni, és az azokban megfogalmazott rendelkezéseknek a megkövetelt szinten és mértékig eleget kell tenni:

1. **Jogszabályok:**

   Az informatikai rendszerek biztonságára, védelmére vonatkozó követelmények törvényi szinten szabályozott. Ezek a jogszabályok az informatikai rendszer kereteit határozzák meg.

   a) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló az Európai Parlament és a Tanács (EU) 2016/679 Rendeletének (GDPR)

   b) 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)

   c) 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

   A jogszabályok az informatikai biztonság szempontjából két csoportra oszthatók:
   - az informatikai rendszert és annak környezetét funkcionálisan szabályozó jogszabályok
   - az informatikai rendszer, illetve az abban kezelt adatok biztonságával kapcsolatos jogszabályok

2. **Műszaki normatívák, szabványok, irányelvek és ajánlások**

   A műszaki normatívák, szabványok, irányelvek és ajánlások az alábbi területeken keresztül szabályozzák az informatikai rendszert, annak környezetét, és ezen keresztül az informatikai biztonságot:
   - informatika
   - beruházás
   - tűzvédelem
   - biztonságtechnika
   - iratkezelés

3. **Tárca- vagy ágazati szintű rendelkezések, végrehajtási utasítások**

   A tárca- vagy ágazati szintű rendelkezések szintjén elsősorban az informatikai, információ-feldolgozási feladatok kiosztása, az adattovábbítások rendjének megállapítása történik.

4. **Helyi (belső) szabályozások**

   A helyi szabályozás szintjén jelennek meg azok a belső szabályzatok, intézkedések és előírások, amelyek valamilyen szinten összefüggésben vannak az informatikai biztonsággal:
   - Szervezeti és Működési Szabályzat (SZMSZ)

- Iratkezelési szabályzat
- Vagyonvédelmi, rendészeti, biztonságtechnikai előírások
- Tűzvédelmi Szabályzat
- Munkavédelmi Szabályzat
- Munkaköri leírások

Az Adatbiztonsági Szabályzat, illetve az SZMSZ szerinti feladatokat, felelősségi köröket és jogokat a munkaköri leírásokban kell részletesen kifejteni.

8. Hatáskör, illetékesség

Az informatikai rendszer használata során el kell különíteni a következő funkciókat:
- Fejlesztő (saját szervezet, vagy külső cég)
- Üzemeltetést felügyelő (Informatikai munkatárs)
- Felhasználó

Az SZKT ügyvezetője kijelöli a fontosabb alkalmazások felelőseit, és meghatározza feladataikat és felelősségi körüket.

Az Informatikai munkatárs feladatkörét munkaköri leírásban kell rögzíteni.

Az Informatikai munkatárs engedélye nélkül hozzáférési jogosultság nem adható ki, és nem változtatható meg (kivéve a kötelező letiltást).

9. Általános intézkedések

1. Szervezet

a) A számítástechnikai rendszerben tárolt adatok biztonsága érdekében az SZKT-nál – az adatkezelés jellegétől függően – az alábbi **védelmi módszereket** kell alkalmazni:

- **ügyviteli védelem**: a számítástechnikai rendszer felelőseinek (IT) és az adatkezeléssel kapcsolatos tevékenységek szervezési és adminisztratív módon történő nyomon követése, az egyes felelősségi körök meghatározása. Kiterjed az informatikai rendszerre és annak szolgáltatásaira, valamint az adathordozók kezelésére, beleértve a hozzáférési jogosultság és a betekintés dokumentálását is.

- **fizikai védelem**: olyan eszközök alkalmazása, amelyekkel azok a helyiségek védhetők, ahol számítástechnikai erőforrásokat használnak, vagy az adatmegőrzés szempontjából fontos. Az adathordozókat úgyszintén védelemben kell részesíteni.

- **algoritmikus védelem**: matematikai algoritmusok alapján működő védelem, amely az egyedi számítógépen és a hálózaton is lehetővé teszi a használó azonosítását és a jogosultság ellenőrzését.

b) Az SZKT-nál a munkaköri leírásokban rögzíteni kell az informatikai feladatok ellátásával, valamint a belső adatvédelmi feladatokkal megbízott(ak) feladat-és felelősségi körét, valamint kompetenciáit.

c) Az SZKT szempontjából jelentős alkalmazásokról és adatállományokról nyilvántartást kell vezetni.

d) Az informatikai rendszeren belül elkülönítetten kell kezelni az egyes titokfajtákat, a személyes adatokat, és a törvények által meghatározott egyéb adatcsoportokat.

e) Szükség esetén az egyes számítógépes alkalmazásokra a biztonsággal kapcsolatos, specifikus előírásokat külön meg kell határozni.

f) Az alkalmazások dokumentációinak tartalmaznia kell az üzemeltetési és kezelési előírásokat, valamint a biztonsági követelményeket.

g) Meg kell határozni a számítógépes alkalmazásokkal kapcsolatban, illetve az SZKT-nál keletkezett egyéb dokumentumok megőrzési határidejét.

h) Ha a számítástechnikai rendszer üzemeltetése során kiderül a biztonság megsértése, illetve sérülése, haladéktalanul meg kell kezdeni a vonatkozó intézkedések érvényesítését.

i) Az informatikai rendszert ért káresemények utólagos elemzését rendszeresen el kell végezni.

j) Az elemzést, amennyiben ez indokolt, személyre vagy személyekre vonatkozó feladat- és hatáskör módosításnak kell követnie.

k) A biztonsági szabályozásokkal kapcsolatos tennivalókat a munkaköri leírásokban is szerepeltetni kell.

2. Beszerzés, üzemeltetés, fenntartás

a) A szoftverek beszerzését jogtiszta, megbízható forrásból kell biztosítani.
b) A hardver és szoftver eszközöket nyilvántartásba kell venni.
c) Amennyiben szoftverfejlesztés történik, azt tervezési és fejlesztési módszertan alapján kell elvégezni.
d) Törekedni kell az egységes hardver és szoftver elemek alkalmazására. A számítástechnikai eszközök üzemeltetését a mindenkori Informatikai vezető irányítsa és ellenőrizze. Az informatikai rendszer használatára vonatkozó biztonsági előírások betartását rendszeresen ellenőrizni kell.
e) A számítástechnikai rendszerben bekövetkezett változásokat dokumentálni kell.
f) A külső cégek, szervezetek javítási és karbantartási tevékenységét ellenőrizni kell.
g) Javítás és karbantartás esetén a bizalmas adatokat védeni kell. (pl. adatmentés és felülírásos törlés révén).

3. Szoftverek

a) A szoftverek beszerzésére vonatkozó irányelvek, illetve előírások az SZKT beszerzési politikájának részét képezik.
b) A szoftverek ellenőrzésére vonatkozó irányelveket és előírásokat az üzemeltetési dokumentációknak tartalmazniuk kell.
c) A szoftverek karbantartására és aktualizálására vonatkozó irányelveket és előírásokat az üzemeltetési előírások keretében le kell dokumentálni. A szoftverek

első üzembe helyezése előtt referencia másolatokat kell készíteni, és azokat biztonságos helyen kell őrizni.

d) A katasztrófa megelőzési és elhárítási tervben meg kell fogalmazni az elhárítási stratégiát és a mentesítés végrehajtási ütemtervét a nem kívánatos mellékhatású programok fellépése esetén.
e) A rendszerprogramokat az illetéktelen hozzáféréstől fokozottan kell védeni.

4. Infrastruktúra

a) A biztonsági szempontok figyelembe vételével, tervszerűen kell a lokális számítógépes hálózat szerverét (eit) tartalmazó helyiséget(ket) kiválasztani.
b) A biztonsági zónák határait (látogatók, munkazónák) tervszerűen kell kialakítani.
c) Az átviteli eszközöket, csatlakozási pontokat, elosztó- illetve rendező egységeket ugyanolyan védelmi igénnyel kell védeni, mint a központi berendezéseket.
d) A számítóközpontok üzembiztonsági szabvány-előírásait (klíma, páratartalom, tűzvédelem) be kell tartani.
e) A központi berendezéseket az illetéktelen vagy erőszakos behatásoktól védeni kell.
f) A számítástechnikai rendszert a villámcsapástól, túlfeszültségtől, feszültségcsökkenéstől védeni kell.
g) A számítástechnikai rendszer üzemszerű működéséhez szükséges legfontosabb egységeinek folyamatos működését az áramszolgáltatás kiesése esetén biztosítani kell. (szünetmentes vagy tartalék áramforrás)
h) A felhasználói számítógépek kiválasztásánál figyelembe kell venni a bizalmas adatok kezelése esetén, hogy a berendezések csökkentett elektromágneses sugárzási jellemzőkkel rendelkezzenek.
i) Az üzemi körülmények tűréshatárainak túllépését (hőmérséklet, páratartalom) figyelni és ellenőrizni kell.
j) A tartalék ellátó berendezések funkcionális működését időszakosan ellenőrizni kell.
k) A számítástechnikai rendszer elemeit (hardver, szoftver, adathordozó) a lopástól védeni kell.
l) A számítástechnikai rendszer elemeit (hardver, szoftver, adathordozó) a manipulációtól védeni kell.

5. Személyzet

a) Az informatikai rendszer tervezéséhez, bevezetéséhez, üzemeltetéséhez, karbantartásához szükséges bizalmi funkciókhoz a személyzetet gondosan kell kiválasztani.
b) A személyzetet az informatikai rendszer bevezetése előtt ki kell képezni.
c) A képzésnek ki kell terjednie az informatikai biztonság területére is.
d) A képzés színvonalát és az elsajátított tudás szintjét ellenőrizni kell.
e) A biztonsági előírások betartását ellenőrizni kell.

10. Eljárások

1. Azonosítás, hitelesítés

a) A hálózati rendszerre való csatlakozáshoz az SZKT informatikai szervezeti egységétől kell igényelni a munkakörhöz kötött belépési azonosítót (login név), és jogosultságokat.

b) Az egyes alkalmazásokhoz való hozzáférési jogosultságot az SZKT ágazati vezetői határozzák meg. A hozzáférési jogokról az informatikai szervezeti egységnél nyilvántartást kell vezetni.
c) Új dolgozók belépése, illetve távozó dolgozók kilépése esetén a személyi jogosultságokat aktualizálni kell.
d) Gondot kell fordítani a felhasználók egyedi azonosítására.
e) Elő kell írni a jelszavak használatának módját (titokban tartás, minimális hossz, bonyolultság, érvényességi idő).
f) A hozzáférési jogosultságok kiosztását, illetve megvonását az SZKT ágazati vezetői jóváhagyása után a Informatikai munkatársnak kell elvégeznie.
g) A hozzáférési jogosultságok kiosztását, zárolását, megvonását és módosítását rendszeresen ellenőrizni kell.
h) A jogosulatlan hozzáférési kísérletek eseményeit ellenőrizni kell.
i) A hálózati felhasználókat hitelesíteni kell.
j) A hálózat menedzselési feladatait csak megbízható és ellenőrzött személy végezheti.

2. Naplózás

a) Elő kell írni, hogy mely események kerüljenek naplózásra.
b) A biztonsági követelmények között szerepelnie kell az illetéktelen, illetve jogosulatlan események naplózásának.
c) A jogosultságok kiosztását, módosítását és megvonását naplózni kell.
d) A napló adatokhoz csak hitelesített személyek férhetnek hozzá.
e) A napló adatok kiértékelését automatizált folyamatokkal kell támogatni.
f) A napló adatok megőrzési határidejét rögzíteni kell.
g) A napló készítő elemeket manipuláció ellen védeni kell.
h) Az őrzésre kerülő napló adatokat manipuláció és megsemmisülés ellen védeni kell.

11. Információk, adatok

1. Tárolás

a) A számítógépek saját adattárolóján kizárólag az SZKT által kifejlesztett, vagy vásárolt szoftverek tárolhatók és csak azok üzemeltethetők.
b) Rendszeresen ellenőrizni kell a tároló eszközökön lévő programokat és adatokat.
c) Rögzíteni kell azon adatok és programok listáját, amelyet nem szabad megváltoztatni, módosítani.
d) A bizalmas adatokat az adathordozókon – amennyiben más védelem nem biztosítható – kódolt formában kell tárolni.

2. Adat-és vírusvédelem

a) A vírusfertőzés lehetőségének minimálisra csökkentése érdekében az alkalmazott összes számítástechnikai eszközt vírusellenőrző programmal kell védeni, amely az SZKT-nál rendszeresítve van. A vírusellenőrzést előírt rendszerességgel, illetve a felhasználók jelzésére soron kívül az SZKT Informatikai szervezeti egységének dolgozói végzik.
b) A vizsgálat eredményét elektronikusan tárolt vírusnaplóban kell megőrizni.
c) Alkalmazás külső hálózatra való kapcsolódása (Pl. WAN) csak vírusellenőrző program védelme alatt történhet.

d) Minden kliens számítógépre víruskereső program telepítése szükséges. A víruskeresők adminisztrálása a belső hálózatban kialakított központi adminisztrációs szerveren történik.

3. Feldolgozás

a) Ki kell alakítani a feldolgozással kapcsolatos üzemeltetési és biztonsági irányelveket.
b) A gondatlanság vagy hibák hatásait rendszeresen fel kell mérni.
c) A munkahely ideiglenes elhagyásakor ki kell lépni a számítógépből.
d) Az információk és az adatok sértetlenségének biztosításához ellenőrzési módszereket kell alkalmazni.
e) Elő kell írni az adott feladatkörhöz szükséges másolatok készítésének feltételeit.
f) Szükség szerint alkalmazni kell a másolásvédelmi intézkedéseket.

4. Mentések

a) Az előre nem kiszámítható adatvesztést okozó események káros hatásának ellensúlyozása érdekében adatmentéseket kell végezni.
b) Teljes mentést kell végezni minden jelentősebb módosítás után, de legalább éves rendszerességgel. Ez alapján egy teljes rendszer összeomlás esetén is biztosítani lehet az operációs rendszer és a futó programok összeomlás előtti állapot visszaállítását.
c) Adatállományok mentését minden nap el kell végezni. A mentéseknél érvényesüljön a háromgenerációs elv.
d) A felhasználói igényeknek megfelelően, vagy meghibásodás esetén a mentett vagy archivált állományok visszaállításáért a Informatikai munkatárs felelős.

5. Eredményadatok kiadása

a) A kinyomtatásra kerülő anyagok biztonságos kezeléséről és tárolásárról gondoskodni kell.
b) A kinyomtatott anyagok kezelésére az Iratkezelési Szabályzat rendelkezései vonatkoznak.

12. Adathordozók

1. Kezelés, tárolás

a) Szabályozni kell a papír alapú, valamint, a mentésre, adatcserére használt egyéb adathordozók kezelésére vonatkozó folyamatokat.
b) Rögzíteni kell az adminisztrációért felelős személyt.
c) Az adathordozókat meg kell jelölni (azonosítás)
d) A különleges védelmet igénylő adathordozókat (bizalmas adatok) elkülönítve kell kezelni.
e) A különleges védelmet igénylő informatikai adathordozók adatait titkosítani kell.
f) A tárolt adathordozók sértetlenségét rendszeresen ellenőrizni kell.
g) A számítástechnikai eszközzel olvasható és a manuális adathordozók tárolását, hozzáférését és felhasználását ellenőrizni kell. Különös figyelmet kell fordítani arra, hogy a biztonságos területről kivitt eszközök maradvány-adatokat ne tartalmazzanak.

2. Továbbadás/szállítás

a) Szabályozni kell a papír alapú adathordozók, az informatikai adathordozók továbbadási folyamatait.
b) Rögzíteni kell az idegen adathordozók átvételi szabályait.
c) Ellenőrizni kell a továbbadási és átvételi jogosultságokat.
d) Ellenőrizni kell az adathordozók visszaadási kötelezettségének teljesülését.
e) Az átvétel során ellenőrizni kell az adatok sértetlenségét, manipulálatlanságát.
f) A különleges védelmet igénylő adatok továbbítására szolgáló adathordozókon az adatokat titkosítani kell.

3. Megsemmisítés

a) Rögzíteni kell a megsemmisítési eljárásra jogosult személyek feladat és hatáskörét
b) A megsemmisítési folyamatot ellenőrizni kell.

13. Intézkedési terv vészhelyzet esetére

A vészhelyzet-megelőzés alapvető követelménye a részletes Katasztrófaterv elkészítése, tesztelése és a végrehajtás rendszeres gyakorlása. Az intézkedési terv elkészítése az Informatikai Iroda feladata.

A katasztrófaterv öt részből áll:

1. A Katasztrófaterv definíciója
Katasztrófaterv: eljárás vagy tevékenység-lépések sorozata annak biztosítására, hogy a szervezet kritikus információ-feldolgozó képességeit helyre lehessen állítani elfogadhatóan rövid idő alatt a szükséges aktuális adatokkal katasztrófa után. A számítógép katasztrófa egy olyan esemény, amely az adatfeldolgozó képesség elvesztését okozza hosszabb időre.

2. Mentési (megelőzési) terv
A mentési terv azon lépések sorozata, amelyeket azért hajtanak végre a katasztrófát megelőzően (a normál üzem során), hogy lehetővé tegyék a szervezet számára a reagálást a katasztrófára. A mentési terv biztosít eszközöket a helyreállításhoz. (számítógép tükrözés, optikai tároló)

3. Helyreállítási terv
A helyreállítási terv eljárások sorozata, amelyeket a helyreállítás fázisában hajtanak végre annak érdekében, hogy helyreállítsák az informatikai rendszert a tartalék központban vagy helyreállítsák az adatfeldolgozó központot.

4. Tesztelési terv
A teszt terv azokat a tevékenységeket tartalmazza, amelyek a Katasztrófaterv működőképességét ellenőrzik és biztosítják.

5. Karbantartási (üzemben tartási) terv
A karbantartási tervet használják a Katasztrófaterv aktuális állapotban tartására a szervezet változása esetén.

14. Ellenőrzési, intézkedési feladatok

A Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.) 375.§, 422.§, 423.§, 424.§ szankcionálja a számítástechnikai rendszer és adatok elleni jogellenes cselekményeket, valamint a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszását.

15. Mentésekkel, helyreállítással kapcsolatos intézkedések

a) A biztonsági másolatok készítésének, kezelésének rendjét be kell tartani, és rendszeresen ellenőrizni kell:
   - a teljes mentéseket a fokozott biztonsági osztály követelményeinek megfelelő periodicitással kell végezni,
   - a biztonsági mentések tárolásánál a háromgenerációs elvet kell érvényesíteni, azaz minimum az utolsó három mentést kell tárolni.

b) A biztonsági mentéseket külön, a fokozott biztonsági osztály követelményeinek megfelelő körülmények között kell tárolni, és a kezelést részletesen kell szabályozni.

c) Biztosítani kell – szerződéses alapon – a rendelkezésre állási követelményekkel arányos, a megbízható működés szempontjából megfelelő szerviz és rendszerkövetési hátteret és reakcióidőt.

d) A rendszer üzemeltetése során biztosítani kell a karbantartó és üzemeltető személyzet rendszeres oktatását és továbbképzését olyan szinten, hogy az előírt kiesési időn belül meg tudják valósítani a rendszer visszaállítását normál üzemállapotra.

e) A rendszerben bekövetkezett hibajelenségeket, rendszerleállásokat, áttéréseket vagy manuálisan, és/vagy a rendszer által naplózni kell. Rögzítésre az alábbi paraméterek kerüljenek:
   - az esemény típusa
   - a bekövetkezés dátuma és időpontja
   - a normál állapot visszaállításának dátuma és időpontja
   - a hibaelhárításban résztvevők neve
   - a hibajelenség rövid leírása

f) A hibajelenségeket utólagosan elemezni és értékelni kell az üzemeltetés minőségének javítása érdekében.

g) Adatbiztosítás
   - Az adatbázisról, és a napló file-okról hetente kell biztonsági másolatot készíteni.
   - A másolatok készítését, tárolását és nyilvántartását rendszeresen ellenőrizni kell

   A megtervezett mentési és visszaállítási eljárásokra üzemeltetési előírásokat kell készíteni, és azok betartását rendszeresen ellenőrizni kell.

h) Újraindítás
   - a hiba megszüntetése után csak a Katasztrófa tervnek megfelelően szabad újraindítani a rendszert, a fokozatosság betartásával.

A meghibásodás okát ki kell elemezni, és meg kell tenni a szükséges intézkedéseket

16. Jogosultságok

a) Az SZKT biztonságpolitikájának megfelelően az egyéni jogosultságokat a rendszergazdának terv szerint ki kell osztania, és folyamatosan karban kell tartania.
b) Az adatok minősítését, kezelési jelzését kötelezően alkalmazni, és a változásokat automatikusan naplózni kell.
c) A jogosultsági táblákat rendszeresen aktualizálni kell
d) Az észlelt eltéréseket (hibás kezelés, jogosultság megsértésének kísérlete) haladéktalanul ki kell vizsgálni, és az eredményt jegyzőkönyvben kell rögzíteni

17. Záró rendelkezések

Jelen Szabályzat 2018. május 25. napján lép hatályba és visszavonásig hatályos. A hatálybalépéssel egy időben hatályát veszti minden, e tárgyban kiadott szabályzat és igazgatói utasítás.

A Szabályzat rendelkezéseit az érintett munkavállalókkal ismertetni, a szükséges mértékben a munkavállalói oktatások keretében oktatni kell.

Jelen Szabályzatot az SZKT valamennyi szervezeti egysége számára folyamatosan hozzáférhetővé kell tenni.

Alkalmazását elrendelem.

Majó-Petri Zoltán
ügyvezető igazgató