ZHK - 3468/2018

Zempléni Z.H.K.
Hulladékkezelési Közszolgáltató Nonprofit Kft.

3527 Miskolc, Besenyői út 26.

Telefonszám: +36 (46) 504-394

E-mail: info@zhkt.hu
web: www.zhk.hu

Zempléni Z.H.K.

Informatikai Adatvédelmi Szabályzat

Hatályos: 2018. szeptember 17.

Informatikai védelem

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében a BMH-IT, A ZHK Kft.-vel létrejött jogviszony alapján az alábbi intézkedéseket és garanciális elemeket alkalmazza:

- az adatkezelés során használt számítógépek és mobiltelefonok a Társaság tulajdonát, vagy bérleti jogviszony értelmében jogszerűen a birtokát képezik;
- a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval – lehet csak hozzáférni, a jelszavak cseréjéről BMH IT csoport rendszeresen, illetve indokolt esetben gondoskodik;
- a BMH IT által szolgáltatott közös meghajtón tárolt fájlok óránként mentésre kerülnek, valamint 256 verzióig vagy 3 évig állítható vissza. Ez a hálózati berendezés a BMH-IT miskolci szerverén üzemeltetett Synology háttértároló. Ezen a ZHK számára elkülönített merevlemez kötet klaszteren történik az adattárolás. Ez egy titkosítással ellátót olyan tárhely, ahová a felhasználó csak a saját maga által megadott jelszóval tud belépni;
- a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá. A közös mappa struktúrában megtalálható minden felhasználó részére létrehozott saját dedikált privát mappa, ami titkosított és jelszóval védett;
- amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;
- a hálózaton tárolt adatok biztonsága érdekében a szerverek esetén magas rendelkezésre állású infrastruktúrán történik mentésekkel és archiválással kerüli el a Társaság az adatvesztést;
- a személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez, a mentés a központi szerver teljes adatállományára vonatkozik és merevlemezre, valamint privát felhőbe történik;
- a személyes adatokat kezelő hálózaton a vírusvédelemről a Windows Defender vagy az ESET Security folyamatosan gondoskodik;
- A telephelyeket összekötő VPN kapcsolat AES128-as titkosítással SHA1-es autentikációval és DH2-es key grouppal vannak védve. Ezek a kapcsolatok csak belső hálózatból elérhetőek.
- Otthonról dolgozóknak Zyxell kliens oldali vpn szoftvert (ZyWALL IPSec VPN Client 3.7.204.61.13) biztosítunk, melyek AES128-as titkosítással SHA1-es autentikációval és DH2-es key grouppal vannak védve.
- Minden informatikai eszköz jelszóval védett
- A Synology RS-816 NAS (továbbiakban: NAS) közös meghajtón lévő adatok és mappák AES 256 bites titkosítási kulccsal védettek
- A Synology NAS közös meghajtón lévő személyes mappákon belül található egy privát mappa, melyhez csak az adott felhasználó fér hozzá egyedi jelszóval. A hozzáféréshez a jelszó a mappa beiktatásakor kerül kiválasztásra a felhasználó által.
- Az adatvesztés végett a NAS meghajtón és a szervereken található adatok és adatbázis mentések GDPR kompatibilis Microsoft felhőbe szinkronizálódnak AES 256 bites titkosított csatornán, amelyhez csak az informatikai csoport tagjai férnek hozzá
- A hálózati eszközeink az informatika által meghatározott jelszóházirend által védetettek. A jelszavak 3 havonta cserélődnek

Szerverek biztonsága

A BMH-IT minden a céget érintő vagy a cég belső üzemeltetése által keletkezett információt szenzitív és személyes adatként kezel. A BMH IT által kezelt személyes adatok áramlását elektronikus módon szerverek segítségével valósítják meg, fizikai tárolásukat pedig adattárolók segítségével. Mind az adattárolókat, mind pedig a szervereket külön erre a célra kialakított helyiségben kell elhelyezni. A szerverszobába való belépési jogosultságot a munkavállalónak külön kell igényelnie, amit az Informatikai vezetőnek (amelyet az adatvédelemért felelős személlyel egyetértésben) kell elbírálnia.

A személyes adatok tárolásának helyén, a szerverszobákban tárolt szerverek fizikai védelme érdekében a Társaság az alábbi intézkedéseket és garanciális elemeket alkalmazza:

- a szerverszoba a BMH miskolci székhelyén található, azonban az adattárolás más titkos helyen is tükrözve (duplikálva) van. A szerverszoba klimatizált és tűzjelző berendezéssel ellátott,
- a szerverszobába csak BMH IT csoport tagjai rendelkeznek belépési engedéllyel, amit egy proxy beléptető rendszer naplóz,
- a proxy kártyával rendelkező személyekről a BMH IT csoportja nyilvántartást köteles vezetni
- amennyiben a szerverszobába olyan személynek indokolt a belépése, aki arra nem jogosult, úgy minden esetben kötelező egy belépesi engedéllyel rendelkező személy egyidejű jelenléte.

Jogosultságkezelés

A jogosultságkezelés szabályozásának célja, hogy a kiosztott jogosultságok pontosan nyomon követhetőek legyenek, dokumentált formában megőrzésre kerüljenek, valamint az egyes jogosultságokkal rendelkező személyek tevékenysége és az általuk felhasznált adatok köre ellenőrizhető legyen. A hozzáférési jogosultságokat a vállalat vezetése határozza meg. Ezen adatok naprakészsége nagymértékben hozzásegíti a BMH IT csoport tagjait az elvárt, illetve az elérhető biztonsági szint teljesítéséhez, továbbá az informatikai hálózat törvényi és szakmai normák szerinti üzemeltetéséhez.
A szabályozás kiterjed az elektronikus megfigyelőrendszerek informatikai rendszerére és az azokhoz csatlakozó eszközökre.

Az informatikai rendszerben a jogosultságok változásait (létező jogosultságok, új jogosultságok kiosztása, módosítása, megszűnése) dokumentálni kell.

A személyes adatok biztonsága érdekében a Társaság az alábbi jogosultságkezelési előírásokat alkalmazza:
Alapelvek

- Új jogosultság beállítását, illetve jogosultság megváltoztatását a jogosultság birtokosának felhatalmazása alapján az IT-vezető végzi.
- A jogosultságok megállapítása során kizárólag a munkavégzéshez szükséges és elégséges jogosultságokat kell kiosztani.
- El kell kerülni, hogy teljes hozzáférést, illetve adminisztrátori jogosultságokat kapjanak más munkát végző, illetve a jogosultság birtoklására nem igényt tartó személyek.
- Adminisztrátori jogosultsággal rendelkező nevesített felhasználót kell alkalmazni a rendszer adminisztrálása érdekében minden esetben, ahol ez lehetséges. A nem nevesített rendszergazdai jelszavakat zárt borítékban, felbontást gátló módon, aláírva kell tárolni. Ezek használatát az adatkezelő vezető tisztségviselője vagy akadályoztatása esetén helyettesítési rend szerinti helyettese engedélyezheti. A nem nevesített felhasználói jogosultságok használatát indokolni és dokumentálni kell.

- Külső – karbantartó vagy fejlesztő – cég alkalmazottja folyamatosan működő, korlátlan időre szóló hozzáférési jogosultsággal nem rendelkezhet.

Jogosultságkezelési folyamat

Jogosultságigényléshez, -módosításhoz az IT-vezetőnek címzett elektronikus kérelem szükséges.

- Az IT-vezető minden esetben konzultál az megrendelőlapon szereplő jogosultság megadásáról vagy módosításáról annak indokoltságának tekintetében a jogosultság birtokosával és az igénylő feletti munkáltatói jog gyakorlójával. A jogosultság megadásával vagy módosításával kapcsolatosan a vezető tisztségviselőnek és az igénylő feletti munkáltatói jog gyakorlójának vétójoga van.
- A megszületett döntést követően az IT vezető által kijelölt munkatárs beállítja a jogosultságokat, amelyről visszaigazolást küld az igénylő felé.
- A jogosultság birtokosának munka vagy egy jogviszonya megszűnésével közvetlen felettesének kötelessége értesíteni az IT vezetőt, valamint a munkáltatói jogok gyakorlóját a jogosult eddig birtokolt jogosultságainak törlése érdekében.
- A jogosultság megszűnése esetén a jogosult felettese a megszűntetési kérelmet elektronikus módon vagy papír alapon a jogosultságkezelési megrendelőlapon küldi meg az IT vezetőnek, aki gondoskodik a jogosultság törléséről. Ezt követően az IT vezető vagy az általa megbízott munkatárs visszajelzést küld a törlést kezdeményezőnek.
- Áthelyezés esetén a korábbi munkakör feletti munkáltatói jogokat gyakorló felettes és az új munkakör feletti munkáltatói jogokat gyakorló felettes egyetemlegesen kötelesek gondoskodni a régi jogosultságok törlésének, módosításának vagy új jogosultságok felvételének kezdeményezéséről.
- Az informatikai rendszerben a kilépő felhasználók profiljait fel kell függeszteni, használaton kívül kell helyezni. A felhasználói fiókok törlése a rendszerek ellenőrzését követően történhet meg, ha a törlés nem okoz adatvesztést.

IT folyamatok rögzítése és dokumentálása

A BMH IT csoportja elektronikus naplóban rögzíti a biztonsági procedúrákban és az infrastruktúrában történő változásokat, továbbá folyamatosan rögzíti az alvállalkozók munkaállomásain elvégzett munkafolyamatokat.

Ez az elektronikus napló AES 256 bites titkosítási metódussal rendelkező tárhelyről érhető el. A BMH IT csoport a Teamvieweren elvégzett távsegítség folyamatát is rögzíti, ami videó formátumban igényelhető. Ezeket a felvételeket szintén titkosított helyen tároljuk 30 napig.

Mobil eszköz menedzsment

Az adatvédelmi szabályozás szempontjából a mobil eszköz menedzsment területén a Társaság üzletmenetéhez fontos szolgáltatások, műszaki technikai, informatikai biztosítása mellett adatvédelmi szempontból fontos kötelezettség keletkezik, azaz biztosítani kell a Társaság birtokába kerülő adatok titkosságát, sérthetetlenség és a biztonságot garantáló keretrendszerben való működését.

A Társaság rendszerében mobilmenedzsment szolgáltatásokat biztosító informatikai beruházást kell elvégezni, amely az alábbiakat kell, hogy biztosítsa:

- összetett és rendszeresen változó jelszóhasználat kikényszerítése
- használati eszközök automatikus kiléptetése
- titkosítás használata a rendszerben levő eszközökön
- adatok távoli törlésének lehetősége (csak a céges adatokra, vagy az összes adatra vonatkozóan)
- eszköz távoli letiltása
- eszköz távoli ellenőrzése
- nyomkövetés és helymeghatározási opció távoli bekapcsolásának lehetősége

Kelt: Miskolc, 2018. szeptember 17.

ZHK
zempléni hulladékkezelési közszolgáltató nonprofit kft

mint adatkezelő
képviseletében: **Hercsik István**
ügyvezető