Tervezet!!!

Fejlesztés és szerkesztés alatt!

Informatikai Biztonsági Szabályzat

1. § A Szabályzat jogi háttere és kapcsolódó belső irányítási eszközök

Az Informatikai Biztonsági Szabályzat (továbbiakban IBSZ) jogi alapját az alábbi jogszabályok, közjogi szervezetszabályozó eszközök és belső irányítási eszközök képezik:

a) 2013. évi L. törvény (a továbbiakban: Ibtv.) az állami és önkormányzati szervek elektronikus információbiztonságáról,

b) **2003. évi C. törvény az elektronikus hírközlésről**

c) 233/2013. (VI. 30.) Korm. rendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről,

d) 301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról,

e) 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról,

f) 73/2013. (XII. 4.) NFM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről,

g) g) 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről,

h) a NySzC Széchenyi István Közgazdasági, Informatikai Szakgimnáziuma és Kollégiuma (továbbiakban iskola) Szervezeti és Működési Szabályzata,

2. § A Szabályzat célja

a) Az IBSZ alapvető célja, hogy az iskolai informatikai rendszerek alkalmazása során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

b) Az IBSZ célja továbbá:

i. a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
ii. az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
iii. az üzembiztonságot szolgáló karbantartás és fenntartás,
iv. az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
v. az adatállományok tartalmi és formai épségének megőrzése,
vi. az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
vii. a munkaállomásokon lekérdezhető adatok körének meghatározása,
viii. az adatállományok biztonságos mentése,
ix. az informatikai rendszerek zavartalan üzemeltetése,
x. a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
xi. az adatvédelem és adatbiztonság feltételeinek megteremtése.

c) A szabályzatban meghatározott védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

d) A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

3. § A Szabályzat hatálya

a) Az IBSZ személyi hatálya kiterjed a Nyíregyházi Szakképzési Centrum Széchenyi István Közgazdasági, Informatikai Szakgimnáziuma és Kollégiuma (továbbiakban iskola, vagy intézmény vagy NYSZC Széchenyi) valamennyi alkalmazottjára és tanulójára, valamint az iskola informatikai rendszeréhez hozzáférést kapó valamennyi partnerre.

b) Az IBSZ tárgyi hatálya
   i. kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
   ii. kiterjed az NYSZC Széchenyi tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre, valamint a gépek műszaki dokumentációira is,
   iii. kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési stb.),
   iv. kiterjed a rendszer- és felhasználói programokra,
   v. kiterjed az adatok felhasználására vonatkozó utasításokra,
   vi. kiterjed az adathordozók tárolására, felhasználására.

c) A Szabályzat hatálya kiterjed működési és működtetési helytől függetlenül az iskola tanáraira, dolgozóira, diákjaira, valamint az eszközöket időlegesen használó személyekre (vendégek, eszközöket bérbevevők, továbbiakban vendégek).

d) A szabályzatot a diákok számára a balesetvédelmi és tűzvédelmi oktatással egyidejűleg kell ismertetni. Annak tudomásul vételét aláírásukkal igazolják. A tájékoztatás megszervezése az intézmény vezetőjének feladata.

e) A dolgozókat az egységvezetők kötelesek tájékoztatni a szabályzatról.

4. § A felhasználókra vonatkozó szabályok

4.1 Az iskolában valamennyi felhasználó – jogosultságtól és állományba tartozástól függetlenül –

a) felelős az általa használt, az IBSZ hatálya alá eső eszközök rendeltetésszerű használatáért,

b) a rá vonatkozó szabályok szerint felelős az általa elkövetett informatikai vonatkozású szabálytalanságokért, valamint a keletkező károkért és hátrányért, különös tekintettel az informatikai biztonsági incidens fogalomkörébe tartozó cselekményekért,

c) köteles az IBSZ-ben megfogalmazott szabályokat megismerni és betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni,

d) köteles a számára szervezett informatikai biztonsági oktatáson részt venni, az ismeretanyag elsajátításáról számot adni,

e) köteles a rendelkezésére bocsátott számítástechnikai eszközöket megóvni,köteles a belépési jelszavát (jelszavait) az előírt időben megváltoztatni, biztonságosan kezelni,

g) felügyelet nélkül a munkahelyen (munkaállomáson) személyes adatot vagy minősített adatot tartalmazó dokumentumot, adathordozót nem hagyhat,

h) információ biztonságot érintő esemény gyanúja esetén az észlelt rendellenességekről köteles tájékoztatni a közvetlen felettesét és elektronikus információs rendszer biztonságáért felelős személyt,

i) köteles a folyó munka során nem használt hivatalos adatokat, dokumentumokat, nem nyilvános anyagokat, adathordozókat elzárni,

j) köteles a munkahelyről történő eltávozáskor az addig használt – kivéve, ha ez a rendszer(ek) más által történő használatát, vagy a karbantartást akadályozza – eszközt szabályszerűen leállítani,

k) az elektronikus levelezés és az internet használat során tartózkodik a biztonság szempontjából kockázatos tevékenységektől.

4.2 Az iskola informatikai rendszerét használó valamennyi felhasználónak tilos:

a) az általa használt eszközök biztonsági beállításait megváltoztatni,

b) a saját használatra kapott számítógép rendszerszintű beállításait módosítani (ide nem értve az irodai programok felhasználói beállításait),

c) a munkaállomására telepített aktív vírusvédelmet kikapcsolni,

d) belépési jelszavát (jelszavait), hardveres azonosító eszközét más személy rendelkezésére bocsátani, hozzáférhetővé tenni,

e) a számítógép-hálózatot fizikailag megbontani, számítástechnikai eszközöket lecsatlakoztatni, illetve bármilyen számítástechnikai eszközt rácsatlakoztatni a hálózatra az informatikai rendszert üzemeltetők jóváhagyása nélkül,

f) a számítástechnikai eszközökből összeállított konfigurációkat megbontani, átalakítani,

g) bármilyen (kivéve tanár által engedélyezett, oktatási célra használt) szoftvert installálni, internetről letölteni, külső adathordozóról merevlemezre másolni az elektronikus információs rendszer biztonságáért felelős személy engedélye, illetve az üzemeltető közreműködése nélkül, a munkaállomásokon nem az iskolában rendszeresített, vagy engedélyezett szoftvereket (szórakoztató szoftverek, játékok, egyéb segédprogramok) installálni és futtatni,

h) online játékokat használni,

i) bármilyen eszközt számítástechnikai eszközökbe szerelni és használni,

j) az általa használt adathordozó (pl. CD, DVD, pendrive stb.) eszközt számítógépben hagyni a munkaállomásáról való távozás esetén,

k) ellenőrizetlen forrásból származó adatokat tartalmazó adathordozót az eszközökbe helyezni,

l) más szerzői, iparjogvédelmi, egyéb szellemi tulajdonhoz fűződő, vagy egyéb személyhez fűződő jogát vagy jogos érdekét sértő dokumentumokat, tartalmakat (zenéket, filmeket, stb.) az eszközökön tárolni, oda le-, illetve onnan a hálózatra feltölteni,

m) láncleveleket továbbítani, levélszemetet, továbbá azok mellékleteit, vagy linkjeit megnyitni,

n) rendszer biztonságáért felelős személy külön engedélye nélkül – feliratkozni, kivéve a munkavégzéshez szükséges:

   I. az iskola által megrendelt, működtetett, vagy előfizetett szolgáltatásokat,

   II. belső információs rendszereket,

   III. közigazgatási, illetve nemzetközi, vagy uniós szervek/szervezetek által biztosított szolgáltatásokat,

   IV. közigazgatási szervek által felügyelt szervek, vagy szervezetek által biztosított szolgáltatások levelező listáit.

4.3 A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tranzakcióért a bejelentkezéstől a kijelentkezésig a bejelentkezett felhasználó a felelős. Ez a felelősség akkor is fennáll, ha a tranzakciókat harmadik személy hajtotta végre, amennyiben erre az IBSZ előírásainak felhasználó általi be nem tartása miatt kerülhetett sor.

4.4 Amennyiben a munkaállomást több személy is használhatja, a felhasználó a munkaállomást csak akkor hagyhatja el, ha minden futó programból, azonosított kapcsolatból és abban az esetben, ha nem egyedi felhasználói fiókos rendszer üzemel a számítógépen, az operációs rendszerből is kijelentkezett.

4.5 A felhasználó dokumentum nyomtatásakor köteles biztosítani, hogy az általa kinyomtatott irathoz illetéktelen személy ne férjen hozzá. Közös használatú hálózati nyomtató esetében a kinyomtatott iratot köteles a nyomtatóból eltávolítani, sikertelen nyomtatás esetén köteles meggyőződni – amennyiben szükséges, informatikus munkatárs segítségével – arról, hogy a nyomtató memóriájában nem maradt nyomtatandó dokumentum.

4.6 A felhasználó a rendelkezésére bocsátott, hordozható informatikai, irodatechnikai, multimédiás eszközt vagy adathordozót köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.

5. § A hálózat használata

a) Az intézményben üzemelő belső és külső (Internet) hálózat használatát külön részekben célszerű tárgyalni, különös tekintettel arra, hogy az intézmény az Internetre a Hungarnet és a SuliNet tagjaként is csatlakozik, s ezen szervezetek a tagok részére kötelező Internet használati szabályokat írnak elő.

b) Internet

a) A Hungarnet és a SuliNet által előírt, az intézményre is kötelező szabályokon túlmenően, illetve azokat kihangsúlyozva az alábbiak kötelezőek minden felhasználóra.

i) Az Internetet, illetve azokkal szorosan kapcsolatba hozható eszközöket csak az intézményi oktatásra, ügyvitelre, és az ezekhez kapcsolódó tevékenységekre lehet igénybe venni.

ii) Az intézményben üzemeltetett Internetre kapcsolt szerverekre az intézmény dolgozói és diákjai szabadon igényelhetnek felhasználói jogosultságot a szerverek rendszergazdáitól. Ezzel a felhasználó önálló elektronikus levelezési címhez jut (e-mail). A jelszót mindenki személyesen adja meg az account rögzítésekor. A levelezési címekről az illetékes rendszergazda nyilvántartást vezet, melyet harmadik fél számára nem adhat át sem részleteiben, sem egészében.

iii) A külső hálózat szűkös sávszélessége miatt lehetőség szerint kerülni kell a külső levelezőszerverek használatát, illetve a nagy állományok csatolt állományokként való transzportálását.

iv) Amennyiben bárki elveszti, elfelejti jelszavát, újat csak indokolt esetben kaphat.

c) Belső hálózat:

b) A hálózatba kötött számítógépek használata nem különíthető el az Internettel foglalkozó rész szabályozásától, mivel az intézményben minden számítógép kapcsolódik az iskolai hálózathoz, így potenciálisan elérheti az Internetet.

c) A hálózati erőforrásokat oktatási, és intézményi adminisztrációs feladatok ellátására szabad igénybe venni. Ezzel ellentétes magatartást folytatókat figyelmeztetni kell a helyes használat rendjére. A figyelmeztetést írásban rögzíteni kell. Többszöri szabályszegés után a felhasználó jogainak részleges, vagy teljes korlátozását kell elrendelni. A korlátozás elrendelése, annak időtartama az intézmény vezetőjének feladata. A korlátozás kezdeményezése, végrehajtása az illetékes rendszergazda feladata. A korlátozás esetleges feloldásáról a korlátozott személyt értesíteni kell.

d) Különös figyelmet kell fordítani a nagy hálózati terhelést okozó illegális tevékenységek kiszűrésére, mivel ezek a normális oktatási, ügyviteli folyamatokat korlátozzák, vagy lehetetlenné teszik. Ezen magatartások felderítése a rendszergazdák feladata. Ha bármely felhasználó ilyen tevékenységről tudomást szerez, köteles az illetékes rendszergazdát tájékoztatni.

e) A szabályzat megsértése a hálózat használatában korlátozást, szélsőséges esetben kizárást jelenthet a felhasználó számára. Ha egy adott gépen nem azonosítható egyértelműen a szabálytalanságot elkövető felhasználó, akkor a gépen dolgozó felhasználó, illetve gépleltár szerinti használója ellen kell foganatosítani a rendszabályokat. A számítógépes szaktantermek gépeinek használatáért a tanítási órákon az adott tanár a felelős. Tanórán kívül elkövetett visszaélés esetén a felügyeletet ellátó személy ellen kell eljárni, amennyiben a visszaélő személye ismeretlen marad. Az intézkedésről az érintetteket tájékoztatni kell. A

felderítés megkönnyítése érdekében a rendszergazdák kötelesek, amennyiben ez lehetséges, a bejelentkezésekről gépenként és személyenként nyilvántartást vezetni.

f) Felhasználói jogosultságokat (account-ot) a megosztott nyomtatók és egyéb hálózati eszközök használatára az intézmény dolgozói és diákjai alanyi jogon kapnak. Erről az illetékes rendszergazda a rendelkezésre álló adatok alapján gondoskodik. Az intézmény vendégei erre kijelölt formanyomtatványon igényelhetnek az érintett rendszergazdától. *Ezen jogosultság független az előző pontban említett e-mail cím igényléstől*. A kiadott jelszót a felhasználónak kötelessége azonnal megváltoztatni.

g) Minden felhasználónak gondoskodnia kell, hogy a jelszava más felhasználó tudomására ne juthasson. Egyidejűleg két számítógépen a diák felhasználók nem jelentkezhetnek be. Ebben az esetben a felhasználó account-ja automatikusan tiltásra kerül.

h) A jelszavaknak egyedieknek kell lenniük. Ezeket rendszeres időközönként meg kell változtatni.

i) A jelszavakra vonatkozó frissítések gyakoriságára, a jelszavak hosszára, felépítésére vonatkozó előírásokat egy erre hivatott belső szakmai fórum hozza meg, melyet a biztonságpolitikának és az ide vonatkozó ajánlásoknak megfelelően aktualizál. A jelszavak kialakítására vonatkozó ajánlásokat ezen szabályzat 3. számú melléklete tartalmazza. Ezen rész minden felhasználó tetszőleges jelszavára érvényes.

j) A rendszerben sehol nem engedélyezett a vendégfelhasználó (guest), vagy a csoportos felhasználói azonosítás.

k) Vendégek az intézmény vezetőjének engedélye alapján kaphatnak hálózati hozzáférést. A vendég hozzáférése korlátozott ideig érvényes, melyet az igénylésben fel kell tüntetni. A lejáratkor a felhasználó fiókja zárolásra kerül, majd 30 nap után a felhasználó véglegesen törlődik a rendszerben a hozzá tartozó állományokkal egyetemben. A törlés alól kivételt képeznek a rendszeresen ismétlődő feladatokhoz rendelt felhasználói fiókok. Ezek ürítéséről a 30 nap letelte után a rendszergazda gondoskodik.

l) A diákoknak kiadott account-ok érvényességi ideje az iskolában folytatott tanulmányok várható befejezéséig tart. Amennyiben ezen időtartamban változás történik azt idejében jelezni kell az illetékes rendszergazdának. Amennyiben jelzés nem érkezik, a lejárat után az account, és a vele kapcsolatba hozható adatállományok automatikusan törlődnek.

m) Amennyiben bárki elveszti jelszavát, felhasználói fiókja zárolásra kerül. A zárolás feloldása, új jelszó megadása csak rendszergazda által történhet. A rendszert úgy kell konfigurálni, hogy 3 sikertelen próbálkozás után zárolja a felhasználó fiókját, melyet csak a rendszergazda tud feloldani.

n) Bizonyos cselekedetek számítógéppel való visszaélésnek minősülnek. Az elkövetők felelősek a károk megtérítéséért és korlátozó intézkedések alá eshetnek. Ezek lehetnek a számítógépen meghatározott jogosultságok megvonása, illetve a hálózat használatából való kizárás. Indokolt esetben fegyelmi felelősségre vonásra is sor kerülhet. Az érvényes jogszabályok alapján tiltottak az alábbiak:

   - Levéltitok megsértése.
   - Szerzői és szomszédos jogok megsértése.

(1) A számítógépek és a hálózat normális működésének lehetetlenné tétele, a gép tönkretétele, szándékos károkozás a BTK-ba ütköző cselekedet, amely a hálózat használatának megvonásán túl, fegyelmi, illetve büntetőjogi következményekkel jár. A Büntető törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 386. §-a szerinti „Védelmet biztosító műszaki intézkedés kijátszása”, vagy a BTK. 422. §-a szerinti

„Tiltott adatszerzés", vagy a Btk. 423. §-a szerinti „Információs rendszer vagy adat megsértése", vagy a Btk. 424. §-a szerinti „Információs rendszer védelmét biztosító technikai intézkedés kijátszása" bűncselekmény gyanúja felmerülésének alapján az intézménynek az illetékes hatóság felé feljelentést kell tennie.

- Az Adatvédelmi Törvényben foglaltak megsértése.
- A felhasználóknak tilos a gépek operációsrendszerének hálózat elérését szabályozó részének bárminemű módosítása. Az IP címek és a hálózati kártya egyedi azonosítói adatbázisban vannak tárolva, bármelyik megváltoztatása esetén a rendszer a gépet a hálózatból automatikusan kizárja. IP címet megváltoztatni csak rendszergazdai beleegyezéssel lehetséges. Az IP címek kezelése rendszergazdai feladat.

o) A felhasználó nem kísérelheti meg a számára, ill. a besorolása szerinti felhasználói csoport számára nem engedélyezett erőforrások, szolgáltatások használatát, jogosultságok megszerzését. Minden szolgáltatás csak arra a célra vehető igénybe, melyre azt létrehozták. Különösen nem megengedhető pl. mail, telnet használata nagyméretű adattömegek hálózati átvitelére, mozgatására.

p) Az account-okat, a hálózatot és annak erőforrásait tilos kereskedelmi, vagy egyéb nem oktatási és kutatási célra használni. Azok használatából a felhasználónak jövedelme nem származhat.

q) Tilos felhasználói jogosultságok megváltoztatása diákok számára!

r) Tulajdonosuk tudomása nélkül tilos bármely felhasználó:

- állományainak olvasása,
- állományainak átvitele bármely más gépre,
- az ő területére állományok másolása és azok módosítása.
- Annak érdekében, hogy a hálózati rendszer védett legyen jogosulatlan használat, illetve károkozás ellen, az üzemeltető fent tartja magának azt a jogot, hogy bárkit a gép és a hálózat használatából kizárjon; megnézzen, lemásoljon, megváltoztasson, vagy töröljön bármely állományt, amely kapcsolatban lehet a rendszer, vagy a hálózat jogosulatlan használatával. Az ilyen módon tudomására jutott információt az üzemeltetőnek hivatali titokként kell kezelnie. Az üzemeltető fent tartja magának a jogot, hogy a számítógépes rendszereket bármikor ellenőrizze, leállítsa vagy átkonfigurálja, illetve bármely egyéb intézkedési jogot, amely szükséges lehet a hálózat erőforrásainak megvédéséhez és a további működés biztosításához. Erről az érintetteket az érintett rendszergazda, az intézmény vezetőjével történt egyeztetés után, tájékoztatni köteles.

s) A felhasználó köteles együttműködni a rendszergazdákkal. A rendszergazdai utasításokat, még ellenkező vélemény mellett is, végre kell hajtani. Az érintett utólag élhet panasszal az intézmény vezetőjénél.

6. § Hardver eszközök használata

(1) A diákok a szaktantermekben lévő számítógépek működési paramétereit csak tanári utasításra - az operációs rendszer alapjait érintő, valamint a hálózat paramétereinek kivételével - változtathatja meg. A szaktantermekben elhelyezett eszközöket rendeltetésszerűen kell használni.

(2) Számítógépek és azok perifériáinak áthelyezése az intézmény vezetőjének döntése alapján *kizárólag* valamely rendszergazda segítségével történik. A módosításokat a rendszergazda által vezetett nyilvántartásokban azonnal át kell vezetni.

(3) A szaktantermekben az órai munka, valamint az otthoni elvégzendő feladatok támogatására nyomtatók vannak elhelyezve. A nyomtatót csak a rendszergazdák, valamint oktatók bonthatják meg, illetve cserélhetnek benne festékpatront. A festékpatron kiürüléséről, az azt észlelő személy értesíti a rendszergazdát, aki köteles a folyamatos munkavégzés biztosítása érdekében minden tanteremben használt nyomtatóhoz rendszeresített festékpatronból biztonsági tartalékot raktározni.

(4) Bármely eszköz meghibásodása esetén a hiba elhárítását jogtalanul megkezdeni tilos. A rendszergazdát kell értesíteni (lehetőleg a hibajelenség minél pontosabb leírásával), aki jogosult a hiba kijavításáról intézkedni.

(5) A tanárok, dolgozók – munkaköri feladataik ellátásához szükséges mértékben használhatják a számítástechnikai eszközöket, azonban az intézményből kivinni csak külön engedély alapján lehet. A kivitel tényéről jegyzőkönyvet kell felvenni, melyet a gazdasági vezető vezet. A jegyzőkönyvnek tartalmaznia kell, hogy ki, mit, mikor visz ki, valamint, hogy mikor hozza vissza, hova vitte, a kivivő és az engedélyező aláírását és ha van, a kivitt eszközök gyári számát. Az engedélyezés egyszemélyi felelőse az intézmény mindenkori vezetője.

7. § Szoftverek használata

(1) Az intézményben csak jogtiszta és vírusmentes szoftver működése és használata engedélyezhető. Erről minden felhasználó egyénileg gondoskodik, melyhez támogatást a rendszergazdák adnak. A programok és adatállományaik vírusmentességét a lehetőségekhez mérten a rendszergazdáknak kell biztosítani. Az intézményben központilag beszerzett vírusvédelmi alkalmazás használatára van lehetőség. Ennek adatdefiníciós állományát a felhasználók önállóan, a rendszergazdák támogatását igénybe véve frissíthetik. A vírusleíró adatbázis frissítése a számítógépes szaktantermekben és a szervereken kötelezően elvégzendő feladata a rendszergazdáknak.

(2) Az intézményben használt jogtiszta szoftver más intézménynek tovább nem adható, de az intézmény dolgozója az intézmény érdekében végzendő munkájához az intézmény területén kívül is felhasználhatja, ha arra lehetőséget biztosít a szoftver licencszerződése.

(3) A szoftverek szellemi alkotások. A szellemi alkotásokat a szerzői jogok védik. Erre a védelemre a nevének megadásával automatikusan jogosult a szerző. A szerzői jogokra nemzetközi egyezmények vonatkoznak, melyek Magyarországon is érvényesek. Szerzői joggal védett szoftvert csak az ide vonatkozó szerződéssel összhangban lehet használni. Gyári programok lemásolása bármely gépről és annak máshol való használata a szerzői jogok megsértése, ezért a BTK hatáskörébe esik.

(4) Az intézményben használt szoftverekről tételes, naprakész nyilvántartást kell vezetni (sorszám, megnevezés, gyártó, licencszám), mely kimutatás rendszeres időközönként ellenőrzésre kerül. A nyilvántartás az illetékes rendszergazda feladata.

(5) Szoftvert bármely az iskola tulajdonába lévő gépre csak az rendszergazda tudtával lehet telepíteni, függetlenül annak jogállásától. A telepítés tényét az illetékes rendszergazda nyilvántartásba köteles azonnal rögzíteni.

(6) Telepített szoftver eltávolításáról értesíteni kell az illetékes rendszergazdát, ahol a változást haladéktalanul át kell vezetni a nyilvántartásban.

7. § Adat-, titokvédelem

2.1 Az adat-, és személyiségjog védelem előírásai a rögzítendő adatokra

Személyes adatok kezelése kizárólag a c.)-g.) biztonsági kategóriájú gépeken kezelhetők (a kategóriákat lásd korábban). Tanulói gépek ezen adatok kezelésére nem használhatók. A személyes adatok kezelése során fokozott figyelemmel kell eljárni, a következők betartásával:

- A személyes adatok kezelésére szolgáló gépek őrizetlenül nem hagyhatók. Ha a felhasználó a gépet elhagyja, akkor köteles zárolni vagy kilépni. Azokat az irodákat, amelyben személyes adatokat tárolnak nyitva hagyni nem lehet. Ha az illetékes dolgozó távozik az ajtót köteles bezárni.
- Az adott nyilvántartás kezelésére csak megadott személyek jogosultak. Ezekhez a nyilvántartásokhoz illetéktelen személy nem férhet. Az illetéktelen hozzáférés a BTK 375.§, 423.§ és 424.§ alá tartozik, és az azokban meghatározott módon büntethető. A felelős adatkezelő köteles a biztonság érdekében a tőle elvárható gondossággal eljárni. Belépési adatait nem adhatja át, nem teheti elérhetővé senkinek.
- A rendszergazda gondoskodik a hálózaton tárolt adatok hozzáférési jogosultságainak kiosztásáról. Felelős a hálózati adatok (nyilvántartások) hozzáférési jogosultságaiért az alkalmazott rendszer lehetőségeinek figyelembevételével.
- A személyes adatok rendelkezésre állása az iskola működése szempontjából kiemelt fontosságú. Kiemelt biztonsági igényű adatok: az elektronikus napló, munkaügyi és bérrendszer, gazdasági ügyviteli rendszer. Ezen adatok napi (éjjeli) mentése a rendszergazda feladata. A rendszer meghibásodása esetén a rendszergazda köteles azonnal megkezdeni a helyreállítást, amit a lehető legrövidebb idő alatt be kell fejeznie. Ez a tevékenység elsőrendű feladat, az elvégzését akár más teendők rovására is előnyben kell részesítenie.
- Az adatok illetéktelen adathordozóra mentése, elvitele, nyilvánosságra hozatala TILOS!
- Az adatkezelés körében végzett nyomtatáson kívül az adtok nyomtatása is tilos. Az adatkezelés során kinyomtatott személyes adatokat bizalmasan kell kezelni, a papír alapú adatokat illetéktelen nem láthatja. A kinyomtatott adatokat a nyomtatás céljának megszűnésekor meg kell semmisíteni.
- Személyes adatokat tartalmazó irat nem hagyható illetéktelenek által hozzáférhető helyen.

Az elektronikus nyilvántartások megőrzéséért a rendszergazda és az adott nyilvántartás gazdája felel. Gondoskodni kell arról, hogy az adatok az esetleges program vagy technológia váltástól függetlenül elérhetők maradjanak.

Az intézmény garantálja, hogy a felvett személyes adatokat csak az előre

megadott célra használja fel, azokat más célra nem használja, harmadik félnek nem adja át. Kivételt képeznek ez alól az oktatással kapcsolatos olyan speciális adatok, amelyek a tanuló személyes adatai, azonban a szülő, gondviselő azokba betekintést nyerhet (pl. tanulmányi előmenetel adatai, jegyek, hiányzás stb.) Kivétel továbbá az az eset, amikor a harmadik félnek történő átadást jogszabály írja elő (pl. igazolatlan hiányzás esetén szülő, jegyző, KIR rendszer, stb.)

Az intézmény személyes adatot nem hoz nyilvánosságra, kivéve a jogszabályban előírt eseteket, az adatok azonban felhasználhatók statisztikai kimutatásokhoz, amelyek már nyilvánosságra hozhatók.

2.2 Az üzleti titkot képező adatok körének meghatározása

A polgári törvénykönyvről szóló törvény alapján az intézmény üzleti titoknak minősítheti azokat a tényeket, információkat, adatokat, amelyek titokban tartásához az intézménynek méltányolható érdeke fűződik.

Az üzleti titok körébe vont adatokat az intézmény vezetője határozza meg. A határozatot, az érintett adatok körével és az azokba betekintést nyerhetők listájával az érintettek tudomására hozza. Ha az ebbe a körbe bevont adatok, információk tárolása, feldolgozása, továbbítása számítástechnikai eszközökkel (is) történik, akkor az értesítettek körébe be kell vonni az adatok fizikai kezelését, mentését végző személyt (személyeket) is. (rendszergazdák) A számítógépes hozzáférés korlátozásáért a rendszergazdák a felelősek.. Az ebbe a körbe tartozó információkat, adatokat, írott vagy nyomtatott formában, a „Titkos” megjelöléssel kell ellátni.

(1) Az intézmény számítástechnikai eszközeinek használatával összefüggésben az adat és titokvédelemre vonatkozóan a személyiségi jogok, az egészségügyi adatok védelméről és az adatvédelemről szóló törvények az irányadóak.

(2) Az üzemeltetői jogosultságok által megszerezhető, ill. tevékenységek naplózásával, forgalom ellenőrzésével, továbbá más számítástechnikai eszközökkel gyűjtött információk csak a működés érdekében, a rendellenességek kiszűrésére, a szabálysértő magatartás felderítésére használhatók.

(3) Valóságos személyi adatokat tartalmazó rendszerek oktatási célra nem használhatók.

(4) Az eredeti adathordozókról biztonsági másolatot kell készíteni és az eredetit biztonságos helyen kell tárolni. Az eredeti adathordozókról az illetékes rendszergazda külön nyilvántartást vezet.

(5) Az adatvédelmi felelősi tevékenységgel járó teendőket, az intézmény vezetője által kijelölt személy látja el.

(6) Az adatvédelmi felelős a szoftverek szabályszerű tárolásáért és használhatóságáért, köteles az adatok védelméről a mindenkori jogszabályok, illetve a Szabályzat előírásai szerint gondoskodni, s ellenőrzési jogát és kötelezettségét is e körben gyakorolja, illetve teljesíti.

(7) A szabályzatban nem, vagy nem kellő részletességgel szabályozott kérdésekben a hatályos jogszabályok rendelkezései az irányadóak.

A számítástechnikai szaktantermek használati rendje

(1) A szaktantermet az intézmény diákjai és dolgozói a következő megkötések figyelembevételével használhatják:

a) Munkanapokon 7 órától 18 óráig. Munkaszüneti napokon csak az intézmény vezetőjének írásos engedélyével vehetők igénybe.

b) A terem kulcsát diákok nem kezelhetik. A teremből való távozás előtt a kulcsot használó személy feladata még az eszközök hiánytalanságának ellenőrzése, a terem áramtalanítása, ablakok bezárása, légkondicionáló berendezés kikapcsolása.

c) A szaktantermi hardverek, szoftverek használatára a „Szabályzat a számítástechnikai eszközök (hardverek, szoftverek, hálózat) intézményi kezelésére” c. dokumentumban leírtak vonatkoznak.

d) A 107.sz. szobában lévő eszközöket, különös tekintettel a hálózati eszközökre és szerverekre, a vonatkozó utasítások betartásával kizárólag a rendszergazdák használhatják. A 107.sz. szobában diák csak rendszergazdai felügyelet mellett tartózkodhat, az ott lévő gépeket ebben az esetben sem használhatja.

Általános szabályok:

e) A termekben enni, inni, dohányozni szigorúan tilos. Ételt, italt csak táskába elzárva lehet bevinni.

f) A kabátokat az erre a célra rendszeresített fogasokon kell tárolni.

g) A teremben engedéllyel nem rendelkező személy nem tartózkodhat. Azok számára, akik alkalmi jelleggel egy meghatározott időpontban szeretnének a teremben dolgozni, és engedéllyel nem rendelkeznek, lehetőség van "ideiglenes teremhasználati engedély" kiállítására. Ebben az esetben az engedélyezettre a következő korlátozások és megkötések vonatkoznak:

- a termet csak az engedélyen szereplő időpontban használhatja,
- kizárólag az engedélyen feltüntetett gépen dolgozhat.

h) A teremben dolgozók mindegyike egyetemlegesen teljes anyagi és erkölcsi felelősséggel tartozik a terem rendjéért, az ott elhelyezett eszközökért.

i) A teremhasználati engedély visszavonható, ha tulajdonosuk a teremhasználatra vonatkozó szabályokat megszegik.

j) A teremben dolgozók mindegyike köteles bármely eszközön észlelt hiba esetén haladéktalanul értesíteni a rendszergazdát.

k) Ezt a dokumentumot minden szaktanteremben ki kell függeszteni.

l) Az intézmény kollégiumában működő számítógépteremre vonatkozóan is ez a szabályzat az irányadó. Az eltérő rendelkezéseket a kollégium számítógéptermében ki kell függeszteni.

8. § Vagyonvédelem

(1) A számítástechnikai eszközökre, szoftverekre a vagyonvédelemre vonatkozó általános szabályok az irányadóak.

(2) A számítógépet kezelő dolgozó a számítástechnikai eszközt – gépet – jegyzék alapján veszi át. Az átvett eszközökért leltárilag felelős. Az általa kizárólagosan használt gépben (eszközben) bekövetkezett kárért az oktató, dolgozó,tartozik kártérítési felelősséggel.

(3) Az iskola diákja a hatályos jogszabályok szerint tartozik fegyelmi felelősséggel az általa, a számítástechnikai eszközökben, okozott kárért.

(4) Az intézmény vezetése köteles biztosítani a portai szolgálaton keresztül, hogy azokba a szobákba, irodákba, amelyekben számítógép, illetve tartozékai vannak elhelyezve, a tanáron, illetve az iroda dolgozóján, a rendszergazdákon kívül más személy ne juthasson be.

(5) A diák nem szaktantermi gépet csak külön engedéllyel használhat, kizárólag tanulmányi vagy kutatómunkára. A gépet csak az adott gépet használó tanár, vagy dolgozó engedélyével használhatja. Ha a tanári, dolgozói gép diák általi használata rendszeres, erről az intézmény vezetőjét tájékoztatni kell.

(6) A géptermekben és a számítógépek közelében csak CO_2 oltó készüléket szabad használni. A géptermekben és azokon a helyeken ahol a számítógépek folyamatosan üzemelnek a tűzoltó készülékek meglétéről, azok üzemkészségéről az intézmény köteles gondoskodni.

(7) A tűz- és vagyonvédelmi berendezést a portás működteti, külön szabályzat szerint.

(8) Tilos más felhasználók tevékenységének zavarása, illetéktelen jogosultságok és adatok megszerzése, jogosultságok átadása, a szoftverek és a hardver elemek megrongálása, működőképességük veszélyeztetése, eszközök jogosulatlan megbontása vagy önkényes átkonfigurálása, a szoftver licence-jogok megsértése (pl. a szerzői joggal védett szoftverek másolása).

9. § Géptermek, gépek bérbeadása

(1) Az intézményhez nem tartozóknak a géptermek vagy gépek külön megállapodás szerint adhatók bérbe kizárólag oktatási, kutatási feladatokra. A bérbevevő köteles betartani és betartatni jelen szabályzatot. Megsértése esetén a bérbevevő ellen az intézmény köteles eljárni.

(2) Az intézmény a rendszergazdákon keresztül köteles felügyeletet biztosítani a bérbevevőnek, mely tényt a szerződésben rögzíteni kell.

Az számítógépek és felhasználók csoportosítása biztonság szerint

A számítógépeket biztonsági csoportokba soroljuk, amely meghatározza a felhasználók körét, és az azokon végezhető tevékenységeket.

a) kategória A tanárok, tanulók saját eszközei. Ezek az eszközök az iskolai infrastruktúrához csak korlátozott mértékben férhetnek hozzá. A rendszer szolgáltatásainak csak szűk részét vehetik igénybe.
b) kategória Azok a gépek, amelyek csoportosan közvetlenül az oktatást szolgálják, ebbe a kategóriába tartoznak a géptermekben, valamint a gyakorlóirodában található számítógépek,.
c) kategória Azok a gépek, amelyek az osztálytermekben digitális táblákhoz vagy kijelzőhöz, projektorhoz kapcsolódnak.
d) kategória A tanári felkészülést segítő gépek, amelyeken elsősorban nem kiemelt felhasználók dolgoznak. Ebbe a kategóriába tartoznak a tanári számítógéptermek, a könyvtár, a testnevelés tanári gépei.
e) kategória A kiemelt felhasználók gépei, ebbe a kategóriába tartoznak az informatika tanári, valamint az operátori szobák számítógépei.
f) kategória Az iskolai adminisztráció gépei. Ide tartoznak az igazgatói és igazgatóhelyettesi iroda, a titkársági, iskolatitkári, valamint a gazdasági terület, műhely számítógépei kollégiumi tanári szoba.
g) kategória Az intézmény által üzemeltetett valamennyi

szerver és hálózati eszköz. A felhasználókat is csoportokba soroljuk

az általuk végezhető tevékenységek szerint.

a) kategória **Tanulók** azok, akik az iskolával tanulói jogviszonyban állnak. Ebbe a csoportba tartoznak az ideiglenes jelleggel nálunk tanuló olyan diákok, hallgatók is, akik tanfolyam, cserekapcsolat vagy egyéb okból hosszabb ideig az intézmény területén tanulnak.
b) kategória **Tanárok** azok, akik az iskolában állandó, vagy ideiglenes jelleggel tanítanak, ideértve az alkalmazotti jogviszonyban állókat, akik valamilyen okból jelenleg nem tanítanak. (például: GYES, GYED, tartós kiküldetés)

c) kategória **Dolgozók** azok, akik az intézményben nem tanári beosztásban dolgoznak.
d) kategória **Kiemelt felhasználók** azok, akiknek a rendszergazdák saját jogkörük egy részét delegálták, szakmai hozzáértésük megvan a feladatkörük ellátásához.
e) kategória **Rendszergazdák** azok, akik az intézmény legalább egy szerverén rendszergazdai feladatokat látnak el.

10. § Kiskorúak online biztonsága

Jelen szabályozásban a Magyarország Digitális Gyermekvédelmi Stratégiája dokumentum (letölthető: https://www.kormany.hu/download/6/0e/c0000/Magyarorsz%C3%A1g%20Digit%C3%A1lis%20Gyermekv%C3%A9delmi%20Strat%C3%A9gi%C3%A1ja.pdf) irányelveit és iránymutatásait vettük alapul, kiegészítve a helyi sajátosságokkal.

Ennek alapján iskolánkban is a három stratégiai célként megfogalmatzott irányelvek mentén szervezzük meg a digitális gyermekvédelmet.

- Tudatosítás és médiaműveltség
- Védelem és biztonság
- Szankcióalkalmazás és segítségnyújtás

11. § Jelszó kialakításának szabályai

(1) A jelszó célja az, hogy illetéktelenek számára megakadályozza a felhasználói fiók és általában a rendszer elérését, ezért kialakításánál a következőket kell figyelembe venni:

a) A jelszó minimális élettartalma 14 nap, maximális élettartalma 365 nap.

b) A jelszó hossza nem lehet rövidebb 7 karakternél.

c) Csak betűkből és számokból és speciális karakterekből (pl.: _ @ - ? / # & $) álló karaktersor lehet.

d) A jelszó ne tartalmazza az alábbiakat:

i) Nevünk bármely részét vagy családunk bármely tagjának nevét (ide értve ismerőseinket és a háziállatokat is)

ii) Velünk vagy hozzánk közelállókkal kapcsolatos számokat: születési dátum, autórendszám, telefonszám, igazolványszám stb, valaminek vagy valakinek a nevét, aki fontos volt, vagy most is fontos számunkra. (lehet ez kedvenc ételünk, előadóművész, mozi vagy TV sztár, továbbá hely, sportcsapat, kedvenc időtöltésünk)

iii) Intézményünkkel, valamint az oktatással kapcsolatos bármilyen szám, név, személy.

e) A jelszónak amennyire csak lehet, a jelszófeltörő programokkal szemben is ellenállónak kell lennie, ezért az alábbiakat ne válasszuk jelszónak:

i) Helyesen leírt angol szavak (mivel felsorolásuk az online szótárak felhasználásával nagyon könnyen elérhető). Ez vonatkozik más nyelvterületre is.

ii) Helyesen leírt rövidített szavak.

iii) Nyilvánosságra hozott jelszóminták.

(2) Helytelen, könnyen kideríthető jelszót használók, jelszavukat másoknak átadók, vagy hanyagul tárolók a rendszerből kitilthatóak.

(3) A számítógépes hálózat üzemeltetéséhez szükséges felhasználónév jelszó párosokat külön-külön lezárt borítékban biztonságos elzárt helyen kell tárolni.

(4) Az alábbiakban néhány egyszerű módszer helyes jelszó kialakítására.

a) A rossz jelszavak egyszerű módosítása, pl. kiegészítésük egy karakterrel, visszafelé írva őket vagy a betűk permutálása továbbra is rossz jelszókat eredményez. Például ne csak a „john” jelszót kerüljük el, de ennek a „nhoj”, „ohnj” és „john2” vagy ezek hasonló változatait is.

b) Az olyan jelszavak, amelyeknél a közönséges szavakon a következő módosítások közül kettőt vagy többet alkalmazunk, sokkal jobb választásnak bizonyulhatnak:

i) Egy vagy több különleges karakter (különösen szimbólumok) használata.

ii) Hibás helyesírás, egy vagy több karakter helyettesítése másikkal, két vagy több karakter helyének felcserélése,

iii) Szokatlan nagy és kisbetű kombináció. Nem szokatlan, ha mindent kisbetűvel írunk, ha mindent nagybetűvel írunk, vagy ha a szavakban fordított nagybetű-kisbetű írást használunk (pl.: „StarTreck”, „sTARtRECK”). Nem szokatlan a magánhangzó nagybetűvel írása.

iv) A jelszóválasztás egyik jelenlegi divatja, hogy egy jól megjegyezhető mondás, vagy dalszöveg szavainak kezdőbetűiből állítják össze. Pl.: „jobb ma egy veréb, mint holnap egy túzok” Jelszó: „jmevmhet”, jobb jelszó: „Jm1vmh1T”.

11. § Értelmező rendelkezések

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

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

Adatállomány: egy nyilvántartásban kezelt adatok összessége.

Adatátvitel: elektronikus adatok informatikai rendszerek közötti továbbítása, amely lehet párbeszédre épülő (online) vagy nem párbeszédre épülő (offline) elektronikus kapcsolat. **Adatbázis:** azonos minőségű (jellemzőjű), többnyire strukturált adatok összessége, amelyet a tárolására, lekérdezésére és szerkesztésére alkalmas szoftvereszköz kezel.

Adatfeldolgozás: az adatkezeléshez kapcsolódó technikai feladatok elvégzése.

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

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

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

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

Archiválás: a ritkán használt, meghaladottá vált, de nem selejtezhető adatok,

adatbázisrészek változatlan tartalmi formában történő hosszú távú megőrzése.

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

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

Belső felhasználó: a NYSZC SZÉCHENYI valamennyi foglalkoztatottja, tanulója.

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

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

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

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

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

Biztonsági kockázat: az informatikai rendszerrel szembeni fenyegetés, amely a rendszer rendeltetésszerű működését és/vagy a rendszerben kezelt adatok

bizalmasságát, rendelkezésre állását, sértetlenségét veszélyezteti vagy veszélyeztetheti.

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

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

Biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége.

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

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

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

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

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

Felhasználók: a 2.1. pontban meghatározott személyek.

Fizikai biztonság: illetéktelen személyek információs infrastruktúrához, vagy információkhoz való szándékos, vagy véletlen fizikai hozzáférése elleni intézkedések összessége, valamint az illetéktelen személyek, vagy illetékes személyek jogosulatlan

tevékenységével szemben az adott struktúrák ellenálló képességét növelő tervek és útmutatások összessége.

Folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem.

Funkcionális rendszer: a NYSZC SZÉCHENYI működését támogató informatikai rendszer vagy alkalmazás.

Hardver: az informatikai rendszer vagy számítógép fizikai elemei

Hálózat: számítógépek és hozzájuk kapcsolódó eszközök meghatározott szabályok szerinti összekapcsolása, amely adat- és információcserét tesz lehetővé.

Helyreállítás: valamilyen behatás következtében megsérült, eredeti funkcióját ellátni képtelen, vagy ellátni csak részben képes infrastruktúra-elem eredeti állapotának és működőképességének biztosítása, eredeti helyen.

Hitelesítés: a rendszerbe kerülő, ott lévő és onnan kikerülő adatok forrásának (az adat közlőjének), megbízható azonosítása.

Hitelesség: annak biztosítása, hogy a rendszerbe kerülő adatok és információk eredetiek, a megadott forrásból az abban tárolttal azonos, változatlan tartalommal származnak.

Hozzáférés: az infokommunikációs rendszer, vagy rendszerelem használója számára a rendszer szolgáltatásainak, vagy a szolgáltatások egy részének ellenőrzött és szabályozott biztosítása.

Illetéktelen személy: olyan személy, aki az adathoz, információhoz, az informatikai infrastruktúrához való hozzáférésre nem jogosult.

Infokommunikáció: az informatika és a telekommunikáció, mint konvergáló területek együttes neve.

Informatikai alkalmazás: számítógépen, illetve egyéb informatikai eszközön futó program.

Informatikai biztonság: az informatikai rendszer olyan állapota, amikor a rendszer rendeltetésszerűen működik és a rendszerben kezelt adatok bizalmassága, rendelkezésre állása, sértetlensége biztosított.

Informatikai biztonsági incidens: az informatikai rendszerrel szemben olyan külső, vagy belső előre tervezett, szándékos károkozású, vagy nem szándékos cselekmény, melynek célja a NYSZC SZÉCHENYI kezelésében lévő adatok, dokumentumok és egyéb

információk jogosulatlan megismerése, megszerzése, módosítása valamint további károkozással kapcsolatos felhasználása.

Informatikai biztonsági követelmények: az informatikai rendszer használatával, üzemeltetésével és fejlesztésével kapcsolatos elvárások. Részterületei: a számítógépes biztonság, a kommunikációs biztonság, a kisugárzás biztonság és a rejtjelbiztonság.

Informatikai biztonsági politika: a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása meghatározott biztonsági feladatok irányítására és támogatására.

Informatikai biztonsági stratégia: az informatikai biztonságpolitikában kitűzött célok megvalósításának útja, módszere.

Informatikai infrastruktúra: a NYSZC SZÉCHENYI-hez kapcsolódó feladatokat ellátó, illetve a NYSZC SZÉCHENYI működését biztosító hálózatba kapcsolt hardverelemek, az azokon futó szoftverek és a rajtuk megtalálható adatok együttese, amely jól körülhatárolható, önmagában is működőképes, önálló szolgáltatás nyújtására képes infrastruktúra elemekből áll.

Informatikai rendszer: a számítógépek és a hozzájuk kapcsolódó eszközök (hálózat), a számítógépeken futó programok, valamint a számítógépeken kezelt, feldolgozott adatok együttese.

Informatikai vészhelyzet: a NYSZC SZÉCHENYI információs infrastruktúrájának leállása, szolgáltatások megszakadása, elérhetetlensége, a NYSZC SZÉCHENYI nemzeti információs vagyonának jelentős mértékű sérülése, illetve az ezekkel fenyegető rendellenes működés.

Információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.

Információbiztonság: az adatok és információk szándékosan, vagy gondatlanul történő jogosulatlan gyűjtése, károsítása, közlése, manipulálása, módosítása, elvesztése, felhasználása, illetve természeti vagy technológiai katasztrófák elleni védelmének koncepciói, technikái, technikai, illetve adminisztratív intézkedései. Az információbiztonság része az informatikai biztonság is, melynek alapelvei a bizalmasság, sértetlenség, rendelkezésre állás.

Információvédelem: szervezeti, személyi, fizikai, informatikai és adminisztratív

előírások kidolgozása és intézkedések végrehajtása az információbiztonság érdekében.

Jogosultság: az arra felhatalmazott által adott hozzáférési lehetőség valamely információs infrastruktúrához.

Kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye.

Kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése.

Kockázattal arányos védelem: az elektronikus információs rendszer olyan védelme, amelynek során a védelem költségei arányosak a fenyegetések által okozható károk értékével.

Következmény: valamely esemény, baleset, beavatkozás, vagy támadás hatása, amely tükrözi a belőle eredő veszteséget, valamint a hatás jellegét, szintjét és időtartamát.

Külső felhasználó: a NYSZC SZÉCHENYI-vel szerződéses jogviszonyban álló magánszemélyek, jogi személyek és jogi személyiséggel nem rendelkező egyéb szervezetek és ezek alkalmazottai.

Mentés (biztonsági mentés): biztonsági másolat készítése az informatikai rendszerben tárolt adatokról, adatállományokról, illetve az informatikai rendszerben használt alkalmazásokról. A másolat célja az elsődleges adattároló megsérülése esetén az adatok helyreállíthatóságának biztosítása.

Mobil eszköz: asztali munkaállomásnak nem minősülő egyes informatikai és kommunikációs feladatok ellátására használható, operációs rendszerrel, kommunikációs szolgáltatásokkal rendelkező, hordozható elektronikus eszköz. Ide tartoznak: laptopok, notebookok, táblagépek, mobiltelefonok és okostelefonok.

Munkaállomás: a felhasználó számára biztosított számítógép; lehet asztali vagy hordozható (laptop, notebook).

Napló: az informatikai rendszerben bekövetkező eseményeket, felhasználói tevékenységeket és ezek időpontját rögzítő, a rendszer által automatikusan kezelt adatállomány, amely a változások észlelését és a számon kérhetőséget biztosítja.

Naplózás: az informatikai rendszerben bekövetkező események, felhasználói tevékenységek és ezek időpontjának automatikus rögzítése a változások észlelése és a

számon kérhetőség biztosítása érdekében.

Osztályozás: adatok, információk, információs infrastruktúra elemek, információs infrastruktúrák biztonsági szempontból való osztályainak kialakítása és ez alapján osztályokba sorolása.

Program: számítógépes nyelven megírt utasítássorozat. Állhat egyetlen programmodulból vagy programmodulok halmazából.

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

Rendszerelem: információs infrastruktúra elem.

Sebezhetőség: olyan fizikai tulajdonság, vagy működési jellemző, amely az adott információs infrastrukturális elemet egy adott veszéllyel szemben érzékennyé vagy kihasználhatóvá teszi.

Személyi biztonság: az adott rendszerrel/erőforrással kapcsolatba kerülő személyekre vonatkozó, alapvetően a hozzáférést, annak lehetőségeit és módjait szabályozó biztonsági szabályok és intézkedések összessége a kapcsolat felvétel tervezésétől, annak kivitelezésén keresztül a kapcsolat befejezéséig, valamint a kapcsolat folyamán a személy birtokába került információk vonatkozásában.

Szervezeti biztonság: egy adott szervezet strukturális felépítéséből adódó biztonsága és bevezetett biztonsági szabályainak és intézkedéseinek összessége a védendő rendszerhez/erőforráshoz való hozzáférés védelme érdekében.

Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

Szoftver: a számítógép, az informatikai rendszer logikai elemei; a működtető programok (rendszerprogramok, operációs rendszerek) és a felhasználói programok (alkalmazások) összefoglaló neve.

Teljes körű védelem: azon bármilyen típusú aktív, vagy passzív védelmi intézkedések, melyek a rendszer összes elemére kiterjednek.

Tesztrendszer: olyan informatikai rendszer (környezet), amelynek célja a fejlesztés

vagy bevezetés alatt álló program kipróbálásának, oktatásának támogatása.

Titkosítás: az informatikai rendszerben kezelt adatok bizalmasságának biztosítására szolgáló, nem a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet hatálya alá tartozó olyan tevékenység vagy eljárás, amelynek során az adatot úgy alakítják át, hogy annak eredeti állapota a megismerésére illetéktelenek számára rejtve maradjon, de a megismerésre jogosultak számára az adat az eredeti formájába visszaállítható legyen.

Veszély (fenyegetés): természeti vagy mesterséges esemény, személy, szervezet vagy tevékenység, amely potenciálisan káros a jelen szabályzatban védett tárgyakra.

Védelem: a biztonság megteremtésére fenntartására, fejlesztésére tett intézkedések, amelyek lehetnek elhárító, megelőző, ellenálló képességet fokozó tevékenységek, vagy támadás, veszély, fenyegetés által bekövetkező kár kockázatának csökkentésére tett intézkedések.

Visszaállítás: az eredeti infokommunikációs rendszer kiesése esetén a szolgáltatások további biztosítása, korábbi mentésből való visszaállítása.

Zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.