INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Szombathelyi Egyesített Bölcsődei Intézmény

Készítette:

dr. Horváth Bernadett LL.M.

adatbiztonsági és adatvédelmi szakjogász

Tartalomjegyzék

A Szombathelyi Egyesített Bölcsődei Intézmény (székhely: 9700 Szombathely, Váci M. u. 5. adószám: 15573234-2-18) továbbiakban, mint Adatkezelő a jelen Informatikai Biztonsági Szabályzat keretei között (IBSZ) rögzíti az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) 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 (általános adatvédelmi rendelet, GDPR, továbbiakban: GDPR vagy Rendelet) és az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) rendelkezéseinek végrehajtása érdekében az adatvédelemmel kapcsolatos irányadó szabályokat, az ezzel kapcsolatos eljárási rendet, kifejezésre juttatva a rendeletben meghatározott alapelvek tiszteletét és védelmét.

Az Adatkezelő magára nézve kötelezőnek ismeri el jelen szabályzat tartalmát. Kötelezettséget vállal arra, hogy működésével kapcsolatos adatkezelése megfelel a jelen szabályzatban és a hatályos jogszabályokban meghatározott elvárásoknak.

Az Adatkezelő a személyes adatokat bizalmasan kezeli és megtesz minden olyan biztonsági, technikai és szervezési intézkedést, mely az adatok biztonságát garantálja.

Az adatkezelő az alábbiakban ismerteti informatikai biztonsági gyakorlatát.

Az Informatikai Biztonsági Szabályzat hatálya és célja

A szabályzat célja, hogy meghatározza az Adatkezelőnél az informatikai biztonság rendjét, valamint biztosítsa az adatvédelem alkotmányos elveinek, az információs önrendelkezési jognak és adatbiztonság követelményeinek érvényesülését. A Szabályzat további célja, hogy rögzítse az Adatkezelő által alkalmazott informatikai biztonsági elveket, az Adatkezelő informatikai biztonsági politikáját, amelyet magára nézve kötelezőnek ismer el.

A szabályozás célja, hogy a jelen szabályzatban foglaltak alkalmazása és működtetése útján a Szombathelyi Egyesített Bölcsődei Intézmény tevékenysége a gyakorlatban is megfeleljen az informatikai biztonságból eredő jogszabályi előírásoknak, biztosítsa az adatkezelésben meghatározott személyes adatok védelméhez fűződő alapvető jogok érvényesülését, az adatbiztonsági követelmények betartását, biztosítását.

A szabályozás célja továbbá, hogy meghatározza azon személyek körét, akik felhatalmazottak a Szombathelyi Egyesített Bölcsődei Intézmény nevében adatkezelést végezni, illetve megakadályozza az adatokhoz történő jogosulatlan hozzáférést, az adatok törvénysértő megváltoztatását, az adatok jogosulatlanul történő felhasználását, valamint engedély nélküli nyilvánosságra hozatalát.

Az Informatikai Biztonsági Szabályzat személyi hatálya kiterjed a Szombathelyi Egyesített Bölcsődei Intézményre, mint adatkezelőre, továbbá az adatkezelő munkavállalóira.

A Szabályzat tárgyi hatálya a Szombathelyi Egyesített Bölcsődei Intézmény használatában lévő vagy általa üzemeltetett valamennyi elektronikus információs rendszerre (a továbbiakban: rendszer) és azok környezetét alkotó rendszerelemre (adatok, szoftverek teljes körére, a folyamatokra, valamennyi telephelyre és létesítményre), az informatikai folyamatban szereplő valamennyi dokumentációra, azok teljes életciklusában kiterjed.

Jelen Informatikai Biztonsági Szabályzat 2024. január 1. napjától hatályos. Ezzel egyidejűleg valamennyi korábbi, informatikai biztonságra vonatkozó szabályzat, utasítás, egyéb eljárási rend hatályát veszíti.

Jelen Szabályzat visszavonásig érvényes, azonban a Szabályzat visszavonására kizárólag új Informatikai Biztonsági Szabályzat megalkotása esetén van lehetőség, ezzel biztosítandó, hogy az Adatkezelő tevékenysége során mindvégig érvényes és hatályos Informatikai Biztonsági Szabályzat szabályozza a tevékenységet.

A Szabályzat kidolgozásáért és az érintettek részére történt tájékoztatásért felelős a Szombathelyi Egyesített Bölcsődei Intézmény intézményvezetője.

Fogalom meghatározások

- adatállomány: informatikai infrastruktúrában lévő adatok logikai és fizikai összefogása, melyet egy névvel jelölnek vagy azonosítanak;
- adatátvitel: adatok szállítása összeköttetéseken, összekötő utakon keresztül (különösen számítógépek között);
- adathordozó: az elektronikus adatkezelő rendszerhez csatlakoztatható vagy abba beépített olyan eszköz, amelynek segítségével az elektronikus adatok tárolása megvalósítható;
- alkalmazás: egy célfeladatot megvalósító szoftver;
- biztonságtudatosság: a Szombathelyi Egyesített Bölcsődei Intézmény biztonságáért vállalt felelősség; a meghatározott biztonsági szintnek mint követelménynek az elfogadása, illetve a hiánya következményeinek elismerése, valamint a biztonság szempontjából etikus magatartás;
- biztonsági incidens: a rendszer működését biztonságtechnikailag hátrányosan befolyásoló, felismert és fennálló biztonsági kompromittálódás;
- dokumentum: a rendszer által használt vagy létrehozott olyan termék, amely információt tartalmazhat, és amelyet a rendszer hozott létre vagy dolgozott fel;
- folyamatgazda: a folyamat megtervezéséért, végrehajtásáért, ellenőrzéséért és javításáért felelős személy vagy csoport, aki figyelemmel kíséri a külső és belső szabályok betartását, az adott folyamatot értékeli, és szükség esetén javaslatot tesz a módosításokra, fejlesztésekre;
- hardver: informatikai eszközök kézzel közvetlenül megfogható részeinek gyűjtőneve;
- hálózat: az informatikai eszközök közötti adatátvitelt megvalósító logikai és fizikai eszközök összessége;

- hálózati aktív eszközök: a hálózat működését biztosító elektronikus elemek (különösen tűzfal, router, switch, HUB, optikai átkapcsoló);
- hálózati passzív eszközök: a hálózati aktív eszközök kapcsolatát és kommunikációját biztosító elemek (különösen kábelezés, kábelcsatornák, fali csatlakozók és a rendezőszekrények);
- helyi rendszer: helyi szerv által üzemeltetett és menedzselt rendszer;
- hozzáférési jog: annak meghatározása, hogy a kezelésre jogosult milyen szoftvert, adatot vagy adathordozót kezelhet, illetve azokkal milyen műveleteket végezhet;
- információbiztonság: olyan előírások, szabályok és szabványok betartásának eredménye, amelyek az elektronikus információs rendszerben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint az elektronikus információs rendszer és elemeinek sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és kockázatokkal arányos védelmének biztosítását érintik, és amelyeket az informatikai rendszer alkalmazása során megelőző biztonsági intézkedésekkel lehet elérni;
- informatikai biztonság: az informatikai rendszer olyan kedvező állapota, amelyben a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása biztosított, valamint a rendszer elemeinek biztonsága szempontjából zárt, teljes körű, folytonos és kockázatokkal arányos, a biztonság elvárt szintje és az ezt megvalósító intézkedések jellege függ az adott informatikai rendszer biztonsági osztályától;
- informatikai eszköz: minden olyan digitális eszköz és ennek funkcionális tartozéka, amely adatok összegyűjtésére, feldolgozására (rendezésére, csoportosítására, kiszámítására), előállítására, tárolására és megjelenítésére, illetve az e tevékenységekkel kapcsolatos adatmódosításra és adattovábbításra alkalmas;
- intézkedés: a kockázatkezelés eszközei, beleértve a szabályzatokat, eljárásokat, irányelveket, gyakorlatokat, képzést vagy egyéb intézkedést, amelyek lehetnek adminisztratív, műszaki, irányítási vagy jogi természetűek;
- integritás: a sérthetetlenségen túl a teljességet, továbbá az ellentmondás mentességet és a korrektséget jelenti, amelynek eredményeként az információ valamennyi része rendelkezésre áll, elérhető;
- javítás: a hardver vagy szoftver konfigurációjának változásával, az eszközök elszállításával járó hibaelhárítási feladat;
- karbantartás: a rendszerben vagy azok elemein végzett munka, melynek során a telepített hardver és szoftver konfiguráció nem változik, karbantartásnak minősül különösen a biztonsági réseket befoltozó hibajavítások telepítése;
- katasztrófahelyzet: az informatikai erőforrások (különösen az elektronikus adatok, fájlok, szoftverek, számítógépek, hálózati aktív és passzív eszközök) fenyegetettsége, minden olyan nemkívánatos esemény, amely az adatok teljességét, sértetlenségét, megbízhatóságát vagy rendelkezésre állását hátrányosan befolyásolja, a fenyegetettség lehet külső esemény (tűzeset, vízkár, számítógépvírusok), vagy lehet belső tényező (hanyag kezelés, rosszindulatú adatmódosítás, szoftverhiba);
- katasztrófa: bekövetkezett katasztrófahelyzet;
- kibertér: a számítógépes hálózatok és az általuk összekötött számítógépek és egyéb berendezések által alkotott virtuális tér, az a környezet, amelyben az adat technikai

eszközökön (számítógépes hálózatokon) keresztül áramlik, elektronikus adatok tárolódnak, online adatforgalom és kommunikáció zajlik;

- korrektív kontroll: az eredeti állapot visszaállítását célzó intézkedés;
- operációs rendszer: a számítógépek működésének elengedhetetlen részét képező szoftver, amelynek feladata az alapvető szolgáltatások biztosítása a programok számára, valamint az alkalmazások és a felhasználó közötti kommunikáció biztosítása;
- privilegizált felhasználó: az a felhasználó, aki a rendszer/hálózat üzemeltetési vagy fejlesztési feladatainak végrehajtásához kiemelt jogosultsággal rendelkezik;
- privilegizált funkció: a rendszer/hálózat üzemeltetéséhez vagy fejlesztéséhez szükséges beavatkozás;
- rendszerüzemeltető: az a természetes személy, jogi személy vagy egyéni vállalkozó, aki vagy amely az elektronikus információs rendszer vagy annak részeinek működtetését végzi, és a működésért felelős;
- szakmai adatgazda: annak a szervezeti egységnek a vezetője, ahová jogszabály az adat kezelését rendeli, aki az adathoz a hozzáférési jogosultságot engedélyezi, illetve ahol az adat keletkezik;
- szerver: szervernek minősül az olyan számítógép, amely hálózati szolgáltatásokat nyújt és/vagy kliensek kapcsolódnak hozzá;
- szoftver: valamely informatikai eszköz olyan logikai (kézzel nem megfogható) része, amely a hardver(ek) működtetéséhez, vezérléséhez szükséges (különösen alkalmazások, operációs rendszerek);
- területi rendszer: a területi szerv által üzemeltetett és menedzselt rendszer;
- vírus: olyan szoftvertörzs, amely egy szoftver részeként illegálisan készült, a szoftver alkalmazása során átterjedhet, „megfertőzhet" más, az informatikai rendszerben lévő rendszer-, illetve felhasználói szoftvert, sokszorozva önmagát, károkat és teljes működésképtelenséget okozhat.

Alapelvek

A felhasználó kötelessége az információvédelem területén az adott helyzetben általában elvárható magatartást tanúsítani, és tartózkodni minden károkozó tevékenységtől. Az informatikai eszköz felhasználója csak az a személy lehet, aki a Szombathelyi Egyesített Bölcsődei Intézménnyel foglalkoztatási jogviszonyban áll, a munkavégzéshez megfelelő informatikai ismeretekkel rendelkezik, valamint nyilatkozik a Szabályzatban foglaltak tudomásul vételéről. A munkaköri leírásban el kell különíteni a jogköröket és a feladatköröket az egyes személyek között annak érdekében, hogy a személyes felelősség megállapítása mindenkor biztosított legyen. Az informatikai rendszert úgy kell kialakítani, hogy biztosított legyen annak megbízható, zavartalan és folyamatos működése.

A Szombathelyi Egyesített Bölcsődei Intézmény tulajdonát képező vagy használatában álló eszközöket rendeltetésszerűen, csakis munkavégzés céljából, a tásaság érdekeinek szem előtt tartásával, a társaság által meghatározott módon, a felhasználó felelősségére lehet használni.

Az eszközök minden egyéb célú, különösen magáncélú használata a Munka Törvénykönyvének megfelelően tilos.

A felhasználó felelősséggel tartozik a munkavégzés céljából átvett eszközért, köteles megőrizni annak hardver- és szoftverintegritását. Az integritás sérelmének minősül a rendeltetésellenes használat, hardveres (különösen az informatikai eszközből történő alkatrész eltávolítása, illetve alkatrész behelyezése) vagy szoftveres módosítás (különösen nem engedélyezett program telepítése, a gyártói támogatással rendelkező verzió módosítása, biztonsági beállítások módosítása).

A felhasználó csak a saját azonosítójával jelentkezhet be a Szombathelyi Egyesített Bölcsődei Intézmény hálózatára, másnak a saját bejelentkezési hozzáférését nem adhatja át, nem teheti lehetővé, hogy más hozzáférjen. A nem a Szombathelyi Egyesített Bölcsődei Intézmény tulajdonában álló, idegen, információs, számítástechnikai és telekommunikációs eszközt az intézményvezető engedélye nélkül a társaság informatikai struktúrájához csatlakoztatni szigorúan tilos.

A felhasználó köteles a biztonságot támogató szoftverek használatára, azokat az általa használt eszközről nem törölheti le, nem kapcsolhatja ki, valamint kizárólag olyan szoftvereket, programokat használhat, amelyek a munkavégzés céljából szükségesek, engedélyezettek.

A felhasználó kötelessége az általa felismert biztonsági incidenst vagy az általa feltárt biztonsági sebezhetőséget haladéktalanul jelezni a rendszerüzemeltetőnek és az intézményvezetőnek, hogy annak elhárítása a lehető leghamarabb megtörténjen.

Fizikai és környezeti biztonság

A Szombathelyi Egyesített Bölcsődei Intézmény a rendszer védelmét a megfelelő fizikai biztonság kialakításával biztosítja. Az olyan helyiségeket, ahol informatikai eszközökkel történik a munkavégzés, távollét esetén a jogosulatlan hozzáférést megakadályozó módon zárva kell tartani. Amennyiben a személyes felügyelet nem biztosított, az informatikai erőforrásokat koncentráltan tartalmazó helyiségek bejáratát zárva kell tartani. Munkaidőn túl a belépés csak előzetes bejelentkezés és az intézményvezető engedélyezése után, szabályozott módon lehetséges.

A Szombathelyi Egyesített Bölcsődei Intézmény a szervereket külön helységben helyezte el, ami klímával felszerelt, és a helyiség közelében el van helyezve egy szén-dioxiddal oltó berendezés is. A helység kulcsra zárható, csak az informatikusoknak, intézményvezetőnek, valamint egy megbízott munkavállalónak van jogosultsága belépni, aki a biztonsági mentést végzi.

A tűzvédelmi előírásokat a Szombathelyi Egyesített Bölcsődei Intézmény annak megfelelően alakítja ki, hogy az épületben milyen elektronikai rendszer üzemel. Az elektromos és szünetmentes hálózatot, a túlfeszültség-, az érintés- és villámvédelmet, valamint a vészkikapcsoló, továbbá a szükségvilágítást biztosító berendezéseket annak megfelelően alakította ki, hogy az épületben milyen biztonsági osztályba sorolt rendszer üzemel. Az energiaellátás biztonsága érdekében a szünetmentes tápegységet is telepített.

A szerver szünetmentesen tápegysége áramkimaradás esetén 15-20 percet biztosít a leállításra vagy az áram visszatérésére, míg a rack szekrényben egy 30 perces szünetmentes tápegység van felszerelve, amely az internethozzáférésért felelős hardverek működőképességét biztosítja.

A hőmérséklet és páratartalom szintjét az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben szabályozni kell. Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben csak az elengedhetetlenül szükséges közműhálózat csatlakozhat, a helyiségen belül nem mehet át víz-, gáz-, csatorna és egyéb közművezeték, felette és a határoló falfelületek mentén vizesblokkot tartalmazó helyiségrész nem lehet, az esetleges vízbetörés érzékelését biztosítani kell. Fenti feltételek az Adatkezelőnél megvalósulnak.

Az informatikai erőforrásokat koncentráltan tartalmazó helyiségekben a padlóburkolatoknak, az álpadlónak, a berendezési tárgyaknak antisztatikus kivitelűeknek kell lenniük. Tilos az informatikai erőforrásokat koncentráltan tartalmazó helyiség funkciójától eltérő anyagot vagy eszközt tárolni. Az adatkommunikációs kábelek fizikai védelme érdekében biztosítani kell, hogy az alkalmazott technológiák védjék a kábeleket mechanikai sérülés, elektromágneses zavarok, illegális rácsatlakozás, szándékos rongálás, szabotázs és lopás ellen.

Vagyonelemek, adathordozók védelme

A Szombathelyi Egyesített Bölcsődei Intézmény felhasználói eszközei csak a zárt helyiségben hagyhatók felügyelet nélkül. A társaság a számítógépeit jelszavas védelemmel látja el. A társaság munkavállalói különböző szintű jogosultságokkal rendelkeznek, a hálózaton felhasználói név és jelszó segítségével azonosítják magukat. Minden feladathoz két fő felhasználó hozzáférése engedélyezett az esetleges szabadságok miatt.

Az irodákban a hosszabb munkaszünet idejére el kell zárni a védendő információkat tartalmazó dokumentumokat és adattároló eszközöket. Az eszközök képernyőjén a védendő dokumentumokat úgy szabad kezelni, hogy azok tartalmát illetéktelen személyek ne ismerhessék meg.

A beépített adathordozóval ellátott rendszer önmagában is adathordozónak minősül. Az adatot tartalmazó adathordozókat védeni kell a jogosulatlan hozzáféréstől, visszaéléstől vagy megrongálódástól.

Selejtezés alkalmával minden adathordozó tartalmát dokumentáltan törölni kell, ezután olyan fizikai roncsolással kell megsemmisíteni, hogy újbóli használatba vétele lehetetlenné váljon.

A megsemmisítésről jegyzőkönyvet kell felvenni. A mobil eszközöket biztonságos módon kell kezelni, annak érdekében, hogy ne kerülhessenek illetéktelen felhasználásra, ezért amennyiben a technológia rendelkezésre áll, a rajta tárolt információkat központi management eszközzel titkosítva kell tárolni. Külső adathordozóra másolás előtt a felhasználónak vírusellenőrzést kell végrehajtania a másolandó adatállományon, a forrás munkaállomáson rendszeresített vírusellenőrző programmal.

A hozzáférés felügyelete

Az információhoz és az információfeldolgozó eszközökhöz való hozzáférést korlátozni kell az arra jogosultak körére. A felhasználók részére a rendszerhez történő hozzáférést a rendszer biztonsági beállításainak érvényesítése és azok ellenőrzését követően lehet biztosítani, amelyet a rendszerüzemeltető hajt végre.

A rendszernek alkalmasnak kell lenni a hozzáférési jogok egyedi vagy csoportszinten való megkülönböztetésére és szabályozására, valamint a felhasználók személyhez köthető egyedi azonosítására. A felhasználót a vírusírtó egyedi azonosítóval látja el, melynek alapján nyomon követheti a rendszerben végzett tevékenységét. A rendszerhez való hozzáférést a felhasználó megbízható azonosítása előzi meg, amely a személyes használatra kiadott egyedi felhasználói névvel és ehhez tartozó, kizárólag a felhasználó által ismert jelszóval történik. A felhasználó az első bejelentkezése után köteles azonnal megváltoztatni a jelszavát. Minden felhasználónak lehetőséget kell biztosítani arra, hogy jelszavát bármikor megváltoztathassa. Amennyiben a jelszó kompromittálódásának gyanúja megalapozott, azt a felhasználó haladéktalanul köteles megváltoztatni. Egyéb esetben a jelszavakat 90 naponként kell változtatni.

Az intézményvezető az információbiztonság fenntartása érdekében az azonosítókat letilthatják, ha

a) a jelszó kompromittálódásának gyanúja megalapozott;
b) a felhasználó megsérti a rá vonatkozó adatkezelési szabályokat;
c) a felhasználó foglalkoztatási jogviszonya megszűnt, szünetel vagy munkaköre megváltozott;

A jogosultságokat a munkavégzéshez minimálisan szükséges mértékű jogosultságokra kell korlátozni, a szükséges és elégséges ismeret elvének megfelelően.

Az erőforrásokhoz való hozzáférési jogosultságok kiadásánál törekedni kell a csoportszintű jogosultságok alkalmazására. A felhasználók számára tiltani kell a következő tevékenységeket:

a) BIOS hozzáférés;
b) hardver telepítés;
c) szoftver telepítés;
d) hozzáférés a rendszerfájlokhoz (módosítás);
e) rendszeridő és dátum módosítás;

f) naplófájlok módosítása, törlése;
g) operációs rendszer rendszerbeállításainak megváltoztatása;
h) felhasználó jogainak megváltoztatása.

A rendszernek meg kell akadályoznia, hogy a nem privilegizált felhasználók privilegizált funkciókat hajtsanak végre, ideértve a biztonsági ellenintézkedések kikapcsolását, megkerülését vagy megváltoztatását. A távoli hozzáférést, a vezeték nélküli hozzáférést és a privilegizált parancsok és biztonságkritikus információk eléréséhez távoli hozzáférési jogosultság megadását az intézményvezető, mint adatgazda engedélyezhetik. A felhasználó számára csak olyan hálózatokhoz és hálózati szolgáltatásokhoz való hozzáférés biztosítható, amelyek használata engedélyezett a számára. A felhasználó hibájából bekövetkezett kompromittálódás vagy annak gyanúja esetén az intézményvezetőnek vizsgálni kell a felhasználói jogosultság azonnali felfüggesztésének indokoltságát. A hozzáférési jogosultságokat az intézményvezető személyügyi, munkaköri változások bekövetkezésekor minden esetben haladéktalanul felülvizsgálják, és indokolt esetben intézkednek a hozzáférési jogosultságok módosításáról, visszavonásáról. A 90 napja nem használt felhasználói fiókot és a hozzá tartozó postafiókot fel kell függeszteni. A 90 napot meghaladó távollét, betegség esetén a felhasználó jogosultságait fel kell függeszteni, a helyettesítést a hozzáférési jogosultságok ideiglenes megváltoztatásával kell biztosítani.

A Szombathelyi Egyesített Bölcsődei Intézmény munkavállalói közül összesen 1-2 főnek van jogosultsága az informatikusokon kívül távoli asztal hozzáféréssel akár otthonról is dolgozni. A belépőket a router azonosítja.

Az üzemeltetés biztonsága

Az üzemeltetési eljárásokat csak annak a felhasználónak lehet hozzáférhetővé tenni, akinek ez a munkaköri feladatainak ellátásához feltétlenül szükséges. Dokumentált és engedélyezett módon kell kezelni minden olyan szervezeti, folyamatbeli, az információfeldolgozó rendszerelemet és rendszerkonfigurációt, valamint a hálózatot érintő változtatást, amelyeknek hatása van az információbiztonságra.

A rendszerhez alapkonfigurációt kell összeállítani, azt dokumentálni kell, és karban kell tartani. Változatlan állapotban meg kell őrizni a rendszer alapkonfigurációját és annak előző verzióját, hogy szükség esetén lehetővé váljon az erre való visszatérés. A szükséges rendszerteljesítmény biztosítása érdekében az erőforrások használatát nyomon kell követni, optimalizálni kell és a jövőbeni kapacitásszükségletet előre kell jelezni. A felhasználónak a bekövetkezett hardverelem-meghibásodást haladéktalanul jelentenie kell a rendszerüzemeltető szervezetnek.

A Szombathelyi Egyesített Bölcsődei Intézmény informatikai eszközeit a gyártó vagy a forgalmazó előírásai szerint kell karbantartani, folyamatos rendelkezésre állásuk és sértetlenségük biztosítása érdekében. A munkaállomások és szerverek karbantartási feladatai

között ellenőrizni kell a telepített szoftverek listáját és verzióját, valamint a kritikus és biztonsági frissítések állapotát.

A rendszer karbantartását az Savaria Computer Kft. végzi, ő hozzá is fér az adatokhoz, így adatfeldolgozónak minősül.

A Szombathelyi Egyesített Bölcsődei Intézmény operációs rendszerei és a felhasználói programjai kereskedelmi forrásból beszerzett, jogtiszta programok. Az operációs rendszer és alkalmazás verzióját, valamint biztonsági patch szintjét tesztelést követően lehetőség szerint a gyártói támogatással rendelkező, legmagasabb szintre kell hozni.

A Szombathelyi Egyesített Bölcsődei Intézmény többféle operációs rendszert használ: a kliens gépeken Windows 10, de bizonyos gépek már átálltak 11-re. Szerverek operációs rendszere Linux és Windows.

A rendszert úgy kell beállítani, hogy a működése során keletkező nem nyilvános maradvány információk (különösen az átmeneti fájlok) bizalmasságát, sértetlenségét védje. Az informatikai üzemeltetésért felelős vezetőnek a rendszer minden arra alkalmas – megfelelő hardver- és szoftverkörnyezettel rendelkező – elemére jóváhagyott vírusellenőrző szoftvert kell telepítenie és naprakészen tartania.

Valós idejű víruskereső működik, a kliensek gépeken a Windows beépített defender, a Linuxon pedig a Linux Safe program.

Az adathordozón látható módon fel kell tüntetni, hogy vírust, kártékony kódot tartalmaz. A kéretlen és kártékony kódot tartalmazó elektronikus levelek kiszűrésére olyan központilag menedzselt szűrőt kell üzemeltetni, amely automatikusan központilag frissíti az adatbázisát, és frissíti a rendszert új verziók elérhetővé válásakor.

A biztonsági mentés célja az információ és az adatfeldolgozó szoftverek épségének és rendelkezésre állásának biztosítása. A hatékony biztonsági adatmentés érdekében a munkaállomásokon feldolgozott adatállományokat tárolni kizárólag szervereken és központi kiszolgálókon, valamint az adatmentésre szolgáló médián lehet. Bármilyen más helyen történő adattárolás még átmenetileg is tilos. Az adatvesztés elkerülése érdekében a Szombathelyi Egyesített Bölcsődei Intézmény adatszinten állandóan végez biztonsági mentést, fájlszinten pedig minden éjjel. A szerverek gyakorlatilag tükrözik a merevlemezt. Ezen kívül történik hálózaton keresztül még biztonsági mentés egy külön gépre a Polgármesteri hivatalba.

A biztonsági mentések gyakorisága és tartalma alkalmas arra, hogy megelőzze a személyes adatokkal kapcsolatos adatvesztést.

A Szombathelyi Egyesített Bölcsődei Intézmény minden olyan adatot ment, amely az auditálás, ellenőrzés eszköze lehet (különösen naplófájlok, riportok). Ezeket az adatokat a többi felhasználói, illetve rendszer adattól elkülönítetten menti, és minimum öt évig megőrzi.

A naplóbejegyzések vizsgálatát, elemzését és jelentését integrált folyamattá kell alakítani, amely a veszélyes vagy tiltott tevékenységekre és történésekre megfelelően képes reagálni. A

rendszernek naplóznia kell a felhasználói tevékenységet, valamint a privilegizált felhasználó privilegizált jogosultsággal végzett tevékenységeit. A naplózó eszközt, illetve a naplóinformációt meg kell védeni a jogosulatlan hozzáféréstől, törléstől, kiiktatástól vagy módosítástól.

A hálózat biztonsága

A hálózatüzemeltetőnek a rendszer hálózati elemeit menedzselni és felügyelni kell. A hálózatmenedzsment segítségével kell megoldani a hálózatok biztonságát és az infrastruktúra védelmét. Olyan ellenőrző-felügyeleti eszközöket kell használni, amelyek biztosítják a hálózatokban kezelt és továbbított adatok biztonságát, és megóvják a hálózatot a jogosulatlan hozzáférésektől.

A Szombathelyi Egyesített Bölcsődei Intézmény hálózatából más hálózatba csak előre definiált és a hálózatüzemeltető által engedélyezett módon szabad csatlakozni. A Szombathelyi Egyesített Bölcsődei Intézmény gondoskodik a hálózati eszközökön a naplózás beállításáról és a hálózati eszközök rendszer idejének szinkronizálásáról.

Tilos a hálózat biztonságos működését zavaró vagy veszélyeztető információk, programok terjesztése. A hálózat nem használható az alábbi tevékenységekre:

a) a jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, így mások személyiségi jogainak megsértése (különösen rágalmazás), tiltott haszonszerzésre irányuló tevékenység (különösen piramisjáték), szerzői jogok megsértése (különösen szoftver nem jogszerű terjesztése);
b) profitszerzést célzó (különösen kriptovaluta bányászat), direkt üzleti célú tevékenység és reklám;
c) a hálózat, a kapcsolódó hálózatok, illetve ezek erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, veszélyeztető tevékenység, ilyen információknak és programoknak a terjesztése;
d) a hálózatot, a kapcsolódó hálózatokat, illetve erőforrásaikat indokolatlanul, túlzott mértékben, pazarló módon igénybe vevő tevékenység (különösen nem hivatali körlevelek, hálózati játékok, kéretlen reklámok);
e) a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, eszközök és szolgáltatások – akár tesztelés céljából történő – túlzott mértékben való szisztematikus próbálgatása (különösen TCP port scan);
f) a hálózat erőforrásainak a hálózaton elérhető adatoknak illetéktelen kezelése, módosítása, elérhetetlenné tétele, törlése vagy bármely károkozásra irányuló tevékenység;

g) másokra nézve sértő, vallási, etnikai, politikai vagy más jellegű érzékenységét bántó, zaklató tevékenység (különösen pornográf anyagok közzététele);
h) hálózati üzenetek, hálózati eszközök hamisítása, olyan látszat keltése, mintha egy üzenet más gépről vagy más felhasználótól származna (spoofing).

A hálózat külső határán aktív hálózati forgalom vizsgálatára és hálózati támadás felismerésére alkalmas tűzfalat kell üzemeltetni. A Szombathelyi Egyesített Bölcsődei Intézménynél a számítástechnikai hálózaton a kliens számítógépeket a Windows 10 operációs rendszer tűzfala védi, a szervereket pedig a Linux és a Windows tűzfal. Ezen kívül a routerbe is be van építve egy egyszerűsített tűzfal. A tűzfal alkalmas arra, hogy az esetleges külső támadásoktól, behatolásoktól megvédjék a számítástechnikai rendszert.

Minden külső infokommunikációs szolgáltatás használatakor felügyelt interfészt kell működtetni, amelyekhez forgalomáramlási szabályokat kell meghatározni és működtetni. A szabályok meghatározásánál az alapeseti visszautasításból kell kiindulni. A forgalomáramlási szabályok alóli minden kivételt dokumentálni kell, a kivételt alátámasztó alapfeladattal és az igényelt kivétel időtartamával együtt. Félévente dokumentáltan felül kell vizsgálni a forgalomáramlási szabályok alóli kivételeket, és el kell távolítani azokat a kivételeket, amelyeket közvetlen alapfeladat már nem indokol.

A rendszert és a hálózatot túlterheléses – szolgáltatás megtagadás jellegű – támadásokkal szembeni védelemmel kell ellátni.

Az elektronikus levelező rendszer elemeiről, különösen a szerverek fizikai, logikai védelméről folyamatosan gondoskodni kell. Az elektronikus levelező rendszeren keresztül történő támadások esetén, amennyiben a rendszer védelme átmenetileg nem biztosított – különösen olyan vírustámadás esetén, amikor a vírusvédelmi rendszerek még nem nyújtanak kellő védelmet – az elektronikus levélforgalmat az informatikai üzemeltetésért felelős vezetőnek ideiglenesen le kell állítani.

Biztonsági események kezelése

Biztonsági eseménynek kell tekinteni minden olyan nem kívánt, illetve nem várt egyedi vagy sorozatos információbiztonsági kockázatot, amely veszélyeztetheti a Szombathelyi Egyesített Bölcsődei Intézmény tevékenységét, és fenyegetheti az információbiztonságot, továbbá minden olyan tevékenységet vagy mulasztást, amely az utasítás be nem tartásával biztonsági eseményt eredményezhet. A biztonsági eseménykezelési folyamatra olyan rendszert kell alkalmazni, amely támogatja az alábbi tevékenységeket:

a) a biztonsági esemény jelentése;
b) a biztonsági eseménnyel kapcsolatos információk gyűjtése;
c) tudásbázis kiépítése;
d) azonnali válaszlépés meghatározása;
e) azonnali válaszlépés végrehajtása;
f) átfogó válaszlépés szükségességének a meghatározása;

g) javaslat kidolgozása az átfogó válaszlépésre;
h) átfogó válaszlépés engedélyezése;
i) átfogó válaszlépés végrehajtása;
j) a végrehajtás leellenőrzése;
k) a biztonsági esemény dokumentálása;
l) biztonsági esemény kezelési képességek dokumentált tesztelése;
m) statisztikai kimutatások készítése.

Biztonsági esemény felfedezése vagy gyanúja esetén a felhasználónak az eszközt haladéktalanul le kell választani a hálózatról, és értesíteni kell az intézményvezetőt. Ha a biztonsági esemény fokozott kockázatra utal, akkor az intézményvezető intézkedik annak kivizsgálására.

Záró rendelkezések

Jelen Informatikai Biztonsági Szabályzat 2024. január 1. napján kihirdetésre és kifüggesztésre került a Szombathelyi Egyesített Bölcsődei Intézmény szombathelyi irodaépületében.

Szombathely, 2024. január 1.

SZOMBATHELYI EGYESÍTETT BÖLCSŐDEI INTÉZMÉNY
Eum József u. 33
9700 Szombathely

.....
intézményvezető
Szombathelyi Egyesített Bölcsődei Intézmény