BALATONI REGIONÁLIS TÖRTÉNETI KUTATÓINTÉZET, KÖNYVTÁR

ÉS

KÁLMÁN IMRE EMLÉKHÁZ

Informatikai Biztonsági Szabályzata

Siófok, 2018. december 30.

Készítette:

Laki Judit
igazgató

Tartalomjegyzék

Jogszabályok

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.
- 305/2005. (XII.25.) Korm. rendelet a közérdekű adatok elektronikus közzétételére, az egységes közadatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról.
- 2016/679 Európai Parlament és Tanács rendelete 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.
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól.
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információ-biztonságáról.

Az Informatikai rendszer biztonságos működtetése

Az informatikai szabályzat célja, hogy az információk, bizalmasságát, sértetlenségét, valamint rendelkezésre állását veszélyeztető kockázati tényezők azonosításával, a kockázatok csökkentésével biztosítsa az informatikai biztonság növelését, szinten tartását.

Az informatika biztonság fenntartása érdekében a jelentős változás esetén (új technológia, szolgáltatások be-/ és kivezetése) legalább háromévenként felmérést kell végrehajtani az informatikai rendszer teljes elemére (technikai eszközök, személyek, eljárások, szabályok).

A felmerülő kockázatok kezelésére, a feltárt akadályok, gondok csökkentése, megszüntetése érdekében tervet kell készíteni, az alábbi tényezők feltüntetésével:

- javaslatokat a technikai eszközök változtatására, vagy fejlesztésére (pl.: új védelmi eszközök beszerzése vagy a jelenlegi átkonfigurálása),
- javaslatok az érvényben levő szabályzatok megváltoztatására,
- javaslatokat a személyi állományra vonatkozóan.

Megelőző intézkedések:

- információtechnológiai védelmi intézkedések (hálózatvédelem, vírusvédelem, jogosultság kezelés) foganatosít annak érdekében, hogy a fenyegető tényezők ne lépjenek fel,
- szabályozott folyamatot vezet be, a biztonsági kontrollok működtetéséhez, illetve az esetleges incidensek feltárásához (jogosultságkezelés, fejlesztés, stb.).

Az informatikai biztonság irányításának alapjai

Annak érdekében, hogy az informatikai biztonság folyamatosan, minden területen a kívánt biztonsági szinten működjön, az alábbi irányelveket kell érvényesíteni a napi munka során:

- a szabályzat személyi hatálya alá tartozó személyeknek az IBSZ-ben foglalt előírások ismeretében és azokat betartva kell munkájukat végezniük;
- az informatikai biztonsági incidenseket észlelésükkor jelentenie kell az észlelőnek az informatikai biztonságért felelős személynek és az intézmény vezetőjének. A bejelentés e-mailben, telefonon és személyes közlés módján történjen;
- az informatikai biztonsági incidenseket az incidens kezelőjének részletesen szükséges dokumentálnia, hogy elemezni lehessen ezek számosságát, időtartamát és hatását;
- a biztonsági incidensekből levont tapasztalatokat folyamatosan értékelni kell, és azokat figyelembe kell venni a védelmi rendszer tervezése, szervezése és működtetése során.

Helyesbítő intézkedések rendszere

Az incidensek természetét és gyakoriságát az Informatikai Biztonsági Felelősnek kell figyelemmel kísérnie, illetve szükség esetén javaslatot tennie a védelmi intézkedések módosítására.

Védelmi intézkedés módosítása az alábbi esetekben:

- amennyiben a korábbi intézkedés szintje nem érte el a kívánt biztonsági szintet, meg kell fontolni egy szigorúbb intézkedés bevezetését;
- amennyiben az informatikai rendszer változása miatt a korábbi biztonsági kontrollok érvényüket vesztik;
- amennyiben az adott kontroll elavul és/vagy jobb, újabb technológiák bevezetése válik indokolttá.

Informatikai Biztonsági Felelős

Felelőssége:

- a biztonsági szabályok betartatása, az üzemeltetési folyamatok során, az informatikai biztonság elvárt szintjének a biztosítása, folyamatos fejlesztése, intézkedési javaslatok megfogalmazása a biztonsági incidensek megelőzésére, illetve a bekövetkezett incidensek hatásának mérséklésére;
- felelős a beszerzések, informatikai fejlesztések során a biztonsági követelmények érvényre juttatásáét, egy bekövetkezett informatikai biztonsági esemény kapcsán az okok feltárásáért, a felelősök beazonosításáért;
- az intézménnyel bármilyen módon adatforgalmi, illetve információátadási/fogadási kapcsolatban (adathálózat, adathordozók cseréje, stb.) álló külső szervekkel történő szerződéskötés esetén – a BRTKK érdekeinek lehető legteljesebb védelme érdekében – az informatikai részekkel kapcsolatban ellenőrzési, javaslattételi joga és kötelezettsége van;
- a BRTKK informatikai védelmi- és biztonsági rendszere tervezésében való részvétel;
- az informatikai védelmi- és biztonsági rendszer rendszeres felülvizsgálata, a védelmi eszközökkel való ellátottság rendszeres ellenőrzése;
- a BRTKK adatkezelési tevékenységének és az informatikai kommunikációs hálózatának informatikai biztonsági szempontú ellenőrzése;
- az általa észlelt vagy hozzá beérkezett bejelentések alapján, az adatfeldolgozás- és kezelés biztonságát sértő események kivizsgálása – az esetleges rossz szándékú hozzáférési kísérletek, illetéktelen adatfelhasználás kiszűrése;
- az informatikai rendszerben kialakított, aktuálisan beállított jogosultságok és a jóváhagyott jogosultságok összevetése, ellenőrzése;
- az informatikai munkafolyamat bármely részének előzetes bejelentési kötelezettség nélküli ellenőrzése;
- az információ és informatikai biztonság tudatosságának növelése.

Biztonsági területek

- vírusvédelem;
- határvédelem (tűzfalak, spamszűrő, aktív hálózati eszközök, VPN);
- mentések;
- jogosultság-kezelés;
- alkalmazás üzemeltetés.

Felhasználó

- felelős a feladatai ellátása érdekében az informatikai eszközök rendeltetésszerű használatáért,
- felelős az informatikai Szabályzatban leírtak betartásáért;
- **a BRTKK informatikai infrastruktúráját kizárólag munkájával összefüggő feladatok végzéséhez használhatja;**
- köteles minden olyan tudomására jutott információt, eseményt, körülményt a munkahelyi vezetőjének jelezni, amely az intézmény információs rendszerei biztonságos működését veszélyezteti, a funkcionális működési rendjét sérti;
- köteles azonnal jelenteni az informatikai eszközök és alkalmazások működésében bekövetkezett hibákat, rendellenességeket;
- felelős a rábízott a BRTKK tulajdonát képező információs eszközök megőrzéséért, rendeltetésszerű használatáért, a kezelési előírások maradéktalan betartásáért;
- az eszközökön lévő információk védelme;
- a felhasználó a BRTKK informatikai rendszerében saját tulajdonú eszközt csak előzetes bejelentés és nyilvántartásba vétel esetén használhat;
- az eszköz használata megtiltható, ha az eszköz nem vállalható biztonsági kockázatot rejt.

Külső partnerek

- kiemelt figyelmet kell fordítani a külső ügyfelek/szerződéses munkavállalók tevékenységében rejlő kockázatok azonosítására és kezelésére;
- a kockázatok kezelésére olyan írásbeli megállapodást – „Titokvédelmi megállapodást/záradékot – kell kötni, amely tartalmazza, vagy utal olyan biztonsági követelményre, amely biztosítja az Informatikai Szabályzatnak és a BRTKK –n bevezetett szabályoknak való megfelelést;
- az informatikai rendszerhez és információihoz külső fél számára megfelelő hozzáférést biztosítani csak a titokvédelmi megállapodás aláírását követően lehet;
- a titokvédelmi megállapodást a külső felekkel kötött szerződések mellékleteként kell megőrizni, a jogosultságigényléskor pedig utalni kell arra, hogy a Titoktartási megállapodás rendelkezésre áll;
- a külső fél számára – amennyiben értelmezhetőek – a következő feltételeket kell dokumentáltan a rendelkezésükre bocsátani vagy a velük kötött kötött szerződésbe foglalni:
- az Informatikai Biztonsági Szabályzat biztonsági követelményeit,
- a BRTKK kezelésben levő adatok másolásának és nyilvánosságra hozatalának korlátozásait;
- hozzáférés-ellenőrzési megállapodás;
- a megengedett hozzáférési kódokat;
- a hozzáférés és a jogosultságkezelés folyamatát;
- a külső személy képviselőinek egyértelmű megfeleltetését az igénybe vehető informatikai szolgáltatásokkal, azok használatára vonatkozó jogokkal és kiváltságaikkal együtt;
- a hozzáférési mód ellenőrzési feltételeit;
- a problémamegoldás folyamatát;
- a biztonsági eseményekről és a biztonság megsértéséről szóló jelentési kötelezettségek, értesítések és a kivizsgálásokra vonatkozó intézkedéseket;
- a szerződés teljesítésébe további alvállalkozók bevonásának feltételeit, titoktartásukra vonatkozó megállapodásokat;

- az informatikai rendszerében a külső személyek által távolról elért, menedzselt vagy diagnosztizált eszközeihez való kapcsolódást minden hozzáférés igénylésekor egyedileg kell engedélyezni és felügyelni;
- a hozzáférés indokának megszűnte okán a külső személyek hozzáférési jogát azonnal meg kell szüntetni, illetve a szerződés lejártakor is hasonló módon kell eljárni.

Titoktartási megállapodások

Minden alkalmazottnak és a BRTKK informatikai rendszereit és /vagy szolgáltatásait használó külső szervezetnek (cég, egyéni munkavállaló) titoktartási nyilatkozatot kell aláírnia, melyben nyilatkozik arról, hogy a munkája során tudomására jutott, a nem publikus információkat sem a munkavégzés során, sem annak vége után nem hozza harmadik fél tudomására.

Informatikai vagyontárgyak

Valamennyi informatikai vagyontárgyat (információ-feldolgozó eszközt vagy ahhoz kapcsolódó kiegészítő eszközt, perifériát, tároló eszközt) egyértelműen azonosítani kell és valamennyi vagyontárgyról eszközleltárt kell felvenni és folyamatosan karbantartani.

A nyilvántartásban szerepeltetni kell a következő konfigurációs-elemeket:

- hardver elemek (kiszolgálók, kliensek, hálózati aktív és passzív eszközök, háttértárolók, nyomtatók, stb.);
- szoftver elemek (operációs rendszer, alkalmazás, fejlesztőeszköz, stb.);
- információs elemek (adatbázisok, adatállományok, stb.);
- dokumentációs elem (rendszerkommunikációk, felhasználói kézikönyvek).

A nyilvántartásba vett információ-feldolgozó eszközhöz un. Vagyongazdát kell kinevezni, aki az adott eszközök biztonságáért felel.
Az információk, adatok hozzáférése esetében az Adatgazda, a hardverek, szoftverek esetében az Informatikai Biztonsági Vezető a felelős.

Az informatikai rendszerben csak az Informatikai Biztonsági Felelős által jóváhagyott, konfigurációs leltárba felvett:

- hardverelemeket lehet használni;
- jogtiszta szoftvert lehet telepíteni és/vagy futtatni.

Emberi erőforrások biztonsága

A BRTKK munkatársainak meg kell ismerniük az Informatikai Biztonsági Szabályzatot.
A közalkalmazotti jogviszony megszűnésekor az alábbi feladatokat kell végrehajtani:

- jogosultságok megszüntetése vagy módosítása úgy, hogy a régi állapot mentésre vagy dokumentálásra kerül;
- a felhasználó (a BRTKK munkájához kapcsolódó) elektronikusan tárolt információit, e-mailjeit és egyéb általa létrehozott hivatalos adatot másolni kell az általa használt informatikai eszközről, illetve bármely egyéb adathordozóról és biztosítani szükséges a kilépő dolgozó által használt szerver tárhely hozzáférését a munkahelyi vezető által megadott felhasználó számára és biztosítani kell az e-mailjeinek megadott címre történő továbbítását;
- a BRTKK a hálózati meghajtókat és levelezőrendszerét a munkavégzés támogatására vezette be, az esetlegesen itt tárolt magáncélú tartalmakról, levelekről a jogviszony megszűnésekor az intézmény megkeresésre sem készít semmilyen adathordozón másolatot;
- a felhasználó feladata ezen tartalmú levelek eltávolítása az intézmény levelezőrendszeréből;
- a jogviszony megszűnését követő 30 nap múlva a kilépő munkavállaó intézményi elektronikus levelező címét az informatika megszünteti, törlik, és ezt követően az intézmény nem vállal felelősséget a munkahelyi e-mail címre címzett levelekért;
- a munkahelyi vezető intézkedik arról, hogy a kilépés napja és az e-mail cím megszüntetése közötti időszakra az átirányítást kérvényezze az általa megadott felhasználó e-mail címére.

Hozzáférési jogok megszüntetése

Valamennyi alkalmazottnak, a szerződőknek és harmadik feleknek az információkhoz és információ-feldolgozó eszközökhöz való hozzáférési jogosultságot fel kell függeszteni, meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár, vagy módosulás esetén a változáshoz kell igazítani.

Az informatikai környezet fizikai védelme

Azon terület, ahol információkat, vagy információ-feldolgozó eszközöket tárol az intézmény, biztonsági eszközzel kell védeni az illetéktelen hozzáféréstől.
A fizikai védelem során olyan megoldásokat kell bevezetni, melyek alkalmasak az egyértelmű és egyedi azonosításra.

Informatikai helyiség:

- szerver terem;
- biztonsági mentések.

Kiemelten védett a szerverszoba, ahol archivált, mentett anyagokat is tartalmaznak a tárolóegységek a többi adat mellett.
Általánosan védett kategóriái az irodai helyiségek, az adminisztráció területe, a tájékoztató-olvasószolgálati rész, az internetezést igénybevevők által használt számítógépes részleg.

Az informatikai helyiségek védelme

Mindegyik területre érvényes fizikai védelmi és tűzvédelmi szabályokat az intézmény Tűzvédelmi Szabályzata és az Informatikai Szabályzata tartalmazza.

Informatikai eszközök védelme

Az informatikai eszközöket úgy kell elhelyezni, illetve védeni, hogy kockázati besorolásuknak megfelelő mértékű legyen a környezeti fenyegetésekből és veszélyekből, valamint a jogosulatlan hozzáférés lehetősége.

Az adatátvitelt biztosító, információszolgáltatásokat támogató elektromos energiaátviteli és távközlési kábelhálózatot védeni kell az illetéktelen hozzáféréstől és a károsodástól:

- a táp és adat kábeleket lehetőleg föld, álpadló alatt, álmennyezet fölött vagy kábeltálcában kell elvezetni;
- a rendezőszekrényeket minden esetben kulcsra kell zárni.

Informatikai eszközök karbantartása

- informatikai eszközök, szoftverek csak a vezetőjének engedélyével vihetők ki szerviz, javítás céljából az intézményből;
- a szállítást csak az intézmény alkalmazottja vagy az intézménnyel szerződésben álló informatikus végezheti;
- a szolgáltató céggel kötött szerződésbe titoktartási kitételeket is bele kell foglalni;
- a szállítandó eszközöket megfelelő csomagolással kell ellátni a fizikai védelem érdekében;
- a meghibásodott informatikai eszközt a külső partner felé átadás-átvételi nyilatkozattal lehet átadni javítás céljából.

Mobil informatikai eszközök biztonsága az épületen kívül:

- csak vezetői engedéllyel;
- a használó részéről felelősségvállalási nyilatkozattal lehet használni;
- az eszköz nem maradhat felügyelet nélkül nyilvános helyen;
- a BRTKK informatikai rendszeréhez az intézményvezetője által engedélyezett módon lehet;
- a gyártó előírásait az eszköz fizikai védelme érdekében be kell tartani;
- idegen eszköz csatlakoztatása csak írásbeli engedéllyel lehet, mely tartalmazza a csatlakozási ok megjelölését és időtartamát.

Visszaállíthatatlan törlés

A visszaállíthatatlan törlés a szoftveres úton történő törlés esetében, ugyanazon adathordozó legalább háromszoros, titkos adatok/kiemelten védett rendszerek esetében kilencszeres felülírását jelenti, adatot nem tartalmazó mintákkal.
Működésképtelen vagy törölhetetlen eszköz esetében, fizikai törlést kell alkalmazni, az erre alkalmas eszközzel.

Védelem rosszindulatú és mobil kódok ellen

Vírusvédelem:

- az informatikai eszközökre telepíteni kell az ismert sebezhetőségeket kiszűrő, hibákat megszüntető aktuális védelmi programokat illetve javítócsomagokat;
- a felhasználók a BRTKK eszközein csak a BRTKK által biztosított és felügyelt szoftvereket használhatják;
- a BRTKK által nem ismert és tesztelt szoftvert a felhasználók nem tölthetnek le, a hálózatról nem futtathatnak, és nem telepíthetnek;
- szoftverek telepítését, futtatását csak a vezető által megbízott (szerződés alapján) informatikai szakember végezheti;
- a felhasználók kötelesek az adathordozón kapott bármilyen állományt a számítógépre telepített vírusvédelmi szoftverrel leellenőrizni;
- ahol lehetséges az ellenőrzést automatikus beállításokkal kell kikényszeríteni;
- vírusvédelmi adatbázisok rendszeres és automatikus frissítése.

Jogosultság kezelés

A jogosultság kezelés célja, hogy a BRTKK informatikai rendszerében a felhasználói hozzáférés életciklusának valamennyi fázisát lefedve biztosítsa, hogy minden felhasználó csak azokhoz az informatikai rendszerekben tárolt információkhoz, adatokhoz, programokhoz és szolgáltatásokhoz férjen hozzá, amelyek munkaköre ellátásához feltétlenül szükséges.

Az informatikai eszközökön tárolt adathoz hozzáférés csak az intézmény és a felhasználó közötti jogviszony létrejötte után és a megfelelő jogosultság ellenőrzését követően lehetséges.
A felhasználókat megillető jogosultságokat az intézményvezető határozza meg.
A felhasználói jogosultságokhoz szükséges azonosítókat a jogosultságkezelő (intézményvezető) tartja nyilván és zárt helyen tárolja.
Jogosultságokat a jogosultságkezelő engedélyezhet, és vonhat vissza.

Felhasználói jogosultságok alapszabályai:

- az adminisztrátori azonosítók jelszavait minimum 90 naponta meg kell változtatni, a jelszó hossza minimum 12 karakterből kell, hogy álljon vegyesen nagybetűket, számokat és írásjeleket tartalmazzon;
- a rendszerazonosítók (system account) jelszó (jelszavak) elzárva zárt borítékban az intézményvezető tárolja zárt tárolószekrényben.

A felhasználói jogosultságok létrehozása esetén:

- az alapértelmezett azonosítókat át kell nevezni és jelszavukat meg kell változtatni;
- a felhasználói azonosítót minden esetben egyedi felhasználóhoz kell rendelni, tulajdonosát egyértelműen azonosítani kell;
- ezen azonosítókat a tulajdonossal egyetemben az intézményvezető zárt helyen tárolja (írásos változat), más által hozzá nem férhető mappában az informatikai eszközön;
- az anonim azonosítókat fel kell függeszteni, illetve csak a használat idejére aktiválni lehet, majd használata utána fel kell függeszteni;
- kiemelt felhasználói jogosultságokat (adminisztrátori jogosultságok birtoklása) esetileg ki lehet osztani, majd a feladat végeztével visszavonni;
- a kiemelt felhasználói jogosultságok halmozását minden esetben kerülni kell;
- rendszeradminisztrátori jogosultságot az intézménnyel szerződésben álló (titoktartási kitétel) informatikai munkatárs kaphat, ettől eltérni csak az intézményvezető engedélyével lehet.

Hitelesítés és jelszavak:

- a jelszavak 8 karakterből álljanak, vegyesen kis és nagybetűket, számokat és írásjeleket tartalmazzanak;
- a felhasználói jelszavakat félévente változtatni szükséges;
- a felhasználó többszöri jelszó próbálkozása esetében 5 próbálkozás után zárolja az azonosítót;
- rendszergazdák jelszavát negyedévente cserélni kell;
- rendszergazda jelszava: minimum 12 karakter, ki-és nagybetűk, számok, írásjelek váltakozása;
- a rendszergazda téves jelszó használata esetén három próbálkozás után zárolja az azonosítót;
- a jelszó változtatásakor a megelőző 5 jelszó valamelyikét ne lehessen újból megadni;
- a kezdeti jelszót az első belépés alkalmával meg kell változtatni;
- tilos a jelszót más tudomására hozni;
- más számára ismert vagy hozzáférhető helyen tárolni (pl.: monitorra ragasztani);
- jelszó megadásakor ügyelni kell arra, hogy az ne legyen jellemző az adott személyre, és ne legyen könnyen kitalálható;
- a bejelentkezések során a jelszavak olvashatatlanul jelenjenek meg a képernyőn;
- titkosítva legyenek a hálózati adatátvitel során.

Jelszóválasztás szabályai:

- tilos a logon nevet használni jelszóként bármilyen formában;
- tilos a saját vezeték vagy keresztnév használata;
- tilos a jelszót valamely funkcióbillentyűhöz hozzárendelni;
- a jelszavak ne legyen könnyen kitalálhatók;
- ne legyen szótárakban található címszó;
- ne legyen a felhasználó személyéhez köthető;
- ne legyen 8 karakternél rövidebb;
- használjanak számokat, írásjeleket a betű mellé.

A felhasználói azonosítót inaktív állapotba kell helyezni, ha:

- munkaviszony/jogviszony megszűnik;
- 5 egymást követő sikertelen bejelentkezési kísérlet után;
- ha 6 hónapig nem történik bejelentkezés.

Rendszeres időközönként, évente egy alkalommal a felhasználói jogosultságokat felül kell vizsgálni.

IT szolgáltatások biztonsága

Elektronikus levelezés

Az elektronikus üzenetekben foglalt információkat védeni kell a következő módon:

- védeni kell az üzeneteket a jogosulatlan hozzáféréstől, módosítástól;
- biztosítani kell a pontos címzést és célba juttatást;
- biztosítani kell a szolgáltatás megbízhatóságát és hozzáférhetőségét;
- elektronikus aláírások használatát az arra feljogosultnak biztosítani kell;
- külső nyilvános szolgáltatásokat kontroll alatt kell tartani;
- azok a munkavállalók használhatják az elektronikus levelezést, akik rendelkeznek az ehhez szükséges jogosultsággal.

Logikai védelem – levélszűrés

Az elektronikus levelezés biztonságának megteremtését kéretlen levél (spam) szűtő rendszer alkalmazásával, valamint vírusvédelmi rendszer használatával kell biztosítani, melyet rendszeresen frissíteni kell.
A spam-ok minősítését a kéretlen levélszűrő rendszer használatával kell biztosítani.

Az elektronikus levelezés használatának belső szabályai:

- a levelezőrendszer elsődlegesen belső- és külső kommunikációt, a belső folyamatok támogatását szolgálja;
- az elektronikus levelezés használata során az intézmény fenntartja a jogot arra, hogy indokolt esetben betekintsen az elektronikus levelekbe;

- a felhasználók tudomásul veszik, hogy az általuk küldött és fogadott elektronikus küldeményeket az intézmény ilyen módon kezeli, és ennek elfogadásáról írásban nyilatkoznak (Dolgozói nyilatkozat);
- szükség esetén az elektronikus üzenetek bizalmasságának, illetve hitelességének, letagadhatatlanságának védelme érdekében – az adatok biztonsági osztályba sorolásának megfelelően – digitális aláírást és titkosítást kell alkalmazni;
- nyilvános levelezési fórumokon az intézménynél használt levelezési címet használni tilos;
- az intézmény levelezési címének feltüntetésével, felhasználásával – kivéve az intézmény érdekeit szolgáló, feladatait segítő – semmilyen kereskedelmi, hirdetési tevékenységben nem vehetnek részt;
- láncleveleket vagy hasonló üzenetek (ún. hólabda levelezés) küldésére tilos használni a levelező rendszert;
- vírusos levelek szándékos küldése;
- indokolatlanul nagy méretű üzeneteket vagy fájlokat küldeni;
- ismereten feladótól származó levelekben található csatolmány megnyitása;
- kéretlen levelek továbbküldése;
- valótlan információt hordozó levelek tudatos továbbítása;
- az elküldött levél adatainak (feladó e-mail cím, küldés időpont) meghamisítása;
- a munkatársak e-mail címeinek másik félhez történő, jogosulatlan továbbítása;
- a munkahelyi e-mail címről magáncélú regisztrációt végrehajtani tilos;
- nem engedélyezett a feliratkozás egyéb levelezési listákra, fórumokra, stb.;
- intézmény postafiók tartalmának továbbítása külső e-mail címre;
- a BRTKK elektronikus címjegyzékének kiadása harmadik félnek.

Elektronikus levélcímek készítése:

- egyedi levelezési címek;
- név (keresztnév/vezetéknév) @konyvtar-siofok.hu
- név(keresztnév/vezetéknév)@emlekhaz-siofok.hu

Az internet használata során követendő magatartás

A szerzői jogokra, szabadalmakra és egyéb szellemi tulajdonra vonatkozó szabályok alkalmazása az internetre is vonatkozik.

Ebből kifolyólag:

- az internetről származó anyagok felhasználása előtt beszerezni a forrástól az erre vonatkozó engedélyt;
- hivatkozáskor a forrást azonosítani;
- a BRTKK-val kapcsolatos információk honlapon történő közzétételéről az intézményvezető által megadott személy (ek) gondoskodhatnak, az előzőleg jóváhagyott tartalom közzétételéről.

Tiltott tevékenyégek az internet hálózaton:

- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illegális hozzáférés, azok illetéktelen használata, módosítása, megrongálása, megsemmisítésére irányuló tevékenység;
- a hálózat biztonságos működését zavaró vagy veszélyeztető információk programok terjesztése;
- hálózati forgalom lehallgatása, megfigyelése, kivéve, ha ez az adott munkakörhöz kapcsolódik;
- az internetről a legálisan hozzáférhető programok letöltése, kivéve, ha arra a vezető engedélyt adott;
- a szolgáltatások blokkolását, lassítását célzó támadás, az azonosítási, illetve biztonsági intézkedések megsértésére irányuló kísérlet, valamint az egyéb azonosítóhoz, számítógéphez vagy hálózathoz történő illetéktelen hozzáférési kísérlet;
- a felhasználói azonosítóval csak annak tulajdonosa léphet be;
- az adatokhoz történő hozzáférés érdekében választott jelszó titkosságának megőrzése a felhasználó felelőssége;
- az azonosító kölcsönadása nem megengedett, így a felelősségre vonás esetén ez az indok nem elfogadható;
- minden felhasználó számára tilos:

- sértő, társadalomra veszélyes, jó erkölcsbe ütköző szöveg, kép, ábra vagy egyéb formájú információ publikálása, letöltése;
- az interneten elérhető szolgáltatást, bármilyen törvényt, szabályozást, szabványt, nemzetközi egyezményt vagy díjszabást sértő módon használni;
- bármelyik számítógép hálózati biztonságát rombolni, illetve gyengíteni;
- más felhasználó jogosultságát jogosulatlanul használni;
- internetes végpontra, illetve hálózati eszközre jogosulatlanul csatlakozni;
- a hálózatot a szerzői jogvédelem alatt alá eső anyagok átvitelére használni (még közvetten is), ha az átvitel során mások szerzői joga sérül;
- tilos kikapcsolni a munkaállomásra telepített szoftvereket, eszközöket.

Nem látogathatók azon oldalak, melyek a BRTKK törekvéseivel, szemléletével nem egyezhetők össze:

- sértik az intézmény érdekeit;
- rasszista oldalak;
- erotikus oldalak;
- warez oldalak (jogvédett tartalmak jogsértő terjesztése);
- terrorizmust támogató oldalak;
- chat oldalak;
- fegyverekre vonatkozó információkat tartalmazó oldalak;
- kábítószerekre vonatkozó információkat tartalmazó oldalak;
- adathalász oldalak;
- internetes fogadási oldalak, szerencsejáték oldalak;

Nem megengedett:

- az internet segítségével futtatható állományok letöltése a munkaállomásokra;
- tömörített fájlok letöltése nyílt és a jelszóval védett állományokra egyaránt, kivétel a munkavégzéshez szükséges adatállományok;
- média állományok letöltése, kivétel a szorosan a munkához köthető fájltartalmak;
- böngészés közben tilos bármilyen böngésző bővítés letöltése direkt módon és felugró ablakon keresztül egyaránt (JAVA, ActiveX, különböző médialejátszók, MS XML, Toolbar-ok, chat alkalmazások);
- automatizált letöltő alkalmazások, kliensek használata;

- minden olyan alkalmazás letöltése/telepítése/használata, amely alkalmas interneten keresztül történő erőforrás megosztására.

Az informatikai rendszert üzemeltető személyzet által kialakított megoldásokon kívül tilos más irodai munkaállomásokon külső frissítő szerverről való frissítés (operációs-rendszer, alkalmazások).

Webszolgáltatás

A Balatoni Regionális Történeti Kutatóintézet, Könyvtár és Kálmán Imre Emlékház honlaptartalmának biztosítása az intézményvezető által engedélyezett, előre egyeztett tartalmakkal történik. Ezen tartalmakat a vezető által megbízott személy (ek) végzik.

Külső szolgáltatók:

Monguz Információtechnológiai Kft.

Techno-Tel távközlési és Informatikai, Kivitelező Szolgáltató Kft.

A szolgáltatók feladataikat a megrendelővel rögzített szerződés alapján látják el.

Fogalmak

Adat: az információ megjelenési formája.

Adatbiztonság: az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

Adatbiztonság megsértése: az a cselekmény vagy mulasztás, amely ellentétben áll az adat védelmére vonatkozó biztonsági szabályokkal és amelynek következményei az adatot veszélyeztetik.

Adatvédelem: az adatok kezelésével kapcsolatos törvényi szintű szabályozás formája, amely az adatok előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik.

Bizalmasság (szervezeti állapot): az intézmény olyan állapota, amely biztosítja, hogy az adatokhoz csak azon személyek férhessenek, akiknek a szervezet jogot adott.

Biztonság: olyan szervezeti állapot, amelyben az adott szervezetnek a lehető legkisebb veszélyekkel kell számolnia. A biztonság az informatikai rendszerekben olyan előírások és szabványok betartását jelenti, amelyek a rendszer működőképességét, az információk rendelkezésre állását, sértetlenségét, bizalmasságát és hitelességét erősítik.

Biztonsági rendszer: az informatikai biztonsági rendszerek összessége.

Felhasználó: az a személy, aki egy vagy több informatikai rendszert vesz igénybe feladatai megoldásához.

Hálózat: számítógépek összekapcsolása és az összekapcsolt rendszerek legkülönbözőbb komponensei közötti adatcserét megvalósító logikai és fizikai eszközök összessége.

Illetéktelen személy: az a személy, aki az adat megismerésére nem jogosult.

Incidens: minden olyan informatikai vonatkozású esemény, ami nem része a normál működésnek és a felhasználókat akadályozza feladataik ellátásában.

Információvédelem: az informatikai rendszerek által kezelt adatok által hordozott információk bizalmasságának, hitelességének és sértetlenségének védelme.

Külső személy: az intézménnyel szerződéses kapcsolatban álló személy vagy szervezet, aki az intézmény informatikai rendszerével kapcsolatban áll.

Sértetlenség: az adat olyan tulajdonsága, mely arra vonatkozik, hogy az adat fizikailag és logikailag is teljes, ép, módosulatlan.

Teljes körű védelem: teljes körűnek nevezik az informatikai rendszer védelmét, ha az informatikai rendszer összes elemére kiterjed.

Vírus: rosszindulatú programtörzs, mely engedély nélkül készült egy felhasználói program részeként. A program használatakor átterjedhet, „megfertőzhet” más, az informatika rendszerében lévő rendszer-, illetve felhasználói programot.

Vírusvédelmi rendszer: védelmi mechanizmusok összessége, mely feladata az informatikai rendszerhez kapcsolódó vírusok felkutatása, működésük, aktív vagy passzív károkozások meggátolása, illetve megsemmisítése.

Zárt védelem: az összes releváns fenyegetés figyelembe vételével alakított védelmi rendszer.