Melléklet a Vig. ut.: 34/2018 (XII.21.) Vezérigazgatói utasításhoz

Szám: SZAB 11-02

INFORMÁCIÓ BIZTONSÁGI SZABÁLYZAT

Jóváhagyás dátuma: 2018. 12. 21

Jóváhagyó:

Rajnai Attila
vezérigazgató

Tartalomjegyzék

1 Az Információ Biztonsági Szabályzat célja, alapelvei

Jelen Információ Biztonsági Szabályzat (a továbbiakban: IBSz) célja a BM HEROS Zrt. (a továbbiakban: BM HEROS) tulajdonában lévő, bérelt és általa üzemeltetett [1]informatikai rendszerekben lévő adatok bizalmasságát, hitelességét és rendelkezésre állását biztosító védelmi tevékenységek vállalati szinten történő szabályozása.

Az IBSz általános iránymutatással, fogalmi keretrendszerrel és irányelvekkel szolgál az utasítás-szintű munkautasítások elkészítéséhez.

Az IBSz kiadásának általános célja a BM HEROS informatikai rendszereiben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása és az ezt elősegítő védelmi intézkedések megteremtése és szabályozása.

Jelen Információ Biztonsági Szabályzatnak a célja továbbá, hogy átlátható és nyomon követhető formában rögzítse azon célokat és irányelveket, melyek segítségével az információ biztonság magasabb fokú kialakításának további teendői, illetve további szabályzatai, leírásai egy komplex, átfogó és széleskörű információbiztonságot alkossanak.

Az IBSz alapelve azon szándék kifejezése, hogy olyan normák kerüljenek bevezetésre a Társaságnál, melyek mentén a szabályozás rendelkezései, módszertana a lehető legteljesebb mértékben hozzájárulnak ahhoz, hogy a tulajdonosi jogkörgyakorló IT biztonsági és adatvédelmi szabályozási rendjével az összhangot megteremtsék.

Az IBSz alapelve továbbá, hogy biztosítsa annak a lehetőségét a Társaságnál, hogy az állami elektronikus információs rendszerek biztonságáról szóló 2013. évi L. tv. valamint 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 szóló BM rendelet rendelkezései, módszertana a lehető legteljesebb mértékben érvényesüljenek. A Társaság attól függetlenül, hogy nem tartozik a hivatkozott jogszabályi rendelkezések hatálya alá, törekszik arra, hogy a Társaság az említett jogszabályi rendelkezéseket alkalmazza az IT biztonsági és adatvédelmi előírásokat érintően. (Az IT feladatterv - OVI űrlapok - az IBSz mellékletét képezi).
A Társaság IT biztonsági szempontból a fentiek értelmében 2-es osztályba tartozik - ez alól kivétel a HR rendszer, amellyel kapcsolatban kiemelt biztonsági intézkedések kerülnek kialakításra a 3-as osztályú besorolásnak megfelelően.

[1] Külső szolgáltatók igénybevételével, szerződéses alapon

2 Az Információ Biztonsági Szabályzat hatálya

2.1 A szabályzat tárgyi hatálya

Az IBSz által megfogalmazott irányelveket érvényre kell juttatni a BM HEROS tulajdonában lévő vagy az általa üzemeltetett informatikai rendszerek tekintetében azok teljes életciklusa alatt (a fejlesztési igények megfogalmazásától a rendszerből történő kivonásig).

Az IBSz tárgyi hatálya a BM HEROS által, vagy hozzájárulásával közreműködővel beszerzett, vagy általa üzemeltetésre átvett informatikai infrastruktúra elemekre és az azokon tárolt, illetve szolgáltatott adatokra terjed ki. Ez magában foglalja a számítógépeket (hordozható számítógépeket, mobileszközöket), perifériákat, a számítógépes hálózatot, a hálózati erőforrásokat, szolgáltatásokat, valamint a rendszerszoftvereket és alkalmazásokat.

A tárgyi hatály kiterjed továbbá a BM HEROS területén használt, a szervezet által üzemeltetett, más szervezetek tulajdonát képező informatikai berendezésekre és minden olyan informatikai berendezésre amely engedélyt kapott annak informatikai rendszeréhez való csatlakozásra, valamint az adathordozó egységre (CD-k, DVD-k, PEN drive-ok, memória kártyák, stb.).

Továbbá az IBSz tárgyi hatálya kiterjed a BM HEROS területi szervezeteire, a BM HEROS LEK-re annak szervezeteire, azok területén használt, üzemeltetett és a BM HEROS bármilyen üzleti folyamatával, vagy informatikai rendszerével kapcsolatba kerülő eszközre és azokon tárolt adatokra.

2.2 A szabályzat személyi hatálya

Az IBSz személyi hatálya kiterjed a BM HEROS és a BM HEROS LEK valamennyi alkalmazottjára és (számítástechnikai értelemben vett) olyan egyéb külső személyekre, beleértve a megbízási szerződéssel, vagy egyéb szerződéssel határozott időre/feladatokra foglalkoztatott külső alkalmazottakat is, akik a BM HEROS informatikai rendszereivel, szolgáltatásaival valamilyen módon kapcsolatba kerülnek, vagy olyan adatok kezelését végzik, amelyek a BM HEROS, vagy BM HEROS LEK tulajdonát képezik.

3 A szabályzathoz kapcsolódó munkautasítások jegyzéke

Dokumentum neve	Típusa
Felhasználói tevékenységek szabályozása	Munkautasítás
Jogosultság kezelési munkautasítás	Munkautasítás
Informatikai eszközök javítása	Munkautasítás
HelpDesk tevékenység	Szolgáltatói szerződés
Mentési rendszer leírása	Munkautasítás
Információ biztonsági fogalomtár	Melléklet
Szolgáltatáskatalógus	Melléklet

4 Információ biztonság működtetése

4.1 Az információ biztonság szervezeti struktúrája

A BM HEROS az információ biztonsággal kapcsolatos problémakör menedzselésére egy Információ Biztonsági Bizottságot (IBB) hoz létre, amely összefogja a fizikai, logikai, személyi és informatikai biztonsággal kapcsolatos területeket. Ez egy speciális fórum, mely a szervezet adatvédelmi és biztonsági érdekeit képviseli.

A Bizottság, kötelezően évente, vagy váratlanul felmerült biztonsági kérdések esetén ülésezik. Feladata az informatikai biztonság megteremtése és fenntartása.

Az ülések témáit a következők képezik:

- az Információ Biztonsági Szabályzat (továbbiakban: IBSz) által megfogalmazott ellenőrzési és egyéb feladatok elvégzésének értékelése,
- az IBSz-ben rögzített szabályok megszegéséből, illetve be nem tartásából adódó felelősségre vonási eljárások kezdeményezése,
- felmerült biztonsági kérdések megvitatása, szervezetre való hatásának megvizsgálása és megfelelő válaszlépésekhez szükséges döntések meghozatala,
- biztonsági feladatok tervezése, koordinálása, megfelelő biztonsági környezet tulajdonságainak meghatározása,
- rendkívüli biztonsági események megvitatása.

Az Információ Biztonsági Bizottság tagjai az informatikai vezető, a BM HEROS LEK igazgatója által kijelölt személy, a humánpolitikai vezető, és az üzemgazdasági vezető. Ideiglenes tagjai lehetnek azon területek vezetői, amelyek egy biztonsági incidens esetén vagy egyéb ok (fegyelmi eljárás, szakmai konzultáció) miatt döntési hatáskörrel rendelkeznek.

Az informatikai biztonsággal összefüggő kockázatokat, az azok csökkentésére szolgáló ellenőrzéseket az Információ Biztonsági Bizottság értékeli.

A biztonsági ellenőrzés annak feltárására irányul, hogy maga az IBSz, a tényleges folyamatok és a szervezet elfogadhatóan biztosítja-e az üzleti funkciók ellátásának biztonságát, a nem kívánt események megelőzését, felismerését, elhárítását, azaz a biztonsági kockázatok megfelelő kezelését.

Az ellenőrzés nyomán - ha indokolt - kezdeményezni kell a hatályos szabályok, az IBSz és a kapcsolódó utasítások módosítását. Amennyiben új rendelet lép érvénybe vagy a meglévő szabályozás változik ezeket követni szükséges a hatályos biztonsági szabályzatokban.

4.2 Az információ biztonsági dokumentum rendszer felépítése

Információ Biztonsági Politika: A vezetői elkötelezettséget deklaráló, a BM HEROS Zrt. irányelveit tartalmazó dokumentum. A dokumentum irányelv szintű előírásokat tartalmaz, amely deklarálja a szervezet vezetőségének elkötelezettségét, információbiztonsági elvárásait (vezetői akaratát) az információbiztonság területén.

Információ Biztonsági Szabályzat: Az informatikai biztonság alapvető dokumentuma, a BM HEROS által használt IT biztonsági szabályok és előírások ISO/IEC 17799:2000, BS7799 szerint rendszerezett, eljárás szintű követelmények meghatározása.

Rendszer szintű biztonsági előírások, IT biztonsági munkautasítások – A BM HEROS informatikai rendszerének egyes elemeire vonatkozó, üzemeltetési és felhasználói tevékenységeket meghatározó biztonsági követelmények végrehajtási utasításai.

Biztonsági Bizonylatok: - A BM HEROS működése során keletkező információ biztonsággal összefüggő engedélyezési és jóváhagyási folyamat részeit alkotó hivatalos dokumentumok.

4.3 Megfelelés a jogszabályoknak és a belső biztonsági szabályzatoknak

A BM HEROS szabályozásának és működésének meg kell felelnie a vonatkozó törvényi előírásoknak és jogszabályoknak, valamint a jelen IBSz-en túl az egyéb területeket szabályzó belső szabályzatoknak is. Ezen jogszabályok és törvényi előírások, valamint belső utasítások a következők:

Törvények és jogszabályok
2015. évi XCVI. törvény az információs önrendelkezési jogról és az információszabadságról
2015. évi CXXX. törvény az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról
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

BM HEROS belső szabályzatok
Szabályzat a mobiltelefonok használatáról
Szabályzat a munkakör átadás-átvétel rendjéről
Kártérítési szabályzat
Szervezeti és Működési Szabályzat, Intézményi alapító okiratok

4.4 Felülvizsgálati rendszer

A BM HEROS IT biztonsági fenyegetettségének elemzését és kockázatok meghatározását évente el kell végezni.

A szervezet IBSz-nek megfelelő működését igény szerint, de legalább évente teljes körűen ellenőrizni kell. A fenyegetettségek elemzését és a kockázatok meghatározását az informatikai vezetőnek kell végrehajtania, igény esetén független külső szakértőt kell bevonni.

4.4.1 Helyesbítő-megelőző intézkedések rendszere

Az IT biztonsági rendszerrel kapcsolatos

- nem megfelelő működésekről,
- adatvédelmi vagy kezelői hiányosságokról,
- észrevételekről,
- javaslatokról,
- módosításokról,
- tervekről,

a szervezet bármely dolgozója köteles tájékoztatni az informatikai vezetőt.

A vezető az igényeket megvizsgálja, szükség esetén intézkedési terveket dolgoz ki, amelyeket az Információ Biztonsági Bizottság elé terjeszt jóváhagyásra. Jóváhagyás esetén az IT biztonsági rendszert módosítani köteles.

4.4.2 Adatok mérése, kiértékelése, mérési pontok meghatározása

Az IT biztonság szempontjából kritikus pontokon mérési és ellenőrzési rendszert kell bevezetni. A pontok kijelölésénél figyelembe kell venni a szervezet adatvédelmi követelményeit és elvárásait.

A mérési eredmények tárolását ki kell alakítani és az évente elvégzendő felülvizsgálat elősegítése érdekében a vizsgálatban résztvevő személyek részére hozzáférhetővé kell tenni. Az infrastruktúra hozzáférési jogosultságokat az informatikai vezető hagyja jóvá, a célalkalmazások esetén a rendszer kijelölt adminisztrátora (kulcsfelhasználója).

A BM HEROS esetében a minimálisan szükséges kontroll pontok az alábbiak:

Mérendő terület	Mérendő/rögzítendő mennyiség	Beszámolóban szerepel
IT tevékenység	Szerver helyiségekbe való belépési engedélyek rögzítése	-
	Internet hozzáférések statisztikái	-
Illegális IT tevékenység	Észlelt behatolási kísérletek száma	x
Vírusvédelem	Beérkezett vírusok száma	-
	Hatástalanított vírusok száma	-
	Nem internetről beérkezett vírustámadások száma, ezek módja	x
Mentési rendszer	A teszt visszatöltések eredményei	x
Rendelkezésre állás	Rendszerek kieséseinek száma, ezek oka, időtartama, javítási költsége	x
Kapacitásinformációk	Kritikus rendszerekre vonatkozó teljesítményadatok jelentős változása	x
	Tárolási kapacitásokra vonatkozó információk	x
Ellenőrzések eredményei	Feltárt hiányosságok, és azok megszüntetésére vonatkozó intézkedések	x
IT biztonsággal kapcsolatos fegyelemsértések	IT biztonságot megsértő személyekre vonatkozó fegyelmi statisztikák	x
Az IT biztonsági rendszer összesített értékelése	Az IT rendszer szintjére vonatkozó megállapítások, javaslatok	x
Javaslatok	Javaslatok kidolgozása a hiányosságok megszüntetésére, a biztonsági szint emelésére	x

4.5 Informatikai terület szerepkörei

A BM HEROS Zrt. Vezérigazgatója gondoskodik az IBSz kiadásáról és közzétételéről, valamint felel az IBSz-ben megfogalmazott előírások megtartatásáért, illetve e követelmények teljesítésének ellenőrzéséért.

4.5.1 BM HEROS Vezérigazgató

Feladatai:

- Felelős a BM HEROS és érdekeltségei komplex módon értelmezett biztonsági tevékenységének (objektumvédelem, vagyonvédelem, információbiztonság, titokvédelem, humán védelem, rendkívüli és krízis helyzetek kezelése, tűzvédelem, biztonsági oktatások) szakmai irányításáért, végrehajtásáért, ellenőrzéséért, a szervezet biztonságpolitikai érdekeinek és törekvéseinek érvényesítéséért.
- Felelős a BM HEROS működését, üzletmenetét közvetlenül vagy közvetve érintő adatok és információk rendelkezésre állásának, integritásának, bizalmasságának és sértetlenségének az adatkezelések jogszerűségének és minőségének biztosításáért.
- Feladata a BM HEROS biztonságának, mint állapotnak a fenntartását szolgáló és garantáló műszaki-technikai, fizikai, jogi és adminisztratív, tervezési, szervezési, vezetési, oktatási, végrehajtási feladatok és intézkedések irányítása, összehangolása, kidolgoz(tat)ása, ezek folyamatos korszerűsít(tet)ése, valamint az e területet érintő jogszabályok, belső utasítások és szabályzatok betartásának, illetve betartatásának ellenőrzése.
- Feladata a munkavállalók a BM HEROS területén, vagy a szervezettel kapcsolatba hozható módon veszélyeztető jogsértő magatartások megelőzése, felderítése, illetve folytatásának megakadályozása, ezen események kivizsgálásának kezdeményezése. A vizsgálatot folytató belső ellenőrzés támogatása.

4.5.2 Informatikai vezető

Feladatai:

- Hatásköre a BM HEROS minden informatikai rendszerelemére, legyen az földi, vagy felhőben üzemeltetett egyaránt kiterjed.
- Az informatikai vezető felelős a BM HEROS informatikai rendszerének folyamatos működéséért, a szükséges fejlesztések tervezéséért és kivitelezéséért, illetve az előbbiek sikeres kivitelezése érdekében szükséges döntések meghozataláért.
- Jogosult minden olyan megbeszélésen részt venni, amelynek információbiztonsági, adatvédelmi vonatkozása van. Jogosult észrevételeit és javaslatait megtenni.
- Felelős a felhasználók illetékes vezetőinek kezdeményezései alapján a számítógépes erőforráshoz való hozzáférési jogosultságok meghatározásáért, engedélyezéséért.
- Gondoskodik az üzemeltetési feladatkörök ellátásáról a BM HEROS-al jogviszonyban álló személy kijelölésével, vagy szerződéses kapcsolat létesítésével.
- Kezdeményezi informatikai biztonsági ismeretek oktatását a felhasználók részére.
- Informatikai biztonsági szempontból ellenőrzi az informatikai rendszer szereplőinek tevékenységét.
- Az informatikai rendkívüli eseményeket, az esetleges rossz szándékú hozzáférési kísérletet, illetéktelen adatfelhasználást, visszaélést kivizsgálja. Javaslatot tesz a szervezet vezetőjének a további intézkedésekre, a felelősségre vonásra.
- Az SZMSZ rendelkezései és a munkaköri leírások alapján ellenőrzi az informatikai rendszer szereplőinek jogosultsági szintjét.
- Ellenőrzi a fejlesztői, teszt rendszerek elkülönítésének megfelelősségét az éles rendszertől.
- Felügyeli az IT helyiségeket, eszközöket és infrastruktúrát érintő karbantartási terveket.
- Felügyeli a beruházásokat, a fejlesztéseket, és az üzemvitelt informatikai biztonsági szempontból, illetve javaslatot tesz rájuk.
- Szúrópróba-szerűen ellenőrzi;
  - az egyes felhasználói gépek hardverkonfigurációját és a telepített szoftvereket összeveti a felhasználónak engedélyezett szoftverlistával,
  - azt, hogy a rendszerben aktuálisan beállított felhasználói jogosultságok megegyeznek-e a jóváhagyott jogosultságokkal,
  - azt, hogy a javításra kiszállított eszközökön adat ne kerüljön ki,
  - az adathordozók selejtezését.
- Értékeli a rendszer eseménynaplóit.
- Ellenőrzi a víruskereső programok használatát.

- Ellenőrzi a dokumentációk meglétét és megfelelősségét.
- Ellenőrzi, hogy a vonatkozó információ biztonsági követelményeket a rendszerek fejlesztési és az alkalmazási dokumentációiban is megjelenítik-e.

Jogai:

- A felügyelete alá tartozó teljes rendszer komplex biztonságával összefüggésben minden üzemeltető és felhasználó felé jogosult intézkedni az SzMSz -nek megfelelően, tevékenységüket korlátozni jelen szabályzat be nem tartása illetve az informatikai rendszer működőképességét veszélyeztető fenyegetés esetén.
- Módosíthatja a felhasználók jogosultságait (beleértve új felhasználóknak az informatikai rendszerbe való felvételét) a munkáltatói jogkört gyakorló illetékes vezetővel történt egyeztetés alapján, azt figyelembe véve.
- Engedélyezi szerverek, valamint a közvetlen hatáskörébe tartozó munkaállomások kiszállítását.
- Felelős a rendszerbe állítandó eszközök tesztelésééért, használatba vételéért.
- Engedélyezi a mentések felhasználását.
- Meghatározza a rendszergazda (ák) hatáskörét.
- Az egyes alkalmazásokhoz való hozzáférések, jogosultsági rendszerek kialakításában legalább véleményezési joggal rendelkezik.
- Az IBSz-t és annak helyi kiegészítéseit évente felülvizsgálja, és a gyakorlati tapasztalatok, előfordult informatikai rendkívüli események, a jogszabályi környezet változásai, a technikai fejlődés, az alkalmazott új informatikai eszközök, új programrendszerek, fejlesztési és védelmi eljárások, stb. miatt szükségessé váló módosításokra javaslatot tesz.

4.5.3 Rendszergazdák

A feladatkörrel járó biztonsági feladatok leírása, amennyiben a rendszergazdai munkakört külső szerződő fél (szolgáltató) látja el.

Feladatai:

- Menedzseli a szervereket, virtuális gépeket, bérelt, vagy saját nyomtatókat és hálózati elemeket.
- Tevékenységét szerződés (SLA) szabályozza.
- Összeállítja és módosítja az eszközök beállításának dokumentációját.
- Irányítja, kezeli a szerverek és felhasználói gépek biztonsági beállításait.
- Kezeli a rendszerkonfigurációs-, és a rendszerbiztonsági adatokat.
- Telepíti a rendszerprogramokat.
- Végrehajtja a biztonsági másolatok és archiválások készítését, ellenőrzi a központi mentések lefutását.

- Felelős azért, hogy a javításra kiszállított eszközök merevlemezei adatot ne tartalmazzanak (kivéve a sérült, nem minősített HD).

Jogai:

- Minden olyan jogot gyakorol, amelyek az informatikai rendszer operációs rendszer szintű üzemeltetéséhez szükséges.
- Elvégzi a rendszermentések visszaállítását, egyeztetve az informatikai vezetővel, illetve a szakmai szervezet/alkalmazásgazda kezdeményezését követően.
- Jogait és kötelességeit az IBSz hatálya alá tartozó minden olyan területen gyakorolja, amelynek felügyelete a rá kiszabott számítástechnikai rendszer üzemeltetéséhez szükséges.

4.5.4 Kiemelt felhasználók

Feladatai:

- A kiemelt felhasználók jogosultságai a feladatkörtől és szakmai területtől függően, meghaladják a hagyományos felhasználók jogosultságait.
- Kiemelt felhasználok a Vállalatirányítási rendszer támogatói.
- Speciális célrendszerek kezelői. (pl.: AutoDesk szoftverek)

Jogai:

- Minden olyan jogot gyakorol, amelyek az általa felügyelt informatikai rendszer üzemeltetéséhez szükséges.

4.5.5 Felhasználók

Feladatai:

- Minden felhasználó felelős az általa használt eszközök rendeltetésszerű használatáért.
- Minden felhasználó, a reá vonatkozó szerint, felelős az általa elkövetett szabálytalanságért, valamint a keletkező károkért és hátrányért.
- A vonatkozó informatikai-szakmai és az IBSz-ben megfogalmazott szabályokat megismerni és betartani, illetve ezek betartásában az informatikai rendszer használatát irányító személyekkel együttműködni.
- A számára rendelkezésre bocsátott számítástechnikai eszközöket megóvni.
- Belépési jelszavát (jelszavait) az előírt időben változtatni, kezelni.
- Számítógépét a helyiség elhagyása esetén olyan állapotban hagyni, hogy azt illetéktelen ne használhassa. A munkaállomásokat lezárni szükséges, hogy csak jelszó használatával lehessen hozzáférni.
- Az észlelt rendellenességekről tájékoztatni a közvetlen felettesét és a megfelelő informatikai szakembert.

4.5.5.1 A BM HEROS informatikai rendszerét használó minden felhasználónak TILOS:

- A saját használatra kapott számítógép rendszerszintű beállításainak módosítása (ebbe nem értendők bele az irodai programok felhasználói beállításai).
- A munkaállomására telepített aktív vírusvédelem kikapcsolása.
- Saját belépési jelszavát (jelszavait) harmadik személy rendelkezésére bocsátani.
- A számítógép hálózat fizikai megbontása, a számítástechnikai eszközök lecsatlakoztatása, illetve bármilyen számítástechnikai eszköz rácsatlakoztatása a hálózatra az informatikai rendszert üzemeltetők tudta nélkül.
- A számítástechnikai eszközökből összeállított konfigurációk megbontása, átalakítása.
- Bármilyen szoftver installálása, Internetről való letöltése, külső adathordozóról merevlemezre való másolása a rendszergazda engedélye nélkül.
- Bármilyen eszköz beszerelése és annak használata.
- Belső bizalmas és titkos adatok szervezetből történő kijuttatása vagy magán célú felhasználása, harmadik személy rendelkezésére bocsátása.

5 Általános információ biztonsági követelmények

5.1 Általános biztonsági követelmények meghatározása

5.1.1 Előírások a külső személyek általi hozzáférésekkel kapcsolatban

A külső személyeknek – karbantartók, tanácsadók stb. – a BM HEROS informatikai rendszeréhez való hozzáférése veszélyeztetheti a szervezet adatainak bizalmasságát, sértetlenségét.

Egy külső személy hozzáférésének engedélyezésénél a következő szempontokat kell megvizsgálni:

- A külső személy vagy cég megbízhatóságát.
- A külső személy vagy cég által elvégzendő munka részfeladatait.
- Az elvégzett munka informatikai hátterét.
- Azokat a kockázatokat melyekkel az informatika biztonsága szempontjából számolni lehet.
- Az érintett rendszereket, logikai és fizikai hozzáférés szempontból.
- Az elvégzett munka emberi erőforrás vagy Informatikai igényét.
- A munka befolyásolja-e a napi munka menetét.

Ezt szem előtt tartva a külső személyek munkavégzésének szabályai a következők:

- Az informatikai vezetőnek a külső személy a munkafolyamat egyeztetése során minden munkafolyamatról köteles beszámolni, amely bármilyen módon érinti az informatikai rendszert.
- A BM HEROS IT rendszereivel kapcsolatos, vagy azokat érintő munkavégzés céljából érkező külső személy a BM HEROS területén a szerződés aláírása után, kizárólag az informatikai vezető, vagy az általa kijelölt személy (pl.: Rendszergazda) felügyeletével tartózkodhat.
- A külső vállalkozóval **Titoktartási nyilatkozatot** kell aláíratni a tudomására jutott adatok, információk védelme, és sértetlensége érdekében.
- A BM HEROS külső szakértővel csak olyan szerződést köthet, amely a megbízott külső szakértő tekintetében biztosítja a BM HEROS-ra vonatkozó titokvédelmi jogszabályok érvényesülését. A szerződéskötés során figyelembe kell vennie az informatikára vonatkozó előírásokat, szabályzatokat, jelen IBSz előírásait, a törvényi és egyéb jogi előírásokat, valamint a szellemi és szerzői jogokra vonatkozó előírásokat. Az információ biztonsággal kapcsolatos előírásokat, elvárásokat, esetleges szankciókat a külső személyekkel kötött szerződésekben szerepeltetni kell.
- A BM HEROS informatikai rendszereihez való hozzáféréshez ideiglenes és személyre szóló hozzáférési jogosultságot kell biztosítani, amiről az Informatikai Vezető gondoskodik, amennyiben a munkavégzéshez feltétlenül szükséges.

- Az ideiglenes hozzáférési jogot a külső személy munkájának befejezésekor a rendszergazda visszavonja. A visszavonás ellenőrzése az Informatikai vezető feladata.

5.1.2 Személyi biztonság - humán védelmi intézkedések

5.1.2.1 Munkaerő felvétel informatikai biztonsági vonatkozásai

Minden informatikai rendszert igénybevevő felhasználóval belépésekor a HR szervezet az informatikai vezető esetleges segítségével köteles az Információ Biztonsági Szabályzat felhasználókra vonatkozó részeit és az informatikai rendszer kezelésével, az informatikai rendszer használatával kapcsolatos általános szabályokat megismertetni és azok elfogadásáról nyilatkozatot aláíratni.

5.1.2.2 Helyettesítés az Informatikai szervezetben

A BM HEROS ügyviteli folyamatainak kialakítása és megvalósítása az informatikai rendszerek üzemeltetése, az információ biztonság érvényesítése és ellenőrzése területén, továbbá az ezekhez kapcsolódó feladatok ellátásához biztosított munkaerő létszáma és tudása biztosításakor, illetve a folyamatok szervezése során meg kell oldani, hogy egy személy hiányzása:

- ne hátráltassa elfogadhatatlan mértékben a szervezet ügyviteli folyamatait, vagy
- maximum 5 napon belül a feladatait és felelősségét átvehesse egy másik megfelelő ismeretekkel és jogosultságokkal rendelkező személy.

A feladat és felelősség átvétele során a feladatot átvevő személy betöltheti a hiányzó személy munkakörét és/vagy kizárólag a helyettesítéssel járó feladatokat láthatja el, vagy amennyiben összeférhetetlenség nem áll fenn a saját munkakörét is betöltheti, feltéve, hogy a kettős munkakör ellátás nem hátráltatja elfogadhatatlan mértékben egymást.

Amennyiben a helyettesített személy távolmaradása meghaladhatja a két hónapot, úgy a helyettesítést nem lehet kettős munkakör ellátással folytatni. Ebben az esetben olyan személyt kell alkalmazni, aki kizárólag a helyettesített személy feladatait látja el.

5.1.3 Az információ biztonság fenntartása

Az informatikai vezető gondoskodik az IBSz és a vonatkozó belső utasítások egységes szerkezetbe foglalásáról és a vezérigazgatói utasítás útján történő kiadásáról. Ennek felülvizsgálatát évenként egy alkalommal kezdeményezi.

Az egyéb jogviszonyban a BM HEROS területén munkát végző személyek részére is el kell készíteni, át kell adni az informatikai biztonsággal összefüggő hatályos szabályok rájuk vonatkozó részének közérthető kivonatát. A szervezeti egység vezetője felel azért, hogy a beosztott munkavállalók megismerhessék a rájuk vonatkozó biztonsági szabályzatokat. Az új belépők tájékoztatása a HR és az informatikai terület feladata.

5.2 Az informatikai rendszerben keletkező adatok besorolási követelmények meghatározása

5.2.1 Adatok biztonsági besorolása

Az informatikai rendszerben keletkező adatokat bizalmasság, sértetlenség, és rendelkezésre állás szempontjából osztályozni kell.

A BM HEROS és BM HEROS LEK esetében az alábbi három szint megvalósításával kezeli.

5.2.1.1 Az adatok osztályozásának irányelvei

Osztályozási szintek

- 1. Publikus adatok
- 2. Belső adatok
- 3. Titkos adatok

Az osztályozás alapját a bizalmasság, a sértetlenség, és a rendelkezésre állás sérüléséből, vagy elvesztéséből keletkező, a BM HEROS és a BM HEROS LEK számára kimutatható lehetséges hátrány nagysága illetve a törvényi szabályzás képezi.

A bizalmasság, sértetlenség, és rendelkezésre állás sérüléséből, vagy elvesztéséből vagyoni, erkölcsi, és jogi hátrány származhat.

Az adatok osztályozását az adatgazdák végzik. Az adatgazda szerepét annak a szervezeti egységnek a vezetője tölti be, aki az adott folyamatért felelős. Több egymáshoz kapcsolódó vagy független folyamat esetén az érintett szervezeti egységek közös felettes vezetője dönt, a szervezeti egységek javaslata alapján.

5.2.1.2 Adatok nyilvántartása és kezelése

A BM HEROS adat nyilvántartásnak az alábbiakra kell kiterjedni:

- Az adat, vagy adatcsoport (rendszer) megnevezése
- Az adatosztályozási szint bizalmasság, sértetlenség, és rendelkezésre állás szerint
- Az adatgazda megnevezése
- Az adatokat kezelő eszközök megnevezése

A nyilvántartás vezetéséért az informatikai vezető felel, a nyilvántartáshoz szükséges információk szolgáltatásáért az adatgazdák felelősek.

	Publikus adatok	**Belső adatok**	**Titkos adatok**
Jelölés	Nincs követelmény	A belső adatokat tartalmazó adathordozókat „belső használatú", „szolgálati használatra" jelöléssel kell/célszerű ellátni.	A titkos adatokat tartalmazó adathordozókat „titkos" jelöléssel kell ellátni.
Tárolás	Nincs követelmény	Az adathordozókat zárható szekrényben, vagy asztalfiókban kell tárolni. Az informatikai rendszerben biztosítani kell az adatokhoz való hozzáférés vezérlését.	A titkos adatokat tartalmazó adathordozókat páncélszekrényben kell tárolni. Az informatikai rendszerben biztosítani kell az adatokhoz való hozzáférés hitelesítésen alapuló elérését.

Adatátvitel	Nincs speciális követelmény	Belső hálózaton való továbbításkor nincs speciális követelmény. Külső kommunikáció esetén megfelelő protokollt, vagy fájltitkosítást kell alkalmazni.	Szigorúan titkos adatokat csak titkosított csatornán, hitelesített felhasználónak szabad küldeni, vagy csak helyi hozzáférés lehetséges.
Adatmegosztás	Nincs speciális követelmény	Adatmegosztás csak az adatgazda engedélyével lehetséges.	Adatmegosztás csak az adatgazda engedélyével lehetséges.
Megsemmisítés, törlés	Nincs speciális követelmény	Megsemmisítés az adatgazda engedélyével.	Megsemmisítés az adatgazda engedélyével. Megsemmisítés előtt az adatokat visszaállíthatatlanul törölni kell.

6 Információ Biztonsági Eljárások

6.1 Biztonsági szintektől függő intézkedések és eljárások

6.1.1 Berendezések fizikai védelme- Fizikai és környezeti biztonság

A BM HEROS épületében különböző biztonsági zónákat kell kialakítani annak érdekében, hogy az informatikai rendszer kritikussága és a benne kezelt adatok besorolása alapján az informatikai rendszer és környezete a besorolt rendszerek, adatok megfelelő fizikai és környezeti védelmét garantálni tudják. Az 5.2.1. pontban meghatározott osztályozási szintek alapján a fizikai és környezeti biztonság a következő biztonsági zónák és fizikai illetve környezeti védelemi megoldások kialakításával valósítható meg.

Zóna követelmények	1. szintű biztonsági zóna (pl.:Normál iroda)	2. szintű biztonsági zóna (pl.:hálózati rendezők)	3. szintű biztonsági zóna (pl.:Szerverszoba)
Építészeti, kialakítási követelmények			
Falak	-	-	Tömör falak kialakítása szükséges.
Nyílászárók		A hálózati rendezők ajtajai zárhatók.	Ablakok kialakítása nem lehetséges, zárt ajtó és beléptető, vagy megfigyelő rendszerrel történő kialakítás szükséges.
Födém, padlószerkezet	-	-	Álpadló, antisztatikus burkolat kialakítása szükséges.
Hozzáférési, belépési követelmények			

Zóna követelmények	1. szintű biztonsági zóna (pl.:Normál iroda)	2. szintű biztonsági zóna (pl.:hálózati rendezők)	3. szintű biztonsági zóna (pl.:Szerverszoba)
Belépés, beléptetés eszközei	-	A hálózati rendezőkhöz való hozzáférés kulccsal történik.	A helyiségekbe történő belépés mágneskártyával, vagy dokumentáltan történik.
A belépés engedélyeztetése, naplózása	Normál a BM HEROS területére érvényes belépési engedélyezteté s szükséges. Általános belépési követelmények hez kapcsolódó naplózások vonatkoznak rá.	A hálózati rendezőkhöz való hozzáférés kulcsok felvételével és dokumentálásá val lehetséges. Másolásvédett kulcsok használata szükséges, a kulcsokból egy példány a raktárért felelős rendszergazdá nál, egy pedig lepecsételt borítékban a biztonsági szolgálatnál.	A szerverszobához történő hozzáférések engedélyezése az informatikai vezető hatásköre. A belépés naplózva (automatikus, kézi) kell kialakítani.
Környezeti követelmények			
Klimatizálás	-	Klimatizálás kialakítása javasolt.	Klimatizálás kialakítása szükséges.
Páratartalom szabályozás a	-		A páratartalom szabályozása Javasolt.

Zóna követelmények	1. szintű biztonsági zóna (pl.:Normál iroda)	2. szintű biztonsági zóna (pl.:hálózati rendezők)	3. szintű biztonsági zóna (pl.:Szerverszoba)
Áramellátás szabályozása	-	Az áramellátás szabályozása szükséges.	Az áramellátás szabályozása, és redundáns kialakítása szükséges.
Biztonsági követelmények			
Tűzvédelem	A tűzvédelmi előírásoknak megfelelően.	Kézi tűzoltó készülékek elhelyezése szükséges.	Kézi tűzoltó készülékek elhelyezése szükséges.
Árnyékolás védelem	-	Minimum 20 dB-es csillapítás szükséges az elektromos, és mágneses sugárzás ellen.	Minimum 40 dB-es csillapítás szükséges az elektromos, és mágneses sugárzás ellen.
Riasztás	-		Riasztó eszközökkel kialakítással kell ellátni, mely illetéktelen behatolás (betörés) és tűz esetén jelez.
Biztonsági kamerák	-	-	Videokamerás megfigyelő rendszer elhelyezése szükséges a helyiségben és a helyiségbe történő belépési pontokon.

A kialakított informatikai biztonsági zónákban történő munkavégzésre, a zónát veszélyeztető fenyegetettségek függvényében, más-más informatikai biztonsági követelmények tartoznak.

Az 1. biztonsági zónába tartozó alap védelemmel ellátott zónán kívül a biztonsági zónákban történő munkavégzésre a következő biztonsági szabályozások érvényesek.

A 2. szintű biztonsági zónába tartozó helyiségekben történő munkavégzés:

- Az informatikai rendszer egyes elemeinek karbantartását, javítását, szerelését csak olyan személyek végezhetik, akik titoktartási nyilatkozatot írtak alá, vagy a munkavégző személyt foglalkoztató vállalkozás – a megbízásából kiküldött személyre vonatkozóan is – titoktartási kötelezettséget vállalt.

A 3-as biztonsági zónába tartozó helyiségekben történő munkavégzés:

- A kiemelt biztonsági zónába tartozó helyiségbe csak a BM HEROS informatikai munkatársai és a rendszergazdák léphetnek be. Az informatikai rendszer egyes elemeinek karbantartását, javítását, szerelését csak olyan személyek végezhetik, akik titoktartási nyilatkozatot írtak alá, vagy a munkavégző személyt foglalkoztató vállalkozás – a megbízásából kiküldött személyre vonatkozóan is – titoktartási kötelezettséget vállalt és a munkájukat csak és kizárólag a BM HEROS informatikai munkatársának felügyelete mellett végezhetik.

6.1.1.1 Irodahelyiségek és informatikai eszközök biztonságának szavatolása

A BM HEROS informatikai területére vonatkozó egyéb fizikai védelmi intézkedések a következők:

- Az IT helyiségek olyan ajtókkal legyenek ellátva, amelyek legalább 30 perces műbizonylatolt tűzgátlással rendelkeznek.
- Az IT helyiségeken belül tűzjelzésadók kerüljenek telepítésre. A jelzésadók jelzéseit mind a helyiségen belül, mind a rendészetnél meg kell jeleníteni. Az informatikai eszközöket működtető szervezeti egységekben a tűzvédelmet a BM HEROS Tűzvédelmi Szabályzata szabályozza.
- A számítógép helységeket klimatizálni kell, úgy, hogy az információtechnológiai eszközök környezeti hőmérséklete működés közben 15-22 C°, tárolási hőmérséklete 0-40 C° között maradjon, a relatív páratartalom pedig ne haladja meg a 40%-ot. Ezekben a helyiségekben vagy legyen olyan tartalék klímaberendezés, amely az addig működő berendezés meghibásodásakor automatikusan beindul, vagy pedig olyan jelzőrendszert kell telepíteni, amely a klímaberendezés meghibásodásakor a jelez.

Felhasználói számítógépekre és a kapcsolódó perifériákra vonatkozó előírások:

- A felhasználó köteles az általa használt informatikai eszköz épségét, annak működőképes állapotát megőrizni. Bármilyen állapot-, vagy működésbeli rendellenességet tapasztal, azt az informatikai vezetőnek jeleznie kell.
- Tilos a felhasználó részéről bármilyen illetéktelen beavatkozás, ami a berendezés műszaki állapotában, működésében valamilyen változást okozhat. Ide értendő a berendezés szétszedése, átalakítása, vagy bármilyen szoftver telepítése.

A rendszergazdák a saját azonosítójukkal és jelszavukkal jogosultak a felhasználók munkaállomásához hozzáférni a felhasználók távolléte esetén is, ha beállítási, karbantartási, ellenőrzési, szoftvertelepítési műveleteket hajtanak végre. A hozzáféréshez a felhasználók előzetes hozzájárulása szükséges.

Hibajavítás esetén a felhasználó HelpDesken (support@securicum.hu) keresztül jelzi a meghibásodást és az üzemeltetés ez alapján kezdi meg a hiba elhárítását.

6.1.2 Logikai hozzáférés

6.1.2.1 A hozzáférés követelményrendszere

- A használt informatikai rendszereknél az informatikai vezető meghatározza a jogosultság-kiosztás szempontjából irányadónak tekinthető szerepköröket, azokat jogosultsági mátrix formájában rögzíti.
- Az informatikai rendszerekhez hozzáféréssel rendelkező alkalmazottak (felhasználók) konkrétan meghatározott szerep(munka-)körbe sorolandók, a vezetőjük kérésére a rendszergazdáktól megkapják a vonatkozó hozzáférési jogosultságokat.
- A jogosultságok kiosztását (a felhasználók felhasználó csoportokba sorolását) a felhasználó közvetlen szakmai (szervezeti) felettese határozza meg, majd átadja az informatikai vezetőnek (rendszergazdának) végrehajtásra.
- A szerepkörök (munkahelyi beosztás, feladatok) változásakor a hozzáférési jogosultságokat 5 napon belül át kell állítani. A megszűnő jogokat a korábbi, az újonnan adományozandóakat a szakterületi közvetlen felettes határozza meg.
- A hozzáférés-védelem szempontjából kiemelten fontos biztosítani, hogy az informatikai rendszerek felhasználóinak tényleges hozzáférési jogosultságai a szerepkörüknek megfelelő legyenek. Ezzel kapcsolatosan:
  - A tényleges jogosultság-kiosztást időközönként ellenőrizni kell,
  - Az ellenőrzést az informatikai vezető (rendszergazdák) végzi, az ellenőrzés során össze kell vetni az elvárt (jogosultsági mátrixban szereplő) és a tényleges jogosultság-kiosztást,

- Eltérés esetén az informatikai vezető a jogosultságokat visszaállítja az elvárt beállításoknak megfelelően, és vizsgálatot kezdeményez az eltérés okainak megállapítására.
- Egyes szervezeti egységekre vagy rendszerekre kiterjedő, rendkívüli (eseti jellegű) ellenőrzést a Vezérigazgató és informatikai vezető, adott szervezeti egység vezetője, vagy az IBB kezdeményezhet.

6.1.2.2 Hozzáférési jogosultságok nyilvántartása

- A felhasználók azonosítása alatt az informatikai rendszerhez hozzáférő felhasználók személyazonosságának (identitásának) a rendszerben történő egyedi, egyértelmű és hiteles megjelenítését értjük.
- Az egyedi felhasználói azonosítót a hozzáférések (jogosultságok) szabályozására, az adat védelemre, és a hitelesítés támogatására kell használni.
- A felhasználó azonosítónak meg kell felelni az egyediség kritériumának. különböző felhasználók számára egyazon azonosító nem adható ki. Kivételt képez a szervezeti egységhez kötött csoport e-mailek használata, melyekhez írásos felhatalmazásában megnevezett felhasználók férhetnek hozzá.
- A felhasználói azonosítók képzésére és új felhasználók rendszerbe történő felvitelére kizárólagosan a rendszergazda jogosult.
- Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakör ellátásához szükséges minimális funkcióelérést biztosíthatják.
- A hozzáférési jogosultságok kezelése, a jogosultság igénylés folyamata, a ***Jogosultság kezelési, kiadásai munkautasításban*** van rögzítve.
- A felhasználói azonosítók nem visszavonhatatlanok. Ezzel összefüggésben:
  - A BM HEROS munkatársai és külső munkavállalói, munkába állásukat követően a lehető legrövidebb időn belül meg kapják felhasználói azonosítójukat. Ennek megtörténtéig jelenlegi vagy korábbi felhasználói azonosító használata – akár átmeneti jelleggel is –szigorúan tilos.
  - A kiosztott azonosítót haladéktalanul használatba kell venni. Ennek első lépéseként az induló (alapértelmezett) jelszót meg kell változtatni.
  - A BM HEROS dolgozóinak felhasználói azonosítóját munkaviszonyuk megszűnésekor (a külső munkavállalók felhasználói azonosítóját a megbízási jogviszony megszűntével) haladéktalanul érvényteleníteni kell. (a fiók először tiltásra kerül, majd 30 napos átmeneti fázis után törlésre)
  - A munkaviszonyukat huzamosabb ideig szüneteltető, vagy a munkavégzésben hosszabb ideig más ok miatt részt nem vevő felhasználók azonosítóját újra munkába állásukig fel kell függeszteni

(inaktiválni kell). Az inaktiválást a közvetlen felettes kéri az informatikai vezetőtől. Az azonosító újraaktiválási igényének felmerülésekor a hozzáférés helyreállítását szintén a közvetlen felettes kérheti.

- A felhasználók szervezeten belüli áthelyezése kapcsán felmerülő jogosultsági változásokat (megszűnő felhasználói azonosítók felfüggesztése vagy törlése, új azonosítók létrehozása) haladéktalanul át kell vezetni.
- Külső munkatársak csak meghatározott időre és korlátozott lehetőségeket biztosító (pl. csak írási joggal vagy csak bizonyos területre érvényes) felhasználói azonosítót kaphatnak. A részükre kiadott azonosítóról legyen egyértelműen megállapítható, hogy az külső munkatársi státuszú felhasználóhoz tartozik. Külső munkatársak azonosítójának létrehozását, számára jogosultságok megadását azon szervezeti egység vezetőjének kell kezdeményeznie informatikai vezetőnél, akivel a szóban forgó felhasználó közvetlen (szerződéses) viszonyban áll.
- Gyakornokok esetén a hozzáférési jogosultságok hasonlóan a külső munkatársak számára létrehozott azonosítókhoz, csak bizonyos, a munkavégzéshez feltétlenül szükséges területekhez való hozzáférést tegyenek lehetővé.

6.1.2.3 Felhasználói és rendszergazdai jogosultságok létrehozása, megszűntetése, megváltoztatása

Új munkatárs hozzáférési rendszerbe való illesztését a Jogosultságigénylő űrlap kitöltésével és elküldésével, az adott szervezeti egység vezetője írásban (e-mailben) igényelheti az informatikai vezetőtől.

A rendszergazdák feladata a jóváhagyott, a felhasználó megfelelő, alkalmazásokra lebontott jogosultsági szintjeinek beállítása, az elektronikus levelező fiók létrehozása, a címtár bejegyzések elvégzése, valamint a felhasználói azonosító aktiválása.

Minden felhasználó definiálásánál törekedni kell az egy-egy értelmű megfeleltetésre, azaz kerülni kell a közösen használt felhasználói azonosítók létrehozását. Csoportos azonosítót csak és kizárólag az informatikai vezető előzetes írásbeli engedélye alapján lehet beállítani.

A rendszergazda a jogosultságot fizikailag beállítja és átvezeti a jogosultság-kiosztási nyilvántartásban a változást. A nyilvántartás rendszeres időközönkénti ellenőrzése az informatikai vezető feladata.

A felhasználói hozzáférés zárolása történik az alkalmazott kilépésekor. Ennek biztosítására:

- Azonnali felmondás esetén, illetve ha a kilépő alkalmazott vezetője úgy ítéli meg, a jogosultság azonnal visszavonásra kerül. A kilépő alkalmazott vezetője ebben az esetben köteles telefonon értesíteni az informatikai vezetőt.
- Határozott idejű felmondás esetén a jogosultság visszavonása „kilépési"" lap aláírásával egy időben történik.

A kilépett munkavállaló munkáltatói jogú vezetője a munkavállaló tájékoztatása mellett köteles rendelkezni a felhasználó levelezésének, adatainak, dokumentumainak további kezeléséről (archiválás, törlés, harmadik személy általi hozzáférhetőség).

A BM HEROS informatikai rendszereinek elérésére használható hozzáférés szintjei a következők lehetnek:

- Névre szóló rendszergazdai hozzáférés esetén, a rendszergazdai jogosítványt a rendszergazda a saját nevére szóló, kizárólagosan általa használt, megfelelő rendszergazdai jogkörrel felruházott felhasználói azonosító segítségével használhatja. A beépített (root, administrator, stb.) rendszergazdai hozzáférés csak abban az esetben tekinthető ilyennek, ha azt kizárólag egy személy használja. Ha a rendszerben van lehetőség személyhez kötött rendszergazdai jogosítványok kiadására, az említett beépített jogosultságokat használni tilos!
- Csoportos rendszergazdai hozzáférés esetén, a rendszergazdai jogosítványt a rendszergazda egy csoportos, több rendszergazda által is használt, rendszergazdai jogkörrel felruházott felhasználói azonosító segítségével lehet használni. A beépített (root, administrator, stb.) rendszergazdai hozzáférés abban az esetben tekinthető ilyennek, ha azt több személy ismeri, használja. Amennyire technikai és egyéb szempontok lehetővé teszik, a csoportos rendszergazdai hozzáférést kerülni kell!
- Névre szóló felhasználói hozzáférés keretében a felhasználó külön, saját névre szóló, más által nem használt, kizárólag a munkája ellátása miatt elengedhetetlen jogosítványokkal rendelkezik az informatikai rendszerekhez és azok erőforrásaihoz, az üzleti folyamatok ellátásához kapcsolódó feladatok elvégzéséhez.
- Csoportos felhasználói hozzáférés keretében több felhasználó azonos, a munkája ellátása miatt elengedhetetlen felhasználói hozzáférést használ az informatikai rendszerekhez és azok erőforrásaihoz, az üzleti folyamatok ellátásához kapcsolódó feladatok elvégzéséhez. Amennyire technikai és egyéb szempontok lehetővé teszik, a csoportos felhasználói hozzáférést csak a védelmet nem igénylő adatokat tartalmazó rendszerek esetén szabad alkalmazni, az egyértelműség és követhetőség miatt inkább a névre szóló felhasználói hozzáférést kell választani.

6.1.2.4 Jelszómenedzsment

A BM HEROS számítógépes hálózatába bejelentkezési névvel rendelkező felhasználó köteles a bejelentkező nevéhez tartozó jelszó megőrzésére. A saját bejelentkező névhez tartozó jelszót elárulni, mások által is elérhető módon feljegyezni nem szabad.

Bejelentkező névhez tartozó jelszót csak a kijelölt rendszergazdák állíthatnak be, illetve közölhetnek abban az esetben, ha

- Új felhasználó felvétele, vagy egyéb ok (pl. elfelejtés) miatt a felhasználó előtt még ismeretlen új belépési jelszót definiált.
- Ebben az esetben a következő szabályok érvényesek:
  - Elfelejtés esetén a felhasználó a rendszergazdától igényelhet új jelszót. A felhasználó azonosítása a rendszergazda feladata.
  - A felhasználó az átvételt követő első bejelentkezésekor azonnal köteles a jelszó megváltoztatására.

Azon informatikai rendszerek esetén, melyek rendelkeznek a megfelelő technikai feltételekkel, a hitelesítéshez használt felhasználói hozzáféréshez rendelt jelszavaknak az alábbi kritériumoknak kell megfelelni:

- A jelszavakat a számítógépes rendszerben nyílt formában tárolni tilos, gondoskodni kell megfelelő titkosítási védelemről.
- Belépéskor a beírt jelszó ne legyen olvasható a képernyőn.
- A felhasználói azonosító és a hozzá tartozó jelszó együtt nem tárolható, továbbítható (sem papíralapú, sem elektronikus formában).
- A jelszónak tetszőlegesen megváltoztathatónak kell lennie.
- A felhasználói jelszavak minimális hossza 8 karakter.
- A felhasználói jelszavak maximum 180 napig lehetnek érvényesek.
- Egy jelszó minimum 1 napig érvényes (1 napon belül nem lehet kétszer megváltoztatni).
- Az utolsó 5 jelszót nem lehet újra használni.
- A felhasználóknak be kell jelentkezni a jelszó megváltoztatásához.
- A felhasználóknak meg kell változtatniuk a jelszavukat, amikor első alkalommal használják felhasználói azonosítójukat.
- Szabályozni, és szűrő segítségével biztosítani kell a jelszavak összetettségét: szükséges nagybetűk, kisbetűk, számok és speciális karakterek együttes használatával.
- Mind a sikeres, mind a sikertelen belépési és kilépési kísérleteket naplózni kell.

- Ha egy felhasználói azonosító 60 napig inaktív, akkor azt a szervezeti egység vezetőjének tájékoztatása mellett a rendszert üzemeltető rendszergazdának fel kell függeszteni.
- A rendszergazdai jelszavak minimális hossza 12 karakter.
- A rendszergazdának lokálisan kell bejelentkezni a jelszó megváltoztatásához.

A fenti szabályok SSO (Single Sign-on) használata esetén fokozottan érvényesek.

6.1.2.5 A munkaállomások hozzáférésére vonatkozó előírások

- A számítógépes munkaállomások képernyőit (monitor) úgy kell elhelyezni, hogy az azon megjelenő információkat illetéktelen személy ne láthassa.
- A BIOS beállításait rendszergazdai jelszóval kell védeni módosítás ellen.
- A folyó munka során nem használt nem nyilvános anyagokat, adathordozókat el kell zárni.
- Felügyelet nélkül hagyott munkahelyen személyes adatot vagy üzleti titkot tartalmazó dokumentum/adathordozó nem maradhat védelem nélkül.
- A számítógép-hálózatba bejelentkezett munkaállomásokon, nem a BM HEROS-ban nyilvántartott szoftverek (szórakoztató szoftverek, játékok, egyéb segéd programok, filmek) installálása, futtatása, tárolása nem megengedett.

6.1.3 Adat- és rendszermentések

6.1.3.1 Az informatikai rendszerek mentési rendszerének kialakítási elvei

Az adatok és a rendszerek besorolását figyelembe véve, a mentésért felelős rendszergazda és az informatikai vezető kötelesek a mentési terv alapjait minden rendszerre nézve mentési utasításban meghatározni. Az adott rendszerre vonatkozó mentési, archiválási munkautasítást a mentésért felelős rendszergazda készíti el.

Az alapkövetelmények, melyek köré a mentési utasítás felépíthető a következők:

- Mentési frekvencia, – a mentések sűrűsége.
- Mentési eljárás, – központi mentés, mely a következő módszerek egyikével történhet:
  - teljes mentés,
  - inkrementális mentés,
  - differenciális mentés,
  - ezen mentések kombinációja.
- Adatbázis kezelők esetében:

- off-line mentés,
- on-line mentés.
- Mentő eszközök fajtája, típusa, mennyisége, elhelyezése.

Szükséges továbbá a vonatkozó rendszerek adattartalmának ismeretében meghatározni az archiválási rendet és módot, illetőleg az őrzési időt és ennek módját.

A mentési rendszerterv kialakításához meg kell határozni a mentés végrehajtását leíró következő paramétereket:

- A mentési időpontot.
- A mentési eljárást a rendszeren belül.
- A mentő eszközök fajtáit.
- A periodikus mentési módszert, azaz a mentési médiumok forgási rendszerét.

A rendszerekre vonatkozó mentési utasításban definiálni kell a mentési rendszertervben szereplő paramétereken túl, a következőket:

- Mentendő munkakönyvtárakat.
- Az alkalmazandó média típusát, nevét.
- A rendszeres mentést indító program vagy script helyét és nevét.

6.1.3.2 Mentési előírások a mentésért felelős munkatársak számára

A szabályzathoz kapcsolódó munkautasításban található **Biztonsági mentések és visszatöltések rendje** rendelkezik a különböző mentések módjáról és gyakoriságáról.

- A biztonsági mentésekre (backup) vonatkozó előírások:
  - Adatbázis- és file-szerver adatok teljes körű mentését hetente, inkrementális mentést naponta kell végezni.
  - Rendszer szintű mentéseket legalább havonta kell végezni, de a rendszert (operációs rendszer, adatbázis-kezelő alkalmazás stb.) érintő változtatások (újabb verzió, javító patch stb.) után közvetlenül is.
  - A biztonsági mentések tárolásánál a "háromgenerációs" elvet kell alkalmazni (legalább mindig az utolsó három adatmentés elérhető).
  - A teljes körű és a rendszer szintű biztonsági mentéseket az éles rendszer üzemi környezetétől logikailag és fizikailag (lehetőség szerint földrajzilag is, bérelt bank-széfben) elkülönítetten kell tárolni.
  - A biztonsági mentésekről és a biztonsági mentések adathordozóiról naplót kell vezetni. A napló lehet elektronikus formában is elérhető, amely a mentést végző szoftver által generált log file.

Az archiválás célja az éles üzemű rendszerek által kezelt adatok csökkentése és az éles üzemű rendszerek adatainak későbbi visszakereshetősége.

- Az archív másolat lehetőség szerint újra nem írható vagy írásvédetté tett adathordozóra kerüljön.

- Az archív mentések biztonságos tárolásáról gondoskodni kell. (pl. legalább egy példányban a BM HEROS üzemi működését ellátó telephelyen kívül kell tárolni)
- Az archivált adatok tárolásának meg kell felelni a jogszabályban előírt kötelezettségnek.
- Archivált adat csak abban az esetben törölhető az éles üzemi rendszerből, miután az a külső adattároló eszközre ellenőrzötten mentésre került.
- Az archivált adatok visszakeresése esetén kiemelten kell gondoskodni az eredeti hozzáférési jogosultságok érvényre juttatásáról.
- Az 5.2.1.2 pontban meghatározott feltételeknek és elvárásoknak meg kell felelni a mentési eszközök és adathordozók kezelése során.

6.1.4 Informatikai üzemmenet-folytonosság

Az üzemmenet folytonosság menedzselésének célja a kritikus informatikai rendszerek igény szerinti rendelkezésre állásának és rendeltetésszerű működésének biztosítása.

Az informatikai üzemmenet folyamatos fenntartása érdekében a létrehozott terveket szükséges alkalmazni, amelyek tartalmazzák a valószínűsíthető fenyegetések bekövetkezése esetén elvégzendő tevékenységeket, továbbá biztosítani kell technikai oldalról az informatikai rendszer backup vagy tartalék megoldásait (Backup gépterem kialakítása, tartalék szerver és hálózati eszközök készletezése, backup hálózati vonalak kialakítása, stb.)

6.1.4.1 Informatikai katasztrófahelyzet-kezelési tervek tartalma

Az informatikai vezetőnek felelőssége a katasztrófahelyzet-kezelési terv elkészítése, melynek a következőket kell tartalmaznia:

1. A katasztrófahelyzet-kezelési terv érvényességének behatárolása.
2. A katasztrófahelyzet-kezeléséhez kapcsolódó felelősségek és hatáskörök behatárolása.
3. A katasztrófa elhárításában résztvevő személyek feladatai jogai és kötelességei.
4. A katasztrófa elhárítás közben történő jelentési kötelezettségek.
5. A katasztrófahelyzet kezelésének menete.
6. A katasztrófa utáni helyreállítási intézkedések.
7. A naplózási/nyilvántartási kötelezettségek
8. A katasztrófa szintek meghatározása.

9. A megelőzés szabályainak és alapelveinek meghatározása.
10. A felkészülés szabályainak és alapelveinek meghatározása.
11. A jelzési és riasztási rendszer kialakítása.
12. A katasztrófahelyzet esetén végrehajtandó tevékenységek.
13. A pótlólagos helységek kiválasztása és kijelölése.
14. A katasztrófahelyzetből és a katasztrófa elhárítási folyamatból levont tapasztalatok kezelése.
15. A katasztrófahelyzet kezelési tervben foglaltak tesztelési és felülvizsgálati gyakorisága.

A katasztrófa kezelési tervet csak a földi környezetre kell elkészíteni, tekintettel arra, hogy felhő szolgáltatások (Azure, EATRAC) esetében a katasztrófa kezelés tervét a szolgáltatás ÁSZF-je tartalmazza.

6.2 Biztonsági szintektől független intézkedések és eljárások

6.2.1 Vírusvédelem

A vírusvédelem célja a BM HEROS informatikai rendszerének rosszindulatú/kártékony programok elleni védelmének biztosítása. A védelem kialakítása során jelentkező biztonsági előírások két szinten jelentkeznek (felhasználói és rendszergazdai szinten).

6.2.1.1 Aktív védelem

A vírusvédelmi rendszer fő komponense az aktív (tárrezidens, valósidejű) védelem, mely a számítógép működése során állandóan dolgozik. Feladata a felhasználói munka során igénybe vett állományok (programok, adatok, dokumentumok) közvetlenül a használat előtti vírusellenőrzése. Az aktív védelem kikapcsolása tilos!

Amennyiben a felhasználó a víruskereső program lefuttatása során vírust észlel, fel kell jegyeznie a vírus nevét, a fertőzött file nevét, a számítógépe nevét, és ezeket az adatokat jelenteni kell a HelpDesk (support@securicum.hu) felé, aki gondoskodik a vírus további terjedésének megakadályozásáról, és – amennyiben a felhasználói gépen futó program automatikusan nem törölte – a vírus szakszerű kiirtásáról.

Az aktív védelem a rendszergazda által bármely okból történt kikapcsolása esetén a passzív védelem kiemelt jelentőségű, ezért a rendszergazda felelőssége a vírusvédelem megoldása (akár pl. hálózati kábel kihúzása stb.).

6.2.1.2 Elektronikus levelezés vírusvédelme

Az elektronikus levelezés a vírusok továbbításának leggyorsabb és leggyakoribb módja, ezért erre külön figyelmet kell fordítani.

Ha a levél vagy a csatolt állomány fertőzött, arról a víruskereső szoftver értesíti a felhasználót és a rendszergazdát. Ha az aktív védelem képes volt a fertőzés eltávolítására, akkor – a felhasználó rendszergazdával történő egyeztetése után – a munka megkezdhető. Ha az aktív védelem nem képes a fertőzés eltávolítására, akkor a víruskereső rendszer a fertőzött állományt karanténba helyezi.

Az e-mailben ok nélkül, váratlanul vagy a levél szövegében nem indokoltan érkezett állomány esetében a melléklet tartalmának személyes (pl. telefonos) vagy e-mailben történő ellenőrzése szükséges. Ha a küldő nem szándékosan mellékelt az e-mailhez állományt, akkor semmi esetre sem szabad megnyitni. Ilyen esetben a rendszergazda értesítése szükséges.

6.2.1.3 Passzív védelem (offline ellenőrzés)

A passzív védelem feladata a teljes állományrendszer átvizsgálása, tekintet nélkül az állományok használatba vételére. A víruskereső rendszer frissítése esetén naponta el kell végezni.

A munkaállomásokon a víruskereső programokat úgy kell beállítani, hogy hetente egyszer (az első bejelentkezéskor) megtörténjen az automatikus és kikényszerített vírusteszt futtatása. A tesztek eredményét automatikusan ellenőrizhető logfile(ok)ba kell rögzíteni. A rendszerbe kívülről bekerülő adatokat (akár cd-n, pendrive-on beérkező, akár az Internetről letöltött adatról van szó) felhasználás előtt vírusellenőrzésnek kell alávetni. A víruskereső programok munkaállomásokon történő lefuttatása a felhasználó feladata és felelőssége.

A passzív védelem futása több időt is igénybe vehet, mivel sok állomány ellenőrzését végzi. A víruskeresést megszakítani tilos.

A passzív védelem különösen fontos akkor, ha az aktív védelem valamilyen okból deaktiválta. Az újbóli aktiválásig a passzív védelem használata a felhasználó feladata és felelőssége, aki köteles minden, a rendszerbe bekerülő adat (pl. CD-ROM, Pendrive, e-mail melléklet) ellenőrzését a passzív védelmi rendszerrel azonnal, a felhasználás előtt elvégeztetni.

6.2.1.4 Telepítés

A víruskereső rendszerek konkrét telepítésének megszervezése, a telepítés automatizálása a rendszergazdák feladata, ennek eredményeképpen minden külső adat fogadására alkalmas munkaállomáson rendszeresen frissített vírus-figyelő és törlő programnak kell működnie.

Az újonnan rendszerbe állított, illetve újratelepített számítógépeken gondoskodni kell a víruskereső rendszer azonnali telepítéséről. Megfelelően friss vírusvédelmi rendszer nélkül szervert és munkaállomást üzembe állítani tilos!

Az alkalmazott víruskereső rendszernek képesnek kell lennie, hogy a hálózaton keresztül központosítva felügyelhető változatokat telepítsen. A telepítéskor gondoskodni kell róla, hogy a hálózati adminisztráció során egyértelműen megkülönböztethetők legyenek a különböző gépektől érkező adatok (üzenetek, jelentések, vírusminták, stb.).

A rendszergazda feladata a központosított menedzselés vagy előkészítetlen telepítőkészlet hiányában telepítéskor a szükséges konfiguráció beállítása, illetve lehetőség szerint gondoskodni arról, hogy a felhasználók önhatalmúlag ne csökkenthessék a vírusvédelmi rendszer működésének hatékonyságát.

A központi gépeken és a tűzfalon a vírusvédelem programjait úgy kell installálni, hogy minden file-megnyitás, futtatható file indítása, és file írási műveletet automatikusan ellenőrizzenek. Az ellenőrzés felfüggesztése tilos.

6.2.1.5 Frissítések

A víruskereső rendszerek frissítése két vonalon zajlik: a vírusadatbázisoknak, illetve maguknak a víruskereső motoroknak a frissítése. Általánosan a vírusadatbázisok frissítése lényegesen gyakoribb.

A víruskereső programok frissítéseit (vírusinformációs adatfájlok és motorok) célszerű az Interneten keresztül elvégezni. A hálózat tehermentesítése érdekében frissítést munkaidő utánra kell tervezni.

A víruskereső rendszert fejlesztő cégektől érkező figyelmeztetésekre reagálva indokolt esetben az azonnali kiegészítő vírusadatbázis-frissítés szükséges.

A vírusvédelemmel kapcsolatos valamennyi frissítést (vírus adatbázis, biztonsági frissítések, keresőmotor, stb.) az üzemeltetésért felelős rendszergazda végzi.

6.2.2 Elektronikus levelezés biztonsága

A BM HEROS-nek joga van az e-mail forgalom archiválására és indokolt esetben, vezérigazgatói írásos engedéllyel betekintésre. Az informatikai vezetőnek csak az írásos engedély birtokában van joga elrendelni a felhasználók levelezésébe betekintést engedélyezni kivételes és indokolt esetben. (fegyelmi eljárás, biztonsági incidens) Az eljárást dokumentálni szükséges az indokok, a hozzáférések időpontjának és a megtekintett postafiókok és érintett felhasználók feltüntetésével.

Az elektronikus levelek személyes adatokat is tartalmazhatnak, ezért az e-mail adatbázisok védelmét a személyi adatokra vonatkozó szabályok alapján kell kialakítani.

Az elektronikus levelezésnél tartalomszűrést kell alkalmazni, amely minimálisan a vírus szűrésre ki kell terjedjen.

- Az elektronikus levelezés kialakításának szempontjai:
  - megfelelő felhasználó azonosítás,
  - felhasználónkénti tár méret korlátozás,
  - távoli elérés esetén titkosítás alkalmazása,
  - távoli elérés esetén az egyes csatornák felhasználónkénti korlátozása.

6.2.2.1 Felhasználók feladatai és kötelességei az elektronikus levelezéssel kapcsolatban

- A munkavégzéssel kapcsolatosan már nem használható leveleket rendszeresen el kell távolítani a felhasználók postafiókjából.
- A levelet csak akkor szabad megnyitni, ha a levél megbízható feladótól származik. Nem szabad körültekintés nélkül megnyitni például az idegen nyelven írt, nyereményekre és ismeretlen, megrendelt küldeményekre utaló leveleket, ezeket haladéktalanul törölni kell. Ha a felhasználó bizonytalan a levéllel kapcsolatos teendőt illetően, segítséget a rendszergazdától kérhet.
- A felhasználóknak tilos láncleveleket készíteni és továbbítani. Tilos továbbá más felhasználóktól, illetve külső hálózatról kapott támadó, vagy „szemét" („junk") jellegű, a hálózat túlterhelését célzó e-mailek továbbítása. Az ilyen levelek automatikus kiküszöböléséhez a rendszergazda nyújthat segítséget.
- A tárterületek védelmének érdekében a BM HEROS informatikai rendszerén belül minimalizálni kell a fájlok küldését. Szükség esetén a fájl hozzáférhető módon történő elhelyezése után, a fájlra mutató linket kell elküldeni az elektronikus levélben. Általános szabály, hogy törekedni kell arra, hogy egy fájl, csak egy példányban legyen tárolva a rendszerben.
- A felhasználóknak tilos a BM HEROS nevében olyan e-mailt küldeni, csatolt fájlt megjelentetni elektronikus hirdetőtáblákon vagy egyéb fórumokon, melyek:
  - a BM HEROS, vagy BM HEROS LEK hírnevét, vagy az ügyfelekkel való kapcsolatát ronthatják, illetve a két szervezet ügyfeleinek érdekét sérthetik,
  - törvényt illetve a belső szabályait sértik,
  - szerzői jogokat sérthetnek,
  - vírusokkal fertőzhetnek meg bármely hálózatot.

6.2.3 Internet szolgáltatás szabályozása

A BM HEROS informatikai rendszerét fenyegető veszélyek száma nő az Internetre való kapcsolódással. Az így keletkező veszélyforrások kiküszöbölése a szükséges technikai feltételek megteremtésével és az előírások betartásával lehetséges. Az internet

felhasználása csak a BM HEROS ügymenetének érdekének megfelelően kialakított és betartott szabályok alapján történhet.

A BM HEROS informatikai infrastruktúráját használó munkatársak az Internet elérést szabályozottan, két felhasználói csoportba sorolva használhatják. A felhasználói csoportok közötti váltást a munkatársak szervezeti vezetője kezdeményezheti az informatikai vezetőnél. A szükséges beállításokat a rendszergazdák végzik. Az új felhasználók belépéskor automatikusan alapbeállítással rendelkeznek.

Az internet szolgáltatás minőségének szinten tartása érdekében a rendszergazda az informatikai vezető engedélyével bizonyos korlátozásokkal élhet.

A korlátozások a következőkre térhetnek ki:

- Bizonyos file típusok letöltésének korlátozása,
- Alapvető etikai normákat sértő oldalak látogatásának tiltása,
- Illetve a látogatható web oldalak körének behatárolása és a maximális file letöltési méret korlátozása.

A BM HEROS munkatársai csak az informatikai szervezet által engedélyezett internet kijáratokon keresztül csatlakozhatnak az Internethez. Bármely egyéb módon történő internet elérés létesítése az azt kialakító munkavállaló felelősségre vonását eredményezi.

Az informatikai rendszer biztonsága érdekében az internet felhasználók által meglátogatott oldalak a rendszergazdák által folyamatosan naplózásra kerülnek. A naplók szigorúan titkosak, azokat az adatvédelmi előírásoknak megfelelően kell kezelni.

Felhasználók internet használatára vonatkozó általános szabályok:

- Csak a munkavégzéshez, szakmai tájékozottság bővítéshez információt, segítséget nyújtó oldalak látogathatók.
- Mindig szem előtt kell tartani a BM HEROS és BM HEROS LEK érdekeit és a törvényi s a belső szabályok által szabott határokat.
- A munkatársak nem tölthetnek fel egyénileg a BM HEROS- al kapcsolatos adatot az Internetre.
- Az Internetről csak a munkavégzéshez szükséges adatállományok, táblázatok, programok tölthetők le, a hálózatra csatlakoztatott gépre, vagy a szerverre való telepítés előtt az Internetről letöltött fájlt egyéni vírusellenőrzés alá kell vetni. Amennyiben a felhasználó a vírusellenőrzést nem tudja lefolytatni, köteles értesíteni a rendszergazdát.

6.2.4 Szoftvereszközök használatának szabályozása

Az informatikai biztonság teljes körű megvalósításához hozzájárul a jogtiszta szoftverek és a szoftvereszközök jogszerű használata, valamint szoftverek biztonságos kezelése.

A BM HEROS szoftvereinek nyilvántartása érdekében szoftverleltárt kell létrehozni. A szoftverleltár kialakítását erre a célra szolgáló szoftver és rendszeres szoftver-audit segítségével kell megvalósítani.

A rendszeres szoftver-vizsgálat során ellenőrizni kell:

- a használatban lévő szoftverek rendelkeznek-e licence-el,
- a megvásárolt licencek számának a használt szoftverek mennyiségével arányban kell lenniük,
- a használt szoftverek verziószámát,
- a ténylegesen használt szoftverek megegyeznek-e a szoftverleltárban foglaltakkal.

A szoftver-vizsgálat lebonyolítása az informatikai vezető felelőssége és a rendszergazdák feladata, amit évente egyszer kell elvégezni. A szoftver-vizsgálat eredményei alapján frissíteni kell a szoftverleltárt.

A szoftvereszközök telepítésére és használatára vonatkozó általános szabályok:

- A munkaállomásaira csak eredményesen tesztelt szoftverek telepíthetők. A telepítést minden esetben a rendszergazda végzi.
- Tilos a munkaállomásokra licence-el nem rendelkező szoftvert telepíteni.
- A vásárolt és kifejlesztett szoftverek (és a hozzájuk tartozó dokumentumok) másolása és átadása harmadik félnek tilos, hacsak megfelelő licencszerződés ezt külön nem szabályozza.
- A felhasználók csak a rendszergazdák által telepített szoftvereket használhatják.
- A felhasználók rendelkezésére bocsátott hardver és szoftver eszközök a BM HEROS tulajdonát képezik, amelyek ellenőrzését az informatikai vezető bejelentés nélkül bármikor kezdeményezheti.

6.2.4.1 Tűzfalakkal kapcsolatos szabályozások

A tűzfalak biztonsági beállításainak meg kell felelniük az alábbi elvárásoknak és a feladatok elvégzését biztosítani kell:

- A tűzfal rendszer naplóinak elemzése (napi szinten).
- A tűzfalak beállításainak és naplóállományainak mentése (naponta).
- A beállított szabályok működésének tesztelése.
- A tűzfalak szabályainak felülvizsgálata, (éves szintű felülvizsgálat minimálisan javasolt).
- A tűzfal rendszer kialakításának felülvizsgálata (minimum évente, illetve az infrastruktúrában történt fejlesztések alkalmával javasolt elvégezni).
- Meg kell határozni a normál működéstől eltérő események, hibák kezelésének felelősségeit, eljárásait, annak érdekében, hogy a visszaállás a leggyorsabban végrehajtható legyen.
- A tűzfal rendszerrel kapcsolatosan dokumentálni kell az alábbiakat:
  - a tűzfalon felismerhető biztonsági incidenseket, azok megszüntetésére tett intézkedéseket,
  - működési incidenseket, azok megszüntetésére tett intézkedéseket,
  - a tűzfalak frissítéseinek (biztonsági frissítések, verziófrissítések) végrehajtását.

6.2.5 Távoli hozzáférés, wireless kapcsolat szabályozása

A BM HEROS informatikai rendszerének távoli elérését csak és kizárólag az egyedi engedélyezési eljáráson átesett authentikáció, illetve a szerződésben meghatározott feltételekkel külső személyek (a rendszerjavításához, karbantartáshoz) használhatják a rendszerek besorolásának függvényében.

A távoli hozzáférés kialakítása kétféle technikai megoldási módot használva lehetséges.

1. WebMail szolgáltatás – OWA elérésen keresztül

2. VPN kapcsolat

   Az Interneten keresztül felépített VPN kapcsolatnál az IP- alapú kommunikáció titkosított adatcsatorna kialakításán keresztül zajlik.

Mindegyik kapcsolat kialakítása esetén a rendszer beállításai által gondoskodni kell az egyértelmű felhasználói azonosításról és authentikációról, a naplózásról, illetve a kapcsolatok megfelelő tűzfalas védelméről.

6.2.6 Mobil IT tevékenység, hordozható informatikai eszközök

A laptopok, táblagépek használatával kapcsolatban a következő biztonsági paraméterek betartása kötelező:

- A BM HEROS tulajdonát képező hordozható személyi számítógépeket a telephelyek területén kívül csak az arra felhatalmazott személyek használhatják.
- A mobil eszközök átvételéhez átadás-átvételi dokumentumokat kell készíteni.
- Valamennyi a BM HEROS tulajdonát képező hordozható személyi számítógépet rendszeres szoftver-, adat- és biztonsági ellenőrzéseknek kell alávetni.

A személyi számítógépeket és az ahhoz kapcsolódó számítástechnikai berendezéseket szállító személyek:

- Kötelesek a számítógépet a szállítás idejére lehetőleg minél kevésbé szem előtt lévő módon elhelyezni.
- Tilos a számítógépet a gépjárműben hagyni.
- Repülés, vagy vonatút alatt a személyi számítógépet kézipoggyászként kell szállítani.
- Azokban az esetekben, amikor az eszközöket nem a szervezet tulajdonában lévő telephelyeken (szálloda, lakás) kell hagyni, fokozott figyelmet kell szentelni a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása, vagy ellopása elleni védelemnek.
- Tilos az engedély nélküli átruházása vagy adatainak közlése.
- Megfelelő védelem nélkül idegen hálózathoz csatlakozni.
- Tilos a gépet bármilyen indokolatlan veszélynek kitenni vagy nem rendeltetésszerűen használni.

A BM HEROS titkos adataiból csak azon adatokat szabad hordozható személyi számítógépen tárolni

- Mely adatokról központi biztonsági mentés készül.
- Biztosítani lehet a törvényileg, jogszabályilag, belső szabályzattal előírt adatbiztonságot és adatvédelmet.
- A hordozható eszközön is megoldott a titkosított tárolás lehetősége.

A mobil eszközök biztonsági beállításait illetve háttértárolóinak tartalmát rendszergazdáknak legalább negyedévenként ellenőriznie kell. Az ellenőrzés során fokozott figyelmet kell szentelni a következőknek:

- Az adott eszközön a biztonsági beállítások, vírusvédelmi és egyéb biztonsági eszközök beállításai megfelelnek-e az előírtaknak.

- Az állományok lokális tárolására vonatkozó szabályok betartásra kerülnek-e.
- Az eszközön fellelhető naplóállományokban nincs-e nyoma rendellenes műveleteknek, jogosulatlan használatnak.

6.2.7 Papír alapú dokumentumokat előállító hálózati eszközök kezelése

A dokumentumok előállítására alkalmas eszközök (nyomtató, plotter, fax) használatára az egyéb informatikai eszközökre vonatkozó szabályozások érvényesek. A felhasználók számára tiltott tevékenységek a BM HEROS adatait nyomtatott formában megjelenítő eszközök esetén is hatályosak.

A BS7799 szabvány által előírt felhasználói felelősségek iratok esetén érvényesek.

- Őrizetlenül hagyott felhasználói információk és dokumentumok.
- Tiszta-asztal politika.

7 Informatikai rendszerek fejlesztése és karbantartása

7.1 Az informatikai rendszerek fejlesztése és karbantartása

A BM HEROS informatikai rendszereinek továbbfejlesztését, módosítását, valamint új alkalmazások fejlesztését a külső törvényi elvárásokhoz és BM HEROS elvárásaihoz igazítva kell elvégezni.

Az informatikai rendszerek fejlesztésének első lépéseként a szakmai oldal elvárásai alapján el kell készíteni a rendszerspecifikációs dokumentumot, amelynek elkészítése során a jogszabályi és az informatikai biztonsági elvárásoknak történő megfelelést is figyelembe kell venni.

Az informatikai biztonság megőrzése érdekében ki kell dolgozni a rendszerspecifikációra vonatkozó biztonsági követelményrendszert. A követelményrendszer kidolgozásának végrehajtása az informatikai vezető felelőssége és a kapcsolódó fejlesztési projekt vezetőjének feladata. A követelményrendszert az alaprendszerbe való illesztéséből adódóan egyeztetni szükséges a rendszergazdákkal.

A követelményrendszer elkészítése során figyelembe kell venni:

- A fejlesztendő rendszer bemenő adatait, annak adatvédelmi és adatbiztonsági besorolási szintjeit.
- A rendszer elvárt rendelkezésre állási idejét.
- A rendszer azon elemeit, ahol hozzáférési jogosultságok kialakítása szükséges.
- A rendszer gyenge, betörésre alkalmat adó pontjait.
- Mentési rendbe való illesztését.

7.1.1 Alkalmazásfejlesztés

7.1.1.1 Szakmai követelmények összeállítása

Szakmai követelmények megfogalmazását követően az alkalmazásfejlesztést igénylő terület feladata az igényléskor benyújtott fejlesztési igény jelzése a szakmai követelmények pontos meghatározásával. A szakmai követelményeket leíró dokumentum elkészítése az igénylő szervezeti egység vezetőjének (illetve az általa kinevezett munkatársnak) a felelőssége.

Szakmai követelményeket tartalmazó dokumentumnak kötelező adattartalma:

- Az igényelt fejlesztéssel szemben elvárt funkcionalitás ismertetése.
- A fejlesztésre vonatkozó (környezeti) korlátok bemutatása.
- A rendszerrel szemben támasztott szakmai követelmények.
- Biztonsági követelmények.
- Felhasználói követelmények.

- Üzemeltetési követelmények.
- Infrastrukturális követelmények.

7.1.1.2 Informatikai követelmények összeállítása

Ezek meghatározása után - a fejlesztéssel szemben támasztott felhasználói követelmények ismeretében - a fejlesztési feladat precíz specifikálása az alábbiak alapján lehetséges:

- A fejlesztési igény alapos megismerése, elemeinek, tevékenységeinek folyamatainak feltárása,
- A rendszer elemeinek, működésének leírása, elemzése,
- Az információs rendszer részletes feltárása, megismerése,
- Az információáramlás és feldolgozás elemzése,
- Az alkalmazni kívánt ki- és beviteli eszközök, módszerek meghatározása,
- A szükséges képernyő és nyomtatási formátumok, ki- és beviteli mezők meghatározása,
- A rendszerben tárolt adatok típusainak, formátumának, mérethatárainak meghatározása.

Ezen feladatok elvégzése a fejlesztést igénylő szervezeti egység vezetőjének felelőssége. Az informatikai fejlesztési feladatnak az előző pontban meghatározottakon túl tartalmaznia kell a következőket is:

- A fejlesztés hardver szükséglete,
- A fejlesztés szoftver követelményei,
- Dokumentációk adattartalmával és felépítésével kapcsolatos elvárások,
- Szükséges erőforrások bemutatása,
- Fejlesztési projekt ütemezése,
- A fejlesztés életciklusának meghatározása,
- Rendszertervek adattartalmával és felépítésével kapcsolatos elvárások.

7.1.1.3 Dokumentációkészítés

A fejlesztett rendszerhez kapcsolódó dokumentációk elkészítése az adott projekt vezetőjének a felelőssége, külső fejlesztés esetén a külső vállalkozónak a feladata. Az informatikai vezető csak abban az esetben veheti át üzemeltetésre a fejlesztett rendszert, ha a dokumentáció a következőket tartalmazza:

- Műszaki leírás, amely tartalmazza a teljes rendszer felépítésére, működésére vonatkozó műszaki specifikációkat.
- Az Implementációs tervet, valamint a Teszt tervet is, amely részletesen leírja az átállás lépéseit, körülményeit, biztonsági követelményeit, szükséges erőforrásokat.
- Üzemeltetési leírás, amelyek tartalmazzák a rendszer üzemeltetésére vonatkozó eljárásokat, rendszerindítás, - leállítás, biztonsági intézkedések,

napi tevékenységek pontos leírását, továbbá mentés/visszaállítási leírás, katasztrófa elhárítási tervet, amely tartalmazza az adott rendszerre vonatkozó speciális feladatokat, igényeket.

- Beállítási terv/leírás, amely a rendszer jogosultsági és egyéb beállításainak az átadás-átvételkori állapotát tartalmazza.
- Felhasználói leírás, amely tartalmazza a felhasználók számára a rendszer rendeltetésszerű használatára vonatkozó használati utasításokat.
- Oktatási anyag, amely tartalmazza a felhasználói és üzemeltetői feladatokhoz kapcsolódó oktatási anyagot, valamint a javasolt oktatási tervet.

7.1.1.4 Teszt

A projektterv alapján elkészült fejlesztési feladat üzemeltetésre való átadás feltétele egy átfogó teszt végrehajtása, amit két fázisban kell megvalósítani. Rendszerteszt során a rendszer üzemszerű működését, működtethetőségét, a felhasználói teszt során pedig a fejlesztési igényben megfogalmazott elvárások minőségi teljesülését kell vizsgálat alá venni. A tesztelési módszertannak javasolt követnie az ISO9126 és az ISO12207 alkalmazásfejlesztéssel és teszteléssel összefüggő (6.4 Verification) fejezeteit.

1. Rendszerteszt

A jóváhagyott Műszaki leírásban szereplő teszt terv alapján a szükséges teszteket el kell végezni. A teszteknek az alábbi területeket kell érintenie:

- Integrációs teszt
- Teljesítmény teszt
- Terhelési teszt
- Katasztrófa teszt

A tervben meghatározott feladatok elvégzéséről Teszt jegyzőkönyvet kell készíteni, amelyet a projektvezetőnek és az informatikai vezetőnek kell jóváhagynia. A tesztek végrehajtását, a kötelező dokumentumok adattartalmát a fejlesztéshez kapcsolódó Projekttervben kell definiálni.

2. Felhasználói teszt

Teszt végrehajtását a Műszaki leírásban szereplő felhasználói teszt-terv alapján kiválasztott felhasználónak kell elvégezni, és az elvégzett feladatokat dokumentálniuk kell a terv mellékleteként csatolt Felhasználói teszt jegyzőkönyvben.

7.1.1.5 Üzembe helyezés

1. Próbaüzem

A teljes rendszer sikeres tesztje után a rendszert próbaüzembe kell állítani, amelynek keretén belül az igénylők megkezdik a rendszer rendeltetésszerű használatát. A próbaüzem során feltárt hibák kijavításáig és a sikeres elfogadási tesztig, de legalább 1 hónapig tart. Az elfogadási tesztről jegyzőkönyvet (Elfogadási teszt jegyzőkönyv) kell készíteni és eljuttatni az informatikai vezetőhöz jóváhagyásra.

2. Éles üzem indítása

Igazolt próbaüzem után megtörténhet az Implementációs terv alapján az éles üzemre való átállás.

3. Átadás az üzemeltetésnek

A projekt során átadott eszközökről, alkalmazásokról, dokumentációkról Átadás-átvételi jegyzőkönyvet kell készíteni, és átadni az üzemeltetés képviselőjének. A feladatok elvégzése Teljesítési igazolás aláírásával kerül dokumentálásra.

7.2 Vásárolt és fejlesztett programokra vonatkozó előírások

A vásárolt és fejlesztett programok esetében figyelembe kell venni a szerzői jogra vonatkozó hatályos törvényi szabályozásokat. A tulajdonjogokat a licencszerződések szabályozzák.

Biztonsági előírások a vásárolt és fejlesztett programokkal kapcsolatban:

- A BM HEROS által vásárolt, vagy számára kifejlesztett szoftverek (és a hozzájuk tartozó dokumentumok) másolása és átadása harmadik félnek - ha a licencszerződés ezt nem teszi lehetővé – szigorúan tilos.
- Felhasználók/programozók, - az arra illetékes vezető jóváhagyása nélkül - nem készíthetnek olyan alkalmazásokat, programokat, melyek a szervezet létfontosságú adatbázisait igénybe veszik, ahhoz kapcsolódnak.

8 Ellenőrzések, rendszeres felülvizsgálatok

Az informatikai biztonság szinten tartása érdekében megfelelő kontrollokat kell kialakítani. A kontrollok kialakításánál elsődlegesen azt kell figyelembe venni, hogy azok által az információbiztonság szintje mérhető legyen.

Ennek érdekében meg kell határozni az ellenőrzések területeit, és minden területhez külön-külön meg kell fogalmazni az ellenőrzési célkitűzéseket. Az ellenőrzési célkitűzések ismeretében meg kell jelölni az ellenőrzés eszközeit (dokumentumok, naplók, szoftverek, adatok, amelyek a biztonsági rendszerről hiteles képet tudnak adni), azok tartalmi követelményeit.

Az ellenőrzés eredményét minden esetben ki kell értékelni, és a megfelelő következtetéseket le kell vonni, illetve vissza kell csatolni a biztonsági folyamatra. Szükség esetén felelősségre vonási eljárást kell kezdeményezni.

Az ellenőrzéseket dokumentumok, dokumentációk, személyes beszámoltatás és helyszíni szemlék alapján lehet végrehajtani.

Az informatikai biztonsággal kapcsolatos ellenőrzések területei az alábbiak lehetnek:

- Megfelelőségi vizsgálat. Célja felderíteni, hogy a BM HEROS rendelkezik-e a törvényi előírásokban meghatározott személyi, eljárási, tárgyi feltételekkel, és azok megfelelően dokumentáltak-e.
- Az információ biztonság szintjére vonatkozó vizsgálat. Célja felderíteni, hogy az információ biztonság szintje megfelel-e a meghatározott védelmi szintnek.
- Az információ biztonsági szabályok betartásának ellenőrzése. Célja felderíteni, hogy a BM HEROS információ biztonsági szabályait az illetékes személyek ismerik-e, illetve betartják-e. Ez az ellenőrzés az informatikai biztonság egy-egy területére is leszűkíthető.
- A biztonsági dokumentumrendszer felülvizsgálata. Célja a BM HEROS belső szabályzatrendszerét képező hatályos eljárások felülvizsgálata, hogy megfelelnek-e az elvárt jogi, informatikai, szakmai elvárásoknak és az általuk szabályozott területen megfelelő szabályok betartására alkalmazhatóak.

Az ellenőrzések során elsősorban az alábbiakat kell vizsgálni:

- Az IT biztonsági rendszer működése megfelel-e a törvényi előírásoknak.
- Az IT biztonsági rendszer felépítése, tartalma megfelel-e az ISO27001/BS 7799-2 szabványnak.
- Az IT biztonsági szabályok érvényesítve vannak-e a folyamatokban.

- Az IT biztonsági rendszer előírt dokumentumai léteznek-e, illetve naprakészek-e.
- Az IT személyzet, illetve a felhasználók rendelkeznek-e a megfelelő IT biztonsági ismeretekkel.
- Az adatokra és rendszerekre vonatkozó kezelési szabályok betartását.
- A naplózási rendszer megfelelő alkalmazását. A biztonsági események kezelésének, a szükséges mértékű felelősségre vonás gyakorlatát.
- A mentési rendszer megfelelő alkalmazását.
- Az informatikai rendszert fejlesztők, üzemeltetők, és felhasználók információ biztonsággal kapcsolatos ismereteit.
- A hozzáférési jogosultságok nyilvántartásának naprakészségét, a kiadott jogosultságok szükségességét.
- A dokumentációk pontosságát - naprakészségét, változás követését, megfelelő kezelését / nyilvántartását.
- Az alkalmazott szoftverek jogtisztaságát.
- A szerződések megfelelőségét.
- A fizikai biztonsági előírások betartását.

8.1 Biztonsági rendszerek felülvizsgálata

Az IT biztonsági rendszer, illetve annak egyes elemeit rendszeresen felül kell vizsgálni. A szükséges felülvizsgálatok az alábbiak:

A felülvizsgálat tárgya	A felülvizsgálat ciklikussága
Megfelelőségi vizsgálat	2 évente
Az információ biztonság szintjére vonatkozó vizsgálat	1 évente
Az információ biztonsági szabályok betartásának ellenőrzése	2 évente
A biztonsági dokumentumrendszer felülvizsgálata	1 évente