BVK HOLDING

11/2012. számú

VEZÉRIGAZGATÓI UTASÍTÁS

BVK HOLDING BUDAPESTI VÁROSÜZEMELTETÉSI KÖZPONT ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG

Informatikai Biztonsági Szabályzata

az informatikai rendszerekben kezelt adatok bizalmasságát, hitelességét, sértetlenségét, rendelkezésre állását és funkcionalitását fenyegető veszélyekkel szemben érvényesített védelmi intézkedések társasági szintű-, általános szabályozása kötelezettségének teljesítéséről

Szakmai előkészítő:	Jóváhagyta:
Egri Zoltán BVK HOLDING Zrt. IT igazgató	Szarvas Ferenc BVK HOLDING Zrt. vezérigazgató

Hatályos: 2012. október 10. napjától	Utolsó módosítás:

11/2012. számú

VEZÉRIGAZGATÓI UTASÍTÁS

BVK HOLDING BUDAPESTI VÁROSÜZEMELTETÉSI KÖZPONT ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG

Informatikai Biztonsági Szabályzata

az informatikai rendszerekben kezelt adatok bizalmasságát, hitelességét, sértetlenségét, rendelkezésre állását és funkcionalitását fenyegető veszélyekkel szemben érvényesített védelmi intézkedések társasági szintű-, általános szabályozása kötelezettségének teljesítéséről

Tartalom

11/2012. számú

VEZÉRIGAZGATÓI UTASÍTÁS

BVK HOLDING BUDAPESTI VÁROSÜZEMELTETÉSI KÖZPONT ZÁRTKÖRŰEN MŰKÖDŐ RÉSZVÉNYTÁRSASÁG

Informatikai Biztonsági Szabályzata

az informatikai rendszerekben kezelt adatok bizalmasságát, hitelességét, sértetlenségét, rendelkezésre állását és funkcionalitását fenyegető veszélyekkel szemben érvényesített védelmi intézkedések társasági szintű-, általános szabályozása kötelezettségének teljesítéséről

I. Általános rendelkezések

1. Az Informatikai Biztonsági Szabályzat kiadásának célja és hatálya

1.1. Az IBSz kiadásának célja

a) BVK Holding Zrt. cég-stratégiája- és feladatai- megvalósulásának elősegítése
b) A BVK Holding Zrt. által üzemeltetett informatikai rendszerekben kezelt adatok bizalmasságát, hitelességét, sértetlenségét, rendelkezésre állását és funkcionalitását fenyegető veszélyekkel szemben érvényesített védelmi intézkedések társasági szintű-, általános szabályozása
c) Egységes elvek, keretszabályok és értelmezések megadása a BVK Holding Zrt. informatikai rendszerek fejlesztői-, üzemeltetői- és felhasználói számára biztonsági tevékenységük összehangolásához
d) Egységes szerkezet és irányelvek megadása az új alkalmazás/rendszer szintű szabályozások elkészítéséhez illetve a korábbiak felülvizsgálatához

A keretszabályozás jelleg a BVK Holding Zrt. tulajdonában lévő, illetve az általa üzemeltett informatikai rendszerekre vonatkozóan kiterjed:

- azok teljes életciklusára (az előkészítés, a megvalósítás, az üzemeltetés és a rendszerből történő kivonás fázisaira)
- az egyes informatikai rendszerek és környezetük minden elemére (legyenek azok akár informatikai, akár egyéb szervezeti természetűek)
- az egyes informatikai rendszerek infrastruktúrájára és alkalmazási szintjeire
- a központi és a munkahelyi (számítástechnikai) erőforrásokra

1.2. Az IBSz hatálya

Az IBSz személyi hatálya

Az IBSz személyi hatálya kiterjed:

a) A BVK Holding Zrt. valamennyi munkavállalójára.
b) A BVK Holding Zrt. informatikai rendszereivel, szolgáltatásaival szerződéses, vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban: külső személy) a velük kötött szerződésben rögzített mértékben, illetve a titoktartási nyilatkozatuk alapján.
c) A BVK Holding Zrt. Igazgatóságának és Felügyelő Bizottságának tagjaira

Az IBSz tárgyi hatálya

Az IBSz tárgyi hatálya kiterjed:

A BVK Holding Zrt. tulajdonában lévő vagy az általa üzemeltetett valamennyi meglévő és a jövőben fejlesztendő informatikai rendszerére, illetve azok környezetét alkotó rendszerelemekre, azok teljes életciklusában (az előkészítéstől a rendszerből történő kivonásig).

Az IBSz szintjei

A könnyebb kezelhetőség és áttekintés érdekében az IBSz-t két szinten kell megvalósítani. Az általános és a mindenkire érvényes szabályokat a jelen társasági szintű IBSz részeként, míg az egyes rendszerekre nézve specifikus szabályokat az illető rendszer/alkalmazás alárendelt biztonsági szabályzatában vagy szabályzataiban.

Társasági szintű IBSz:

1) A BVK Holding Zrt. minden szervezeti egységére általános érvényű, amely:
   - rögzíti a Zrt. informatikai rendszereinek és rendszer környezeteinek biztonsági alapelveit;
   - meghatározza a BVK Holding Zrt.-nél használt (számítástechnikai) eszközök (és alkalmazott adathordozók) kezelésének általános szabályait,
   - tartalmazza az egyedileg kezelendő alkalmazások védelmi rendszereinek kidolgozásánál figyelembe veendő irányelveket.
2) A jogszabályokkal összhangban – illeszkedve a BVK Holding Zrt. egyéb működési, ügyrendi előírásaihoz – meghatározza a biztonsági eljárásokat, a felelősöket, az ellenőrzések rendjét és az esetleges szabálysértések jogkövetkezményeire vonatkozó alapelveket.
3) Kitér a fejlesztés, beszerzés, karbantartás és üzemeltetés általános biztonsági szabályaira. Rögzíti az informatikai rendszerek fejlesztése területén a biztonsági rendszerek tervezésére, megvalósítására, tesztelésére, bevezetésére, követésére és a minőségbiztosítására vonatkozó általános szabályokat, foglalkozik a vírusvédelem, a hálózatok, a külső hozzáférések, az üzletmenet-folytonosság, a változásmenedzsment, a biztonságmenedzsment és az ellenőrzések általános szabályaival.
4) Részletezi az IT rendszerek fejlesztésében, beszerzésével, karbantartásával és üzemeltetésével érintett belső és külső szervezetek (felhasználók, partnerek, szállítók,

szolgáltatók) együttműködésének szervezésével, kezelésével, kiszolgálásával kapcsolatos biztonsági szabályokat, különös tekintettel az un. outsource szervezésmóddal összefüggő állami előírásokra.

Rendszerszintű IBSz:

A rendszerszintű szabályozások a társasági IBSz elveit követik, az abban szereplő előírásokat bontják le az adott rendszerhez kapcsolódóan. Konkrét, a szabályozott területre érvényes és értelmezhető szabályokat adnak. Megnevezik az egyes feladatok végrehajtásában kompetens beosztásokat, szervezeteket (felelős, irányító, végrehajtó, ellenőrző stb.).

Az alárendelt szabályzatoktól nem azt követeljük meg, hogy magukat „biztonságinak" nevezzék, hanem azt, hogy kövessék a társasági szintű IBSz tartalmi előírásait.

A rendszerszintű IBSz-eket az adott témával foglalkozó szabályzatok összessége jelenti.

A rendszerszintű szabályozásokat minden nagyobb alkalmazásra, a számítóközpont(ok)ra és a számítástechnikai infrastruktúra minden jelentős szegmensére külön kell kialakítani. A részletező szabályozások tartalma természetesen függ a szabályozott alkalmazástól-, hálózattól-, számítóközponttól, stb. is. A nem értelmezhető fejezeteket el lehet hagyni, és ha szükséges, újakat kell kidolgozni.

Ha a szabályozott rendszer vagy a BVK Holding Zrt. rendszerintegrációs kötöttsége megköveteli, akkor egyes részkérdésekben a társasági IBSz-nek alárendelt szabályozások akár ellent is mondhatnak ezen keretszabályzatnak. Ilyen esetben azonban előírjuk az illető szabály kivételességének egyértelmű megjelölését és az eltérés pontos indoklását.

A korábban kidolgozott rendszer szintű biztonsági szabályozásokat felül kell vizsgálni és ahol szükséges a társasági szintű IBSz egységes követelményei szerint ki kell egészíteni.

1) A társasági IBSz előírásait követve, az abban szereplő szabályokat bontja le az adott rendszerhez kapcsolódó, konkrét, a szabályozás hatálya alá tartozó területre érvényes és értelmezhető szabályokra, megnevezve az egyes feladatok végrehajtásában kompetens szervezeteket, beosztásokat, személyeket és elérési paramétereiket.
2) A rendszerszintű IBSz-ekben a IBSz által megfogalmazott szabályokat az adott rendszerre, területre nézve részletes szabályokkal kell kifejezésre juttatni. A részletes szabályok kialakítása függ az egyes informatikai rendszerek jellegétől. Az elkészített rendszerszintű IBSz-ek, mint a technikai feladatokat részletesen meghatározó szabályzatok – jóváhagyás után – az érintett alkalmazások, illetve területek számára kerülnek kiadásra, és az adott területen jelen IBSz-el együtt érvényesek.

2. Fogalmak és meghatározások

Bizalmasság

Az adat (és az adathordozó) azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak a jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

Hitelesség

Az adat (és az adathordozó) tulajdonsága, amely arra vonatkozik, hogy az adat bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik és megfelel a rá előírt összes alaki és tartalmi követelménynek.

Információ-védelem

Az informatikai rendszerekben kezelt adatok által képviselt tartalom (emberi értelmezés=információ) bizalmasságának, hitelességének és sérthetetlenségének védelme.

Informatikai biztonság, IT biztonság

Az informatikai biztonság a védelmi rendszer olyan, a BVK Holding Zrt. számára kielégítő állapota, amely az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Kockázattal arányos védelem

A kockázatokkal arányos a védelem, ha egy kellően nagy idő-intervallumban a védelem költségei arányosak a potenciális kárértékkel.

Legkevesebb jog (least privilege)

Alapelv, amely szerint minden szubjektumnak azokat a minimális előjogokat kell adni, amelyekre az engedélyezett programok futtatásához szüksége van. Ezen alapelv használata csökkenti a baleset, hiba vagy egy információs rendszer illetéktelen használata miatt bekövetkező adatsérülést/veszteséget

Megbízható működés

Megbízható a működés, ha az illető informatikai rendszer(ek) és az általuk kezelt adatok folyamatosan rendelkezésre áll(nak) és funkcionalitása(suk) önmagával azonos marad.

Rendelkezésre állás

Az informatikai rendszerelem – ideértve az adatot is – azon tulajdonsága, amely arra vonatkozik, hogy az informatikai rendszerelem a szükséges időben és időtartamra használható.

Sértetlenség

Az adat tulajdonsága, amely arra vonatkozik, hogy az adat fizikailag és logikailag teljes.

Teljes körű védelem

Teljes körű a védelem, ha az illető informatikai rendszer összes elemére kiterjed.

Zárt védelem

Zárt a védelem, ha az összes releváns fenyegetést figyelembe veszi.

3. A szabályozók felülvizsgálata és fejlesztése

A társasági szintű informatikai biztonságpolitika, valamint a jelen IBSz rendszeres áttekintése, karbantartása és szükséges fejlesztésnek a BVK Holding Zrt. vezetése elé terjesztése az IT igazgató feladata.

Az eredeti szabályozás alapjait érintő minden változás (új kockázatok, új káresemények, új veszélyhelyzetek, a szervezeti és a műszaki infrastruktúra átalakítása) esetén soron kívüli új vizsgálatra, elemzésre van szükség.

Rendszeresen át kell tekinteni:

a) Az irányelvek biztonsági hatékonyságát zártság és teljesség szempontjából – (vagyis minden lényeges kockázatot, minden védeni való rendszerelemet meghatároztunk-e, és csak azokat határoztuk-e meg?).
b) Az ellenőrző és a biztonsági eszközök, eljárások érvényességét költséghatékonysági szempontból (kockázat arányossági illetve folytonossági felülvizsgálat).
c) A technológiai váltások hatását (érvényesek-e a régi kijelentések az új körülmények között).

4. Szervezeti biztonság – biztonsági szervezet

4.1. Az informatikai biztonság szervezeti struktúrája

A szervezeti/informatikai biztonság – törvényekben és más jogszabályokban, a Zrt. szerződéseiben és megállapodásaiban, valamint szabályzataiban leírt – megszervezéséért, megvalósításáért és ellenőrzéséért valamennyi szervezeti egység vezetője, kiemelten a Vezérigazgató felelős.

Biztonsági fórum

A biztonsági fórum feladatát a BVK Holding Zrt. Vezetői Értekezlet (VÉ) tölti be.

A Vezetői Értekezlet hatáskörébe tartozik az informatikai biztonság területén:

a) Az informatikai biztonsági irányelvek és feladatok vizsgálata, jóváhagyása.
b) Az (információs) erőforrások súlyos veszélyhelyzeteknek való kitettségében bekövetkező jelentős változásainak nyomon követése.
c) Az informatikai biztonsági események nyomon követése.
d) Az informatikai biztonsági rendszer átalakítását/átszervezését szolgáló jelentős kezdeményezések jóváhagyása.

Az informatikai biztonsági feladatok megosztása

IT biztonsági megbízott

a) Gondoskodik a biztonságra és ezen belül az informatikai biztonságra vonatkozó jogszabályok és jelen Szabályzat végrehajtásáról, e körben szabályozási koncepciókat, szabályzat tervezeteket készít, a BVK Holding Zrt. szervezeti egységeinek megkeresésére vagy saját hatáskörben szakmai állásfoglalásokat ad ki.
b) Az informatikai biztonság szempontjából véleményezi a BVK Holding Zrt. szabályzatait.
c) Az informatikai biztonságot érintő jogszabály változások és a gyakorlati tapasztalatok alapján javaslatokat készít a BVK Holding Zrt. szabályzatainak módosításra, kezdeményezi új szabályzatok kibocsátását.
d) Gondoskodik az informatikai biztonságra vonatkozó rendelkezések betartásának éves ellenőrzéséről, a lefolytatott ellenőrzések, vizsgálatok eredményéről tájékoztatja a Vezetői Értekezletet
e) Irányítja és ellenőrzi a cég informatikai biztonsági szervezetének munkáját.
f) Jelentési kötelezettsége a Vezérigazgató felé van.
g) Felméri és elemzi a BVK Holding Zrt. működéséből eredő az adat- és az információvédelemmel összefüggő veszélyforrásokat, elvégzi ezek osztályozását.
h) Felméri és elemzi a BVK Holding Zrt. informatikai rendszereiben kezelt adat és eszköz vagyont fenyegető kockázatokat, elvégzi az adat és eszközvagyon informatikai biztonsági osztályozását, javaslatokat tesz a védelmi szintekre, közreműködik ezen védelmi szintek tartalmi megvalósításában, felügyeli, jelenti működésüket.
i) Kidolgozza és döntésre előterjeszti az informatikai biztonság kialakítására, a megfelelő informatikai biztonság elérésére, illetve fenntartására vonatkozó szabályokat, utasításokat, terveket és irányelveket.
j) Részt vesz:
   a. a rendkívüli események kezelésére szolgáló tervek elkészítésében. azok naprakészen tartásában,

b. az Informatikai biztonság szempontjából fontosnak minősített munkakörök betöltési szabályainak, feltételeinek meghatározásában,
c. a biztonsági követelmények és az előírások betartásának ellenőrzésében,

k) Szakmai szempontból, közvetlenül irányítja a BVK Holding Zrt.-nél használt informatikai rendszerek védelmét.
l) Szakmai szempontból irányítja az Informatikai biztonságra vonatkozó oktatást.
m) Szakmai szempontból egyezteti és véleményezi a rendszerszintű IBSz-ek tervezetét.
n) Elemzéseket végez, szükség esetén javaslatokat tesz a megfelelő adat- és információvédelmi intézkedésekre, valamint a biztonságos működéssel összefüggő szabályok megváltoztatására.
o) Ellenőrzi az adat- és információvédelmi előírások végrehajtását.
p) Végzi az informatikai rendszerek információvédelmében vállalkozóként résztvevő gazdasági társaságok szakmai irányítását, ellenőrzi tevékenységüket.

Jogosult:

a) A vizsgálati tevékenysége során, a BVK Holding Zrt. tulajdonában, használatában vagy a területén lévő, illetve a BVK Holding Zrt.-re vonatkozó bármilyen iratba, dokumentumba, okmányba, adatbázisba, számítógépes vagy más adathordozó tartalmába való betekintésre.
b) A BVK Holding Zrt. tulajdonában lévő, vagy általa bérelt épületben és azon belül minden – a BVK Holding Zrt. tulajdonában, kezelésében vagy használatában lévő – helyiségben a berendezések, különösen az informatikai eszközök vizsgálatára.

4.2. Az adatfeldolgozás engedélyezési eljárásai

a) Az adatfeldolgozás csak akkor engedélyezhető, ha az – legalább – az adatkörök biztonsági osztályba sorolásának (ld. 5. pont) megfelelő adatfeldolgozó eszközökön történik – ideértve az összeférhetetlenséggel kapcsolatos szabályozások megtartását is.
b) Az új adatfeldolgozási eszközökre és lehetőségekre vonatkozó engedélyezési eljárásban a következő biztonsági megszorításokat kell figyelembe venni:
   1) az informatikai rendszerért felelős vezető új adatfeldolgozási eszközökre és lehetőségekre vonatkozó jóváhagyását csak abban az esetben adhatja meg, ha azok megfelelnek a kiszolgált alkalmazások védelmi osztályának, az arra előírt biztonsági feltételeknek.
   2) ellenőrzéssel kell meggyőződni a hardver, szoftver eszközök és más rendszer összetevők kompatibilitásáról,
   3) a minősített adatokat feldolgozó rendszer használata az IT Igazgató engedélyéhez kötött,
   4) a minősített adatokat feldolgozó rendszerek használatát a rendszerfelelős vezetőjének a IT Igazgatóval egyeztetve szabályoznia kell.

4.3. Informatikai biztonsági tanácsadás

A BVK Holding Zrt. szervezetei részére informatikai biztonsági szakértői támogatást az IT Igazgató ad. Amennyiben erőforrásai nem elegendőek, vagy a feladat speciális jellege nem teszi azt lehetővé az IT Igazgató részt vesz a külső szakértő kiválasztásában, a szerződéskötésben, illetve az eredmények átvételében.

4.4. Együttműködés külső szervezetekkel

Az együttműködés során korlátozni kell a biztonsággal kapcsolatos információk kicserélését, megelőzendő, hogy a BVK Holding Zrt. bizalmas információi illetéktelen kezekbe kerülhessenek.

4.5. Az informatikai biztonság független vizsgálata

a) Az informatikai biztonság megvalósulását független szakérőnek kell értékelnie. Ez lehet a belső ellenőrzés, vagy ilyen vizsgálatokra szakosodott független külső szervezet.
b) Az informatikai biztonságpolitikában, valamint az IBSz-ekben rögzítettek megvalósulását – a Szervezeti és Működési Szabályzatban előírt általános feladatkörének és az összeférhetetlenségi szabályoknak megfelelően Az IT Igazgató ellenőrzi. Ez az általános ellenőrzési jogkör nem mentesíti a szervezeti egységek vezetőit annak felelőssége alól, hogy az informatikai biztonság meglétét a beosztottaik munkavégzésének folyamatos vizsgálata során ellenőrizzék, megállapítsák.

4.6. Előírások a külső személyek által történő hozzáférésekkel kapcsolatban

a) A BVK Holding Zrt. külső személyek számára is hozzáférhető informatikai rendszerei és eszközei biztonságának fenntartása érdekében a hozzáféréseket minden esetben ellenőrizni kell. Az ellenőrzésért a BVK Holding Zrt. részéről a felelős kapcsolattartóként meghatározott szervezeti egysége vezetője – amennyiben a szerződésben nem került feltüntetésre, úgy – a szerződést kötő szervezet vezetője, illetve az általa kijelölt személy a felelős.
b) A biztonsági kockázatokat és az ellenőrzés, valamint a felügyelet követelményeit fel kell mérni. A felmérésért a szerződést – üzletági oldalról – előkészítő személy a felelős. A külső személlyel megkötött szerződésben egyértelműen meg kell határozni az előzőekhez kapcsolódó elvárásokat.
c) Külső személyek hozzáférésénél további résztvevők közreműködésére is szükség lehet. A hozzáféréséről rendelkező szerződésekben rendelkezni kell arról, hogy más, arra jogosult közreműködők is hozzáférhetnek a különböző eszközökhöz, és rögzíteni kell a hozzáférés feltételeit.
d) Jelen szabályzat betartása az ilyen szerződések létrejöttének, valamint az adatfeldolgozás vállalkozásba adásának elengedhetetlen feltétele.

4.7. A külső személyek által végrehajtott hozzáférések kockázatai

A hozzáférések típusai

A külső személyek BVK Holding Zrt. IT rendszerei felé irányuló hozzáféréseinek különleges jelentősége van. A következő hozzáférési típusokat kell elkülöníteni:

a) Fizikai hozzáférések (pl. irodákhoz, számítógéptermekhez, irattároló szekrényekhez, stb.), az ezekre vonatkozó előírásokat részletesen – a szerződéskötéshez előírt előzetes felülvizsgálat során– az IT Igazgató szabályozza.
b) Logikai hozzáférések (pl. adatbázisokhoz, informatikai rendszerekhez, kommunikációs eszközökhöz, stb.), az ezekre vonatkozó előírásokat részletesen – a szerződéskötéshez előírt előzetes felülvizsgálat során – az IT Igazgató szabályozza.

A hozzáférések engedélyezési feltételei

a) Amennyiben külső személyeknek ideiglenes hozzáférési lehetőséget kell biztosítani, ezt csak és kizárólag engedélyeztetési eljárás után lehet megtenni. A hozzáférési engedélyt minden esetben csak a szolgáltatást igénybe vevő BVK Holding Zrt. szervezeti egység vezetője kérheti, mellékelve az esetleg *fedezetlenül maradó biztonsági résekkel, nem érvényesülő szabályozásokkal kapcsolatban kiállított és jóváhagyott* Kockázat Vállalási Űrlapokat. Az IT Igazgató a titokvédelmi előírások figyelembevételével dönt az engedély megadásáról. A hozzáférést mindaddig meg kell akadályozni, amíg a szükséges ellenőrzéseket nem folytatták le, amíg felismert, de fedezetlenül hagyott kockázati elem maradt illetve szerződésben nem határozták meg a hozzáférés feltételeit.

b) A visszavonás illetve a lejárat időpontjának minden esetben szerepelni kell a hozzáférési engedélyben.

c) A BVK Holding Zrt. azon külső személyeknek, akik a Zrt.-nek szolgáltatásokat nyújtanak, tevékenységük végzéséhez munkafeltételként meghatározott és engedélyezett fizikai és/vagy logikai hozzáféréseket biztosít. Ilyen lehet:
   1) a hardver- és/vagy a szoftvertámogató személyzet, akiknek rendszerszintű vagy alacsony logikai szintű alkalmazás hozzáféréssel kell rendelkeznie
   2) kereskedelmi partnerek vagy közös vállalkozások, akik üzleti érdekből – esetleg szolgáltatásként – adat ellátásban részesülnek, információcserében vesznek részt, informatikai rendszerekhez vagy adatbázis részekhez hozzáférhetnek,
   3) alkalmazás szállítók/támogatók, akiknek hozzáférésük lehet az általuk támogatott rendszerekhez. **Ez a hozzáférés kizárólag a támogatott rendszer teszt környezetére irányulhat**, kizárva az érvényes üzleti tranzakció végrehajtásának lehetőségét. Üzleti érdekből és az alkalmazás felhasználójának és/vagy adat-tulajdonosának írásbeli Kockázat Vállalási engedélye alapján ideiglenes/alkalmi hozzáférési engedély adható az éles rendszerkörnyezetekhez is. Az éles rendszerkörnyezetekben biztosított hozzáférési engedélyek felhasználását tranzakciónként dokumentáltan ellenőrizni kell. Az ellenőrzés és a dokumentálás végrehajtásáért az alkalmazásszállító/szolgáltató BVK Holding Zrt. kapcsolattartója – amennyiben a szerződésben ilyen nem került feltüntetésre, úgy – a szerződést kötő szervezet vezetője, illetve az általa kijelölt személy a felelős.

d) Ahol az üzleti érdek megkívánja a külső személyekkel való kapcsolattartást, a közvetlen hozzáférést jelentő munka megkezdése előtt egyértelműen meg kell határozni a munkavégzés célját, helyét, idejét, módját, fel kell mérni az alkalmazás biztonsági kockázatait, a szükséges hozzáférések típusait, a veszélyeztetett adatok, információk értékét, a külső személlyel és tevékenységével kapcsolatban alkalmazni kívánt ellenőrzési- módokat, elemeket. Követelmény a külső személy azonosítására használt eljárások folyamatos ellenőrzése is.

e) A külső partnerek hordozható számítógépein tárolt – a munkavégzés során megszerzett és a BVK Holding Zrt.-vel kapcsolatos – adatokat a munkavégzés befejezése után visszaállíthatatlanul törölni kell. A törlés megtörténtét a kapcsolattartásért felelős személynek ellenőriznie és dokumentálnia kell.

f) A BVK Holding Zrt. érdekeinek védelmére a megkötött alvállalkozói/megbízási szerződéseknek tartalmaznia kell egy titoktartásra vonatkozó pontot, melyben ki kell térni a jelen szabályzat 1.sz. mellékletében foglaltakra, vagy a szerződéskötéskor a jelen szabályzat 1.sz. mellékletét kell a szerződés egy mellékleteként aláíratni az alvállalkozókkal.

Helyszíni munkát végző külső vállalkozók

Szerződéses vagy egyéb jogviszony alapján helyszíni munkát végző harmadik (külső) személyek a biztonság gyengülését okozhatják. Ennek megelőzése érdekében:

a) A harmadik személlyel kötött szerződésekben ki kell kötni a BVK Holding Zrt. ellenőrzési jogosultságát.
b) A harmadik személlyel szemben érvényesítendő informatikai biztonsági követelmények (a rendszerszintű IBSz-ekben előírt módon) egyértelműen rendelkezzenek az ilyen személyek hozzáférési lehetőségeiről.
c) Az informatikai rendszerekhez, az abban kezelt adatokhoz harmadik személyek hozzáférését mindaddig ki kell zárni, amíg a megfelelő (és szerződésben is rögzített) ellenőrzést nem folytatták le.
d) A harmadik személyek helyszíni tevékenységének informatikai biztonsági ellenőrzése során a munkahelyi vezetőnek és az Biztonsági Megbízottnak együtt kell működnie.
e) Még a munka megkezdése előtt kötelező megvizsgálni a harmadik személyek várható helyszíni munkafolyamatát.

Informatikai biztonsági követelmények a harmadik személlyel kötött szerződésekben

a) Harmadik (külső) személyeknek a BVK Holding Zrt. informatikai rendszereihez való hozzáférése kizárólag olyan írásbeli szerződésen alapulhat, melynek az összes – biztonsággal kapcsolatos – előírása igazodik a Zrt. biztonsági előírásaihoz és elfogadott szabványaihoz.
b) Harmadik személyek számára – a velük kötött szerződésben részletezettek szerint – az adathozzáférés elektronikus-, papíralapú-, mágneses-, vagy bármely más típusú adathordozón történő adat/vezérlés transzfer esetén csak az elért adat/rendszer minősítéséhez, kezeléséhez és az informatikai rendszer biztonsági osztályba besorolása szerinti engedélyezési eljárással és dokumentáltan történhet, az adott szerződés elválaszthatatlan mellékletét/részét képező adatvédelmi és titoktartási nyilatkozatok tartalmának megfelelően.
c) A b) pontban felsoroltak alól kivételt képeznek az informatikai biztonsággal kapcsolatos kötelező eseti és rendszeres adatszolgáltatások, továbbá bíróságok, hatóságok hatósági eljárásai során, illetve a hivatalból eljáró ügyvéd, közjegyző eljárásai. Ezekről minden esetben értesíteni kell Az IT Igazgatóat.
d) A számítógépek által papíralapú adathordozóra nyomtatott adatok átadás-átvétele csak az adat- és titokvédelemre vonatkozó szabályzatokban meghatározott – a minősített iratok kezelésére vonatkozó – előírások szerint történhet.
e) Amennyiben valamilyen veszély elhárítására külső szervezet igénybevétele válik szükségessé, úgy a megkötendő szerződésben a munkavédelem szempontjaira is ki kell térni.

4.8. Vállalkozásba adás, kiszervezés

a) A vállalkozásba adás minden esetben csak írásbeli szerződéssel lehetséges, amelyben a jelen szabályzat irányelveit kell figyelembe venni.
b) Vállalkozásba adás esetén az érintett informatikai rendszereket, hálózatokat, környezeteket, az azokat érintő kockázatokat, valamint az alkalmazott biztonsági eszközöket és eljárásokat, felelősségeket a két fél között létrejött szerződésben rögzíteni kell.

Előírások vállalkozásba adási szerződésekben

a) Amennyiben a vállalkozó a saját telephelyén végzi az informatikai fejlesztési tevékenységet, a BVK Holding Zrt. részéről csak rejtjelezve továbbíthatók a fejlesztés tárgyát képező programok és adatok a fejlesztő számára. Az éles üzemű rendszerekhez a vállalkozó nem férhet hozzá.

b) Programokat, adatokat kizárólag átadás-átvételi jegyzőkönyv alapján szabad átadni. Az átadás során – jogai védelmében – a vállalkozó köteles gondoskodni az átadás tárgyát képező fájlok sértetlenségét garantáló rendszabályokról és a rendszabályok közös ellenőrzését garantáló eszközökről. A jegyzőkönyvnek minimálisan tartalmazni kell a következő adatokat:

1) programátadás esetén:
   - program megnevezése,
   - készítője,
   - funkciója,
   - könyvtárstruktúrája,
   - fájlok és verziószámaik (opcionálisan ellenőrző összegeik);

2) fájlátadás esetén:
   - teljes fájlnév (név, kiterjesztés),
   - méret,
   - módosítás dátuma,
   - verzió információ.

3) adatátadás esetén:
   - ha az adat nem tartozik a fájl fogalmába, akkor a papíralapú iratkezelésre vonatkozó szabályok az irányadók.

c) Az a) pont szerinti anyagokat tartalmazó adathordozókat a következő lényeges szabályok szerint kell kezelni:

1) az adathordozók azonosíthatók, ellenőrizhetők legyenek, a minősítési és az azonosítási jeleket vagy jelöléseket olvashatóan, letörölhetetlenül, levehetetlenül kell feltüntetni,

2) a harmadik személy az 1) bekezdésben felsorolt minősítésekkel, jelölésekkel kapcsolatos kezelési szabályokat a teljes munkafolyamat során köteles betartani, ellenkező esetben a teljesítése nem fogadható el. Az adathordozók csak a BVK Holding Zrt. biztonsági (pl. vírus) ellenőrzéseinek elvégzése után vehetők használatba a BVK Holding Zrt. rendszerein.

d) Külső fejlesztő részére tesztelésre éles üzemi adatok nem adhatók át, ezen felül üzemi tesztek csak a BVK Holding Zrt. saját teszt környezeteiben végezhetők. Teszt környezetben csak olyan tevékenységek folytathatók, amelyek bizonyíthatóan nem eredményeznek érvényes üzleti tranzakciót.

e) Ezen szabályok betartásának, a szabályok szerinti tevékenység dokumentálásának ellenőrzésére a BVK Holding Zrt. részéről felelősként, kapcsolattartóként meghatározott szervezeti egysége és Az IT Igazgató vagy az általa megbízott munkatársak jogosultak, illetve kötelezettek.

f) Amennyiben a vállalkozásba vevő a saját telephelyén működő fejlesztő rendszeren dolgozik, akkor a következő főbb biztonsági szabályok az irányadók:

1) a tevékenységet a fogadó szervezet folyamatosan felügyelje, dokumentálja és ellenőrizze szerződéses alapon vállalva jelen informatikai Biztonsági szabályzat betartását,

2) belépési és hozzáférési jogosultságot az általános jogosultsági szinten túlmenően csak külön engedély alapján, a tevékenysége elvégzéséhez szükséges időre kapjon,
3) távoli hozzáférésekkel történő fejlesztés csak indokolt esetben folyhat (pl., amikor az előző pontokban meghatározott fejlesztési mód alapos indok miatt nem valósíthatná meg),
4) távoli hozzáféréssel történő fejlesztés, az érintett szakmai vezető kezdeményezésére, a felhasználó és/vagy adattulajdonos Kockázatvállalási Nyilatkozata alapján az IT Igazgató által kiállított előzetes írásbeli engedélyével történhet.: Az erre irányuló javaslatot a fejlesztő és megrendelője köteles megindokolni.
5) Fejlesztési céllal távoli hozzáférés csak az engedélyben definiált végpontról és csak a BVK Holding Zrt. ellenőrzése alatt álló védelmi rendszerrel megtámogatva történhet.

5. Az eszközök biztonsági besorolása és ellenőrzése

5.1. Számadási kötelezettségek az eszközökkel kapcsolatban

a) Meg kell határozni a leltárilag nyilvántartott eszközök gazdáit – akit fizikai eszközök esetén a Tárgyi Eszköznyilvántartás, míg licence jogok esetén (szoftver eszközök esetén) a Szoftver Licence nyilvántartás „Tároló hely" megjelölése alapján kell megállapitani. Az eszközök mindenkori felelőse az eszköz gazdája.
b) Megfelelő személyekhez – eszközhasználóhoz – kell rendelni szükséges ellenőrző eszközök fenntartásának feladatát és felelősségét.
c) Az eszközhasználók (munka)szerződésében/munkaköri leírásában kell rögzíteni a hw-sw készletgazdálkodással kapcsolatos tevékenységüket illetve a felelősségüket.
d) Az eszközhasználók szolgálatba lépésekor átadás-átvételi jegyzéket kell felvenni a használatba adott eszközökről (amelyet később Ők folyamatosan karbantartanak). A jegyzék aláírásakor elfogadottá kell tenni a használó eszközökre vonatkozó számadási kötelezettségét, valamint ennek megsértésével járó felelősségre vonás módját, mértékét.
e) Számadási kötelezettségek ellenőrzését az Eszközgazdálkodási illetve a Szoftver Licence gazdálkodási szabályzatok előírásai alapján kell végrehajtani (leltári ellenőrzések alkalmával kiegészítve a Leltári szabályzat rendelkezéseivel).
f) Ellenőrzést kell tartani:
   1) az eszközhasználó szolgálati viszonyának megszűntekor – az általa leadott eszközöket össze kell vetni az illető saját- valamint a gazdálkodók aktuális eszköz kimutatásaival. Megfelelés esetén igazolást kell kiadni a számadási kötelezettségének teljesítéséről, eltérés esetén pedig jegyzőkönyvet kell felvenni. Egyidejűleg értesítve az eszköz használó vezetőjét az eszköz hiánnyal/többlettel összefüggő felelősség megállapítása érdekében.
   2) az eszközhasználó más szervezeti egységbe, más munkakörbe való áthelyezésekor – az előző pontban részletezettek megtartásával,
   3) ha okafogyottá válik az eszköz(ök) használata és használója leadja azt – leadás esetén is ellenőrizni kell a nyilvántartásukkal való egyezést,
   4) vezetői elrendelésre (cél- vagy átfogó leltár).

5.2. Az adatok biztonsági osztályozása

a) Az informatikai eszközök kockázat arányos védelméről való gondoskodás magában foglalja, hogy az adatok minősítésének tükröznie kell a védelem szükségességét, prioritásait és mértékét.
b) Az adatok érzékenysége és fontosságának mértéke változó, egyes adatok fokozott védelmet, vagy különleges kezelést igényelnek. A számítástechnikai rendszerek, illetve adatok biztonsági osztályba sorolására vonatkozó előírások segítségével kell meghatározni a védettségi szinteket, valamint közvetíteni kell a különleges kezelés szükségességét.
c) A BVK Holding Zrt. kezelésében lévő összes informatikai rendszert – a felhasználói és adattulajdonosi szándékkal/elvárással összhangban – már a tervezés folyamán információ védelmi, illetve ha a megbízhatóság mérése is elvárás, akkor biztonsági osztályba kell sorolni.

5.2.1. Az osztályozás irányelvei

A BVK Holding Zrt. minden informatikai rendszerét az adatok bizalmassága, hitelessége, sértetlensége, illetve elvesztésével arányos kárérték szintektől függően, informatikai biztonsági osztályokba kell besorolni.

5.2.2. Az adatok minősítése, címkézése és kezelése

A minősítő rendszer eljárásainak ki kell terjedniük a tárgyi és elektronikus információs eszközökre. Meg kell határozni az adatfeldolgozás egyes tevékenységeinél alkalmazható – az adat minősítésétől függő – adatkezelési eljárásokat az alábbi tevékenységekre:

a) adat előállítás
b) adat felvitel
c) másolás
d) tárolás
e) archiválás (biztonsági, illetve üzemszerű)
f) átvitel
g) megsemmisítés

A fokozott vagy a kiemelt biztonsági osztályba sorolt adatokat tartalmazó alkalmazások kimeneti adatait a kimeneten megfelelő címkével kell jelölni. A címkézésnek a hivatkozott biztonsági osztályoknak megfelelően tükröznie kell az adat minősítését és annak időbeli hatályát.

Egyes adattárolási formáknál (elektronikus eszközökön tárolt adatok) a fizikai címkézés nem használható, ezért ezekben az esetekben a címkézés elektronikus eszközeit kell alkalmazni.

6. Személyi követelmények

6.1. Informatikai biztonság a felvételnél és a munkaköri leírásokban

Az emberi hibák, a szándékos kártétel, a lopás, a csalárd magatartás vagy a létesítmények és eszközök nem megfelelő használata olyan személyi kockázatok, amelyek kikerülhetetlenek és amelyeket cégérdekből egységesen és törvényes keretek között kezelni kell, a következők szem előtt tartásával:

a) A biztonsági követelményeket a munkaerő kiválasztás során, szerződéskötéskor, valamint az egyén foglalkoztatása során egyaránt érvényesíteni kell.
b) A munkaerő-felvételi eljárás során – törvényes keretek között – olyan vizsgálatokat kell lefolytatni, melyek kiértékelhető képet adnak a jelölt alkalmazásának informatikai kockázatairól, szakmai-, emberi alkalmasságáról. Az alkalmasság vizsgálat különösen fontos kiemelt informatikai munkakörök betöltésekor. Minden munkavállalónak, a rendszerek külső használóinak (a velük kötött szerződés alapján), alá kell írniuk egy Titoktartási és Adatvédelmi nyilatkozatot.
c) A munkavállalótól csak olyan nyilatkozat megtétele vagy olyan adatlap kitöltése kérhető, illetve vele szemben csak olyan alkalmassági vizsgálat alkalmazható, amely a személyiségi jogait nem sérti, a munkaviszony szempontjából lényeges tájékoztatást nyújthat és ahhoz az érintett írásban hozzájárult.

6.1.1. Informatikai biztonsági követelmények érvényesítése a munkaköri leírásokban:

a) Valamennyi munkaterületre részletes munkaköri leírást kell készíteni. A munkaköri leírásnak tartalmaznia kell az adott munkaterületre vonatkozó, a biztonsággal kapcsolatos követelményeket is.
b) A betöltendő funkciókat úgy kell meghatározni, hogy azok teljes terjedelmükben hozzárendelhetők legyenek a munkakörökhöz és ezáltal el lehessen azokat határolni egymástól, hogy minden munkavállaló csak a szigorúan rá vonatkozó feladatot hajtsa végre.
c) Az informatikai biztonság szempontjából elengedhetetlen a személyügy (HR) és az IT Igazgató folyamatos kommunikációja:
    1) A felhasználó beléptető rendszerbeli jogosultság igénylő / karbantartó lapját a betépő munkavállaló szervezeti vezetője (vagy a HR) tölti ki és Az IT Igazgató veszi nyilvántartásba.
    2) A felhasználó kiléptető lap a munkavállaló kilépési folyamatának része kell, hogy legyen. A nyomtatvány azt a célt szolgátja, hogy a távozó munkavállalónak az informatikai rendszert érintő valamennyi jogosultsága garantáltan, és dokumentáltan letiltásra kerüljön.
d) Minden munkaterületre ki kell dolgozni a konkrét feladatokat amelyeket a területen dolgozók ellátnak és vele együtt az erőforrás szükségletet és az erőforrás használathoz szükséges jogosultságokat (esetleg tiltásokat vagy más szabályozókat), hogy ezeket a munkavállaló megismerhesse és a biztonsági szervezet ellenőrizhesse.

6.1.2. A személyzet biztonsági átvilágítása és a személyzeti politika

A személyzeti politikát a humánerőforrás menedzsment készíti el a biztonsági szegmensek figyelembe vételével. A személyzet biztonsági átvilágításáról külön szabályzatban kell részletesen intézkedni.

Titoktartási és adatvédelmi nyilatkozatok

A titoktartási és adatvédelmi nyilatkozatról a szervezet sajátosságának megfelelő Titokvédelmi Szabályzatban kell részletesen intézkedni.

A foglalkoztatás feltételei

A foglalkoztatás alapvető biztonsági feltételei az általános és a munkakörre vonatkozó speciális biztonsági előírások megismerése, elfogadása, a titoktartási és adatvédelmi nyilatkozat aláírással történő elfogadása.

6.2. Felhasználói képzés

a) A felhasználóknak ismerniük kell a biztonsági eljárások alkalmazását és az adatfeldolgozó lehetőségek korrekt használatát, hogy ezzel is a minimálisra csökkentsék a lehetséges biztonsági kockázatokat.
b) A felhasználói oktatás a biztonsági elképzeléseket is figyelembe vevő Képzési Terven alapul.
c) A Zrt. vezetésének – az IBSz elveinek, valamint a saját hatáskörben meghatározott képzési elveknek megfelelően – a humánerőforrás menedzsmenttel, illetve Az IT Igazgatóval egyeztetve ki kell dolgoznia a Képzési Tervet.

6.2.1. Informatikai biztonsági oktatás és képzés

A cég minden dolgozójának igény szerint rendszeresen, de minimum kétévente részt kell vennie IT biztonsági oktatáson.

6.3. Biztonsági és üzemzavarok kezelése

a) Mérsékelni kell a biztonságot befolyásoló események és működési zavarok következményeit; nyomon kell követni az eseményeket; biztosítani kell a mielőbbi normális üzemre való visszaállást és a tapasztalatokat írásban kell megfogalmazni.
b) Mindazon biztonsági eseményeket, amelyek a folyamatos éles üzemet megzavarják, a napi feldolgozást hátráltatják, azonnal jelenteni kell a feldolgozásért felelős illetékeseknek.
c) Minden munkavállalónak és vállalkozónak ismernie kell a szervezet működésének és az általa használt eszközök használatának biztonságát befolyásoló különböző események (biztonsági előírások megsértése, veszélyek, hiányosságok vagy működési zavarok) jelentésének eljárási szabályait. Az munkavállalóknak e szabályzat elvei ill. az alkalmazás/rendszer szintű IBSz-ekben részletezett helyen és módon kell jelenteniük az észlelt eseményeket. Az események biztonságos kezeléséhez szükség van arra, hogy a történést követően nyomban összegyűjtsék a meglévő bizonyítékokat.

d) Ha az IT Igazgató a logok elemzése közben biztonsági problémát tapasztal, köteles azt emailben jelenteni és a rendelkezésre álló bizonyítékokat átadni a rendszerért felelős területnek/területeknek.

6.3.1. Biztonsági események jelentése

A munkavállaló az általa észlelt eseményeket a szervezeti egysége vezetőjének és az IT Igazgatónak köteles jelenteni, valamint köteles mindent megtenni a szükséges bizonyítékok összegyűjtésére. Az IT Igazgató és a szervezeti egység vezetője jelentéseiket haladéktalanul kötelesek megtenni a cégvezetés felé. Az IT Igazgató az eseményt a lehető legrövidebb idő alatt kivizsgálja, és amennyiben a felelősségre vonás szükségessége fennáll, értesíti a munkáltatói jogkört gyakorló Vezérigazgatót, aki mérlegelve a munkavállaló kötelezettségszegésének mértékét fegyelmi és/vagy bírósági eljárást kezdeményezhet.

6.3.2. Az események tapasztalatainak elemzése és értékelése

a) Az eseményeket
   1) típus,
   2) terjedelem,
   3) általuk okozott károk értéke valamint a helyreállítási költségek,
   4) a jogosultság ellenőrző és monitoring rendszer működési zavara
   szerint értékelni kell.
b) Az elemzés alapján – szükség esetén – kezdeményezni kell a biztonsági irányelvek felülvizsgálatát, a szabályzatok korszerűsítését.

6.3.3. Felelősség vizsgálata

a) A biztonsággal összefüggő munkavállalói kötelességek megszegésének gyanúja esetén a felelősségi vizsgálat megindítása a munkavállaló közvetlen vezetőjének felelőssége, és egyben kötelessége. Az eljárás tényleges megindításáról a munkahelyi vezető és az IT Igazgató valamint HR Igazgató javaslatainak mérlegelésével a Vezérigazgató dönt.
b) A felelősségi, kártérítési eljárást a Munka Törvénykönyve és a Munkavállaló munka szerződése szerint kell lebonyolítani.

7. Fizikai és környezeti biztonság

A fizikai és környezeti biztonság megteremtése, illetve fenntartása érdekében a vonatkozó jogszabályok, biztonsági és tűzvédelmi szabványok, valamint a helyi szabályzatok rendelkezések előírásainak maradéktalanul meg kell felelni. A betartatásukért felelősek: SZMSZ által meghatározott vezetők.

7.1. Biztonsági szegmensek

a) Az illetéktelen hozzáférés, a károkozás és az üzleti helyiségekbe való behatolás, valamint az adatok jogtalan elérésének megakadályozása érdekében a lehetséges kockázatokat fel kell mérni és ennek megfelelően biztonsági területeket kell kijelölni.
b) A kritikus vagy érzékeny üzleti adatokat feldolgozó és tároló egységeket, szervezeteket, létesítményeket meghatározott biztonsági sávval védett, biztonsági korlátokkal és áthaladást ellenőrző pontokkal ellátott területeken (a továbbiakban: biztonsági területek) kell elhelyezni. Gondoskodni kell az illetéktelen behatolást, hozzáférést, károkozást és beavatkozást megakadályozó fizikai, mechanikai, elektronikai és személyi védelem szükséges mértékű együttes alkalmazásáról.
c) A védelemnek arányban kell állnia a megállapított kockázatokkal. Az illetéktelen hozzáférés megakadályozása, a dokumentumok, az adathordozók védelme és az

adatfeldolgozó létesítmények kockázatának mérséklése érdekében szükség van megfelelő beléptetési és megfigyelési szabályok érvényesítésére.

7.1.1. A beléptetés fizikai eszközei

a) A biztonsági területekre és az egyes biztonsági zónákba való belépést, beléptetést ellenőrizni kell.
b) A biztonsági területekre, illetve az egyes biztonsági zónákba állandó belépési jogosultsággal nem rendelkező munkatársak
   1. Fokozott zóna esetén: csak az adott biztonsági zónáért felelős személy engedélyével léphetnek be.
   2. Kiemelt zóna esetén: csak az adott biztonsági zónáért felelős személy vagy az általa meghatalmazott személy jelenlétében léphetnek be.
c) Külső személyek csak kísérettel tartózkodhatnak a BVK Holding Zrt. külön védelemmel felszerelt zónáiban, szegmenseiben.

7.1.2. A kiszolgáló területek és raktárak biztonsági elkülönítése

A központi erőforrások (szerverek, hálózati berendezések), központi adatfeldolgozó (rögzítő) és adattároló helyiségekbe, valamint a raktárakba csak az ott dolgozók részére biztosítható állandó belépési lehetőség. Ezekbe a helyiségekbe oda nem beosztott személy csak felügyelet mellett léphet be, illetve tartózkodhat.

7.2. A berendezések fizikai védelme

Az informatikai berendezéseket, eszközöket fizikai valójukban is aktívan védeni kell a biztonságot fenyegető veszélyektől és a káros környezeti hatásoktól. Függetlenül attól, hogy passzív védelmük (pl. Biztosítás) szintje milyen.

A műszaki eszközök fizikai védelmére azért van szükség, hogy ily módon is mérsékeljük az adatokhoz való illetéktelen hozzáférés kockázatát, valamint gondoskodjunk az adatok és eszközök megfelelő védelméről. Erre már a berendezések elhelyezése során is tekintettel kell lenni. A veszélyek és az illetéktelen hozzáférés elhárításához, illetve a kiszolgáló létesítmények védelméhez különleges eszközökre, többek között áramszolgáltató és kábelrendező infrastruktúrára is szükség van.

a) **Az informatikai rendszerek védelmének – a rendszer megbízható működésbeli biztonsági osztályának megfelelően – ki kell terjednie:**
   1) az extrém hőmérsékletek és a meg nem engedett mértékű levegő nedvességtartalom elleni védelemre (klimatizálás),
   2) a fémes adatvezetékek elektromágneses impulzusok elleni védelmére (elektromágneses ki/besugárzás elleni védelem),
   3) külső tényezők (tűz, víz, vihar, stb.) elleni védelemre, így különösen a tűzjelző berendezések meglétére és működőképességére, illetve a vízelvezetésre,
   4) áramellátó-rendszerek kiesése következményeinek elhárítására (akkumulátoros és generátoros szükség-áramellátással),
   5) az áramellátás területén a villámcsapások elsődleges és másodlagos hatásai, illetve egyéb túlfeszültségek elleni védelemre,
   6) elektrosztatikus kisülések hatásainak elhárítására (a helyiségek és munkahelyek megfelelő kialakításával, amelyekbe az informatikai rendszereket telepítették).

Mindehhez a következő követelményeket kell érvényesíteni:

b) Az információvédelem területén

1) Alapbiztonsági osztályban:

- A központi hardver erőforrások, az azokon üzemeltett alkalmazások és kezelt adatok információvédelmének és megbízható működésének biztosításában nagy szerepet játszik azoknak a helyiségeknek (pl. szerverszobák) a védelme, amelyekben ezek az erőforrások üzemelnek. Az üzemi helyiségek a védelemnek az adatok feldolgozását, tárolását, a hálózat működését biztosító berendezések védelmén túl ki kell térnie a tárolt szoftverek, adatok és dokumentációk védelmére is. A védelemnek az alkalmazások rendelkezésre állásának szükséges mértékével, a hardver és a szoftver beszerzési értékével, az adatok pótlásának költségével kell arányban lennie. Tekintettel ezek fajlagosan magas árára, a védelem teljes körű és mindenre kiterjedő kell, hogy legyen. Az üzemi helyiségek teljes körű védeleméről már a helyiségek kialakítása során gondoskodni kell. A védelem egyaránt terjedjen ki az élőerős, a mechanikai (építészeti) védelemre és a technikai (elektronikai) védelemre. A biztonsági követelményeket az egész építményre vonatkozó összefüggések figyelembevételével (elhelyezés, falazatok, födémek, nyílászárók, zárak, kerítés, megvilágítás, belső közlekedő terek, közös, illetve kiegészítő helyiségek, stb.) kell meghatározni és érvényre juttatni.
- Az építmény egyes helyiségeire vonatkozó biztonsági előírás eltérhet – annál szigorúbb lehet – az építmény egészére megfogalmazott biztonság mértékétől. Ilyen helyiségek a távbeszélő hálózat hozzáférési pontjai, a számítógéptermek, a pénztárak, az ügykezelés helyiségei, ügyeleti szolgálatok. A mechanikai védelemnél, a falazatok, a nyílászárók, zárak biztonsági kialakításánál a vonatkozó építészeti szabványok, a MABISZ és a Rendőrség ajánlásai szerint kell eljárni.
- Az objektumok őrzés-védelmét, nyitását és zárását, a be- és kilépést mind munkaidőben, mind azon kívül a hatályban lévő szabályzatok és az érvényes előírások alapján biztosítani és érvényesíteni kell.
- Az olyan hivatali helyiségeket, ahol számítástechnikai eszközökkel történik a munkavégzés, biztonsági zárral kell ellátni, és a helyiséget távollét esetén zárva kell tartani.
- Biztosítani kell az adathordozók és dokumentációk tűz- és vagyonvédett tárolását.

2) Fokozott biztonsági osztályban az előzőeken túl:

- A területen 12 órás áthidalást biztosító szünetmentességgel ellátott olyan elektronikai jelzőrendszert kell kiépíteni, amellyel biztosítható a teljes felület és a részleges térvédelem.
- A személyzet és a külső személyek belépési és azonosítási rendjét szabályozott formában kell megvalósítani.
- Az őr- és a biztonsági személyzet létszámát úgy kell megállapítani és olyan eszközökkel kell ellátni, hogy esemény esetén az érintett személy jelezni tudjon.

3) Kiemelt biztonsági osztályban az előzőeken túl:

- A mechanikai védelem védjen a közforgalmú területről történő betekintés ellen is. Az elektronikai védelem terjedjen ki a számítás-technikai eszközökre, valamint a felügyelet nélküli helyiségekre is.
- A személyzet és a külső személyek belépési és azonosítási rendjét szabályozott formában, intelligens beléptető-rendszerrel kell megvalósítani, amely a mindkét irányú áthaladásokat naplózza és biztosítja az azonosító eszköz azonos irányban történő többszöri felhasználásának tilalmát.

- A helyiségbe (épületbe) belépni szándékozókat azonosítani kell, és a belépőkről nyilvántartást kell vezetni.

c) A megbízható működés területén:

1) Alap biztonsági osztályban:
   - Az infrastruktúra fizikai védelme egyaránt szolgálja az informatikai rendszerben az információvédelem és a megbízható működés biztosítását. Az előző pontban meghatározottakon kívül a védelem terjedjen ki a tűz, valamint a villámcsapások által indukált és a hálózatingadozások miatti túlfeszültségek elleni védelemre is.
   - A tűz elleni védelmet elsődlegesen személyi felügyelet, valamint a jelenlévő személyzet biztosítja a helyiségen belül készenlétben tartott, a tűzvédelmi előírásoknak megfelelő, kézi tűzoltó készülékekkel. A készenléti helyeken elsődlegesen gáz halmazállapotú oltóanyaggal feltöltött tűzoltó készülékek legyenek. A készülékek típusát és darabszámát, illetve elhelyezését a helyi tűzvédelmi utasításnak kell tartalmaznia. A készülékeket a helyiségeken belül a bejárat mellett, valamint a helyiség erre alkalmas, jól megközelíthető pontjain kell elhelyezni. A helyiségben a vonatkozó szabványok előírásainak megfelelő tűzjelző rendszert kell kiépíteni és üzemeltetni.
   - Az elektromos hálózat elégítse ki az MSZ 1600 sorozatú szabványok előírásait, az érintésvédelem feleljen meg az MSZ 172 sorozatú szabványok előírásainak.
   - A megbízható működés szempontjából lényeges követelmény, hogy az elektromos hálózatot a szünetmenetességre, az áthidalási és újratöltési időre vonatkozó követelményeknek megfelelően kell kialakítani és külön leágazás megépítésével kell a betáplálásról gondoskodni. Ha egy nem szerverszobának kijelölt hivatali helyiségben szerver üzemel, gondoskodni kell lokális szünetmentes tápáramellátásáról.
   - A villámvédelem feleljen meg a kommunális és lakóépületekre vonatkozó előírásoknak.
   - Az átlagostól eltérő klimatikus viszonyú (pl. a hőmérséklet, illetve a páratartalom értéke túllépi a számítástechnikai eszközökre vonatkozó megengedett tartományt) helyiségekben lokális klimatizálásról kell gondoskodni.

2) Fokozott biztonsági osztályban az előzőeken túl:
   - Fizikailag az informatikai rendszernek a megbízható működés szempontjából kritikus részeit kell elsősorban védeni. A mai rendszertechnikai megoldásokból kiindulva ez elsősorban a számítóközpontok, a szerverszobák, és az egyéb "központi" jellegű informatikai helyiségek (de nem az irodák!) védelmét jelentik.
   - A helyiségbe csak annak üzemeltetéséhez elengedhetetlenül szükséges közműhálózat csatlakozhat, tehát a helyiségen belül nem mehet át víz, gáz, csatorna és egyéb közművezeték.
   - A technikai védelmi rendszert a helyiségben ki kell építeni. A riasztásoknak az épület biztonsági szolgálatánál meg kell jelenniük. A védelem szabotázsvédett legyen és tegyen eleget a következő követelményeknek:
     - a nyílászárók nyitott és zárt állapot ellenőrző eszközzel legyenek ellátva,
     - a belső terek védelme mozgásérzékelővel biztosított legyen,
     - a védelem ki- és bekapcsolása a bejáraton kívül elhelyezett és minimum hat számjegyű kóddal működtetett tasztatúráról történjék.

- a személyzet a helyiségbe belépni szándékozókat belépés előtt a biztonság veszélyeztetése nélkül azonosítsa,
- a jelzőközpont és az általa működtetett eszközök 12 órás áthidalást biztosító szünetmentes tápegységgel rendelkezzenek oly módon, hogy a 12. óra letelte után még rendelkezzenek egy riasztási esemény jelzésére és a hozzá kapcsolódó vezérlés végrehajtására elegendő energiával (pl. hang- vagy fényjelző eszköz 3 perces időtartamban való működtetése).
- A helyiség ajtaja rendelkezzen legalább 30 perces tűzgátlással, továbbá a helyiségen belül automatikus és kézi jelzésadók kerüljenek telepítésre. A jelzésadók jelzéseit mind a helyiségen belül, mind az épület biztonsági szolgálatánál meg kell jeleníteni. A jelzésadó eszközök, valamint a jeleket feldolgozó központ feleljen meg az MSZ 9785, valamint az EN 54 szabvány sorozatok előírásainak, rendelkezzenek a hazai minősítő intézetek forgalombahozatali engedélyével. Az automatikus tűzoltó rendszerek tervezése és szabályozása Az IT Igazgató által meghatározottak szerint történjék.
- A helyiséget úgy kell elhelyezni, hogy felette és a határoló falfelületeken vizes blokkot tartalmazó helyiségrész ne legyen, nyomó- és ejtőcsövek ne haladjanak át, gázvezetéket telepíteni tilos.
- Az elektromos hálózat legalább a szerver és a szükségvilágítás vonatkozásában 30 perces áthidalási idejű megszakításmentes átkapcsolással rendelkező szünetmentes tápegységgel legyen ellátva.
- A tápegység akkumulátorai a maximális igénybe-vételt követő töltés hatására teljes kapacitásukat 24 órán belül nyerjék vissza.
- A padlóburkolatok, berendezési tárgyak antisztatikus kivitelűek legyenek.
- A villámvédelem elégítse ki a kommunális és lakóépületekre vonatkozó előírásokat és az MSZ 274-5T:1993 szabvány szerint az LPZ 0B - LPZ 1 zónahatáron túlfeszültség elleni védelembe kell
- bevonni az árnyékolást megtestesítő, az épületbe belépő minden fémszerkezetet (az elektromos hálózatot, víz, gáz, távfűtés, csatorna hálózatokat, antenna bevezetéseket, adatátviteli és távbeszélő hálózatokat, stb.).
- A túlmelegedés elleni védelmet a helyiség klimatizálásával kell biztosítani.
- A légellátás legfeljebb a klimatizáló berendezések által átlagos szinten biztosított porkoncentrációt érheti el.

3) Kiemelt biztonsági osztályban az előzőeken túl:
- A területre történő belépést azonosításra és hitelesítésre alkalmas rendszerrel kell ellenőrizni.
- A fűtést a klímarendszeren keresztül meleg levegő befúvással kell megoldani, a helyiségben vizes fűtés nem létesíthető. A klímarendszer kültéri és beltéri egységből épüljön fel, vízhűtéses klíma nem telepíthető. Központi klímagép telepítése esetén a befúvó és az elszívó légcsatornába légmentesen záró, tűzgátló tűzcsappantyúkat kell telepíteni.
- A szerverszobába csak az annak üzemeltetéséhez elengedhetetlenül szükséges közműhálózat csatlakozhat. A technikai

védelembe legyenek bekötve a hardver-védelemmel ellátott gépek burkolatai az illetéktelen kinyitás jelzésére, a hardver-védelem eltávolításának megakadályozására. A szerverszobák, és az egyéb "központi" jellegű informatikai helyiségek védelmét intelligens beléptető rendszerrel kell kiegészíteni, amely a mozgásokat mindkét irányban regisztrálja, legalább az utolsó 4.000 eseményt naplózza és az utolsó személy távozásakor a védelmi rendszert automatikusan élesítse.

- A hardver-védelemmel ellátott munkaállomások elhelyezésére szolgáló helyiségeket munkaidőn kívül elektronikus védelemmel kell ellátni.
- A helyiség automatikus működtetésű oltórendszerrel egészítendő ki, az oltórendszer működését tekintve legyen gázüzemű, helyi vagy teljes elárasztásos legyen, működése előtt biztosítson elegendő időt a személyzet evakuálására, vezérlő kimeneteinek egyikén adjon jelzést a szervernek az automatikus mentésre, majd azt követően a lekapcsolásra.
- Az energiaellátás biztonsága érdekében a szünetmentes tápegység mellett olyan szükség-áramellátó diesel-elektromos gépcsoportot is kell telepíteni, amely automatikus indítású és szabályozású, akkora teljesítményű, hogy képes legyen kiszolgálni a számítástechnikai eszközökön túl az azok működéséhez szükséges segédüzemi (pl. klíma) berendezéseket is.

7.2.1. Az informatikai berendezések elhelyezése és védelme

A környezeti veszélyek és kockázatok mérséklése érdekében:

a) A berendezéseket úgy kell elhelyezni, hogy lehetőleg megakadályozzuk az illetéktelen hozzáférést, és a helyiség észrevétlen megközelítését.
b) A különleges védelmet igénylő eszközöket elkülönítetten kell elhelyezni és használni.
c) A környezeti határok és a lehetséges veszélyforrások folyamatos vizsgálatával és elemzésével kell törekedni a szükséges működési feltételek biztosítására.

7.2.2. Az informatikai berendezések energiaellátása

Az elektromos hálózat meghibásodása, az energiaellátás megszűnése esetére gondoskodni kell a berendezések védelméről, a következők szerint:

a) Az áramszolgáltatónak meg kell felelnie az informatikai berendezés gyártója által meghatározott követelményeknek.
b) Többféle alternatív áramszolgáltatási lehetőség igénybevétele (pl. aggregátor).
c) Megszakítás nélküli áramforrás (UPS) használata,
d) Tartalék áramfejlesztő rendszerbeállítása.

7.2.3. A kábelezés biztonsága

Az adatátviteli és energiaellátó hálózat kábelezésénél a következő követelményeket kell betartani:

a) Védett kábelek használata:
   1) a károkozás, szándékos vagy gondatlan beavatkozás elhárítására,
   2) a környezeti veszélyek (tűz, robbanás, tűz, víz, por, elektromágneses sugárzás, stb.) káros hatásai következményeinek elhárítására, csökkentésére.

b) Az adatátviteli (távközlési) kábel elkülönítése az energiaellátás kábeleitől.

7.2.4. Az informatikai berendezések karbantartása

A megbízható működés érdekében a berendezések folyamatos használata és rendelkezésre állásának biztosítása érdekében:

a) A specifikációban javasolt időközönként el kell végezni a berendezések karbantartását.
b) A berendezések kezelését,illetve javítását csak megfelelő szakképzettséggel rendelkező személyek végezhetik.
c) Az informatikai berendezések külső helyszínen történő javítása, karbantartása esetén gondoskodni kell a berendezésen tárolt adatok végleges (visszaállíthatatlan) törléséről.

7.2.5. A BVK Holding Zrt. telephelyén kívüli informatikai berendezések biztonsága

A BVK Holding Zrt. telephelyén (telephelyein) kívüli adatfeldolgozás csak a 4.2. és a 4.3. fejezetekben szabályozott módon megengedett. Az alkalmazandó biztonsági előírásoknak meg kell egyezniük egyaránt a BVK Holding Zrt. telephelyén hasonló feladatokhoz használt informatikai berendezésekre vonatkozó előírásokkal.

Az egyes külső helyszínek között jelentős különbségek lehetnek a biztonsági kockázatok (károkozás, lopás, lehallgatás, stb. veszélye) mértéke között, ezt figyelembe kell venni a szükséges biztonsági eszközök és eljárások kiválasztásánál.

7.2.6. Az informatikai berendezések újbóli használata, illetve tárolása használaton kívül

Az informatikai berendezések használaton kívül helyezés előtt gondoskodni kell az összes érzékeny, illetve minősített adat, szolgálati szoftver visszaállíthatatlan eltávolításáról vagy felülírásáról.
A használaton kívül helyezett informatikai berendezés és a BVK Holding Zrt. összes hálózata közötti összeköttetést meg kell szüntetni. A használaton kívüli informatikai berendezés újbóli rendszer-beállításakor úgy kell eljárni, mint egy új eszköz üzembeállítása során.

7.3. Általános védelmi intézkedések

Általában az informatikai eszközöket, illetve az azokban tárolt, kezelt adatokat védeni kell a jogosulatlan betekintés, súlyosabb esetben az eltulajdonítás (lopás), a jogtalan közzététel, és a legsúlyosabb esetben a jogosulatlan módosítás ellen. Fokozottan kell figyelni a megelőzésre, valamint a megfelelő védelmi intézkedések működtetésére a károk és veszteségek mérséklése érdekében.

Az adatkezelési eljárások a 8.6.3 pontban kerülnek leírásra.

7.3.1. Adattárolási és képernyő-kezelési irányelvek

a) A monitorokat úgy kell elhelyezni, hogy az azon megjelenő adatokat illetéktelen személy ne láthassa.
b) A képernyővédőknek jelszavas védelemmel ellátottaknak kell lenniük. A képernyővédő megjelenési idejét úgy kell beállítani, hogy az a rendes munkavégzésben ne okozzon zavarokat.

c) A fokozott illetve a kiemelt biztonsági osztályba tartozó rendszerek munkaállomásait külön fizikai vagy logikai elérés ellenőrző rendszerrel kel ellátni és az ilyen eszközök kizárólag zárolás után hagyhatók felügyelet nélkül.

d) A BIOS-SETUP állítását jelszóhoz kell kötni úgy, hogy annak el kell térnie a felhasználói jelszótól és azt a számítógépet felügyelő rendszer-adminisztrátor állítja be, biztosítva, hogy a felhasználó ne tudja az indítási konfigurációt megváltoztatni. A felhasználói jelszavak kezelése a 9.2.3. pontban kertült szabályozásra.

7.3.2. Eszközök ki/be szállítása

a) Számítástechnikai eszközöket, adathordozókat, programokat kizárólag a szervezeti egységek vezetőinek engedélyével szabad a munkahelyről kivinni / behozni és az ilyen eseményre kizárólag a biztonsági szolgálat ellenőrzése mellett kerülhet sor, egyúttal bizonyító erejű dokumentumot kell csatolni. (nyilatkozat, raktárjegy, szállítólevél, számla, stb.).

b) A BVK Holding Zrt. területéről elvitt eszközöket a biztonsági szolgálat jelentése alapján az eszközgazdálkodónak, szoftver nyilvántartónak nyilván kell tartania

c) A kivitelre kerülő eszközökön tárolt adatok illetéktelenek általi elérhetetlenségére fokozottan kell figyelni.

d) Meghibásodott eszköz cseréje esetén – még garanciális esetben is – adathordozó csak úgy vihető ki, ha arról minden adat visszaállíthatatlan módon törlésre került.

8. Számítógépes hálózati szolgáltatások és az üzemeltetés menedzselése

8.1. Üzemeltetési eljárások és feladatok

a) Az adatfeldolgozó kapacitások megbízható és biztonságos működésének biztosítása érdekében meg kell határozni az összes adatfeldolgozó egység kezelésére és működtetésére vonatkozó feladatokat és eljárásokat. Ebbe beletartozik az összes szükséges működtetési és hibaelhárítási eljárás elkészítése is.

b) Meg kell valósítani a kötelezettségek különválasztását.

8.1.1. Az üzemeltetési eljárások dokumentációja

a) Az üzemeltetési eljárásokat részletesen és szabályszerűen dokumentálni kell.

b) Az üzemeltetési eljárások dokumentációinak a munkafolyamat minden részelemének vonatkozásában részletes utasításokat kell tartalmaznia a következők szerint:

1) az adatkapcsolatok, (feldolgozás és tárolás), adatáramlási utak, formák, átadási-, átvételi eljárások norma szerinti és különleges esetei;
2) tervezett normál működés folyamatai, teljesítendő termelési követelmények (pl. Időrendek, időzítések), ezek közt a biztonsági követelmények, külön kiemelve a más rendszerek biztonsági megoldásaival összefüggő kölcsönhatásokat (pl. a saját vagy a másik alkalmazás adatai bizalmasságának sérülését),
3) üzemeltetés rendkívüli esetei és azok kezelésének szervezése, külön-eljárások előírásai (pl. munkaidőn kívüli munkahelyen való tartózkodás szabályai, értesítendők, stb.),
4) hibaesetekre és rendellenes működésre vonatkozó eljárások, mindenek előtt a rendkívüli helyzet felismerésének, azonosításának kritériumai;
5) munkavégzés közben fellépő kivételes állapotok kezelése, mentések
6) rendszer újraindítása és visszaállítása.

c) Az üzemeltetési eljárások dokumentációját ez üzemeltetés helyén hozzáférhetővé kell tenni, azokat oktatni szükséges és ellenőrizni oly módon, hogy nem elegendő az üzemrend ismerete, a követelmény a jártasság szintjének elérése – beleértve a

biztonsági intézkedések végrehajtását is. A jártasság szintjének eléréséért az üzemeltetés vezető felelős.

8.1.2. Változáskezelés és ellenőrzés az üzemeltetés során

A változásokat a Változáskezelési Szabályzat alapján ellenőrizni és dokumentálni kell, a következő tevékenységeket pedig el kell végezni:

a) Jelentős változások azonosítása.
b) Felelős résztvevők megjelölése.
c) A változások lehetséges hatásainak felmérése.
d) A tervezett változtatások jóváhagyási eljárásainak ellenőrzése.
e) Az összes érintett értesítése a változások részleteiről.
f) A változtatás megszakításáért és az eredeti állapotba való visszaállításáért felelős személy kijelölése.

8.1.3. Váratlan események kezelési eljárásai

A biztonsági eseményre adandó gyors, effektív és szabályos válaszadás érdekében meg kell határozni a váratlan eseményekkel kapcsolatos felelősségeket és eljárásokat. A következő kontrollokat kell alkalmazni:

a) Eljárásokat kell meghatározni a következő biztonsági események kezelésére:
   1) az informatikai rendszer hibái és a szolgáltatás megszakadása,
   2) szolgáltatás megtagadása,
   3) pontatlan és hiányos adatokból származó hibás eredmények,
   4) a bizalmasság elvesztése.
b) Az üzletmenet-folytonossági tervhez kapcsolódóan a következő eljárásokat kell alkalmazni:
   1) azonosítani és elemezni kell az események okait,
   2) terveket kell kidolgozni a nem kívánt esemény ismétlődésének megakadályozására,
   3) az eseményeket naplózni kell,
   4) gondoskodni kell a visszaállítás megoldásáról
   5) az illetékes szervezeti egység vezetője és Az IT Igazgató részére jelentést kell készíteni.
c) A biztonsági események és rendszerhibák javítását szabályozottan kell végrehajtani. A szabályoknak a következő elvek érvényesülését kell garantálnia:
   1) csak az engedéllyel (és a kellő szaktudással rendelkező személyek férhetnek az "éles" rendszerekhez és azok adataihoz,
   2) minden rendkívüli esemény során az alkalmazandó/alkalmazott eljárást a vezetőnek ismernie és ellenőriznie kell,
   3) minden rendkívüli esemény során az alkalmazandó/alkalmazott eljárást részletesen dokumentálni kell,
   4) a rendkívüli eseményeket követően az adatok sértetlenségét haladéktalanul ellenőrizni kell.

8.1.4. A feladatkörök biztonsági szétválasztása

Az informatikai rendszerek biztonsági beállításainak, hangolásának tevékenységeit (operációs rendszerek adminisztrátorok, alkalmazások rendszergazdái) – a véletlen és/vagy szándékos visszaélések elkerülése végett, szét kell választani úgy, hogy azokat több személynek együttesen kelljen végrehajtania.
Gondoskodni kell arról, hogy szabályok betartásának biztonsági ellenőrzése a végrehajtó szervezettől és a menedzsmenttől függetlenül működjék.

Ahol a szétválasztás megoldása aránytalan terheket jelentene a szervezetre, ott monitorozással, az eseménynaplók elemzésével és fokozott vezetői felügyelettel kell eljárni.

8.1.5. A fejlesztési és az üzemeltetési feladatok szétválasztása

a) "Éles" üzemben működtetett informatikai rendszerben fejlesztések, tesztelések nem folytathatók.
b) "Éles" adatokkal tesztelést végezni tilos, teszteléshez mindig tesztadatokat kell készíteni (generálni). Garantálni kell, hogy tesztrendszerből végrehajtott tranzakció semmiként ne válhasson üzletileg érvényessé.
c) Fejlesztés alatt álló rendszerben "éles" üzemi tevékenységet folytatni tilos, az erre vonatkozó felszólítást meg kell tagadni és rendkívüli eseményként kell regisztrálni, jelenteni.
d) A fordító, szerkesztő és egyéb segédprogramok "éles" üzemi rendszerben csak abban az esetben legyenek elérhetők, ha ezekre a programokra dokumentáltan és engedélyezetten szükség van.
e) „Éles" üzemi rendszerben az IT Igazgató és a vizsgálatban érintett szakterület(ek) vezetőjének írásos engedélye nélkül képernyőlopó, operátori tevékenység rögzítő, független hálózati csomag ellenőrző, követő vagy módosító programot, hálózat vagy port felderítő alkalmazást installálni, használni tilos. Ilyenek jelenlétét önmagában veszélyhelyzetként kell kezelni és ki kell vizsgálni. Ilyen programot a BVK Holding Zrt. „éles" környezeteiben csak vizsgálati céllal és csak a korábban leírt engedélyezés után lehet használni.
f) A fejlesztők az üzemi rendszerben rendszergazdai (administrator, root, supervisor stb.) jogosultságokat nem kaphatnak, amennyiben erre ideiglenesen szükség van, ezt követően a jelszavakat haladéktalanul meg kell változtatni, és a rendszer biztonsági beállításait teljes körűen felül kell vizsgálni
g) Az IT Igazgató vagy munkatársa részére kiadott rendszer adminisztrátori jogosultságok, csak az adatvédelmi tevékenységgel kapcsolatos munkák során, jegyzőkönyvezve használhatók.

8.1.6. Külső létesítmények üzemeltetése

A BVK Holding Zrt. informatikai rendszereinek üzemeltetésére, adatfeldolgozására harmadik személlyel kötött vállalkozási szerződésekben ki kell térni a BVK Holding Zrt. ellenőrzési jogosultságára, lehetőségeire, eszközeire és eljárásaira. A szerződéskötés során figyelembe kell venni:

a) Az alkalmazások és adatok érzékenységét, biztonsági osztályát.
b) A szükséges jóváhagyások beszerzését.
c) Az üzletmenet-folytonossági (katasztrófa elhárítási) tervekre gyakorolt hatását.
d) A vállalkozó által alkalmazandó biztonsági szabályokat és alkalmazásokat.
e) A biztonsággal, valamint az adatkezeléssel összefüggő tevékenységek hatékony nyomon-követhetőségét.
f) A biztonsági események jelentéstételi kötelezettségét, illetve a kezelésükre vonatkozó feladatokat és eljárásokat.

8.2. Informatikai rendszerek tervezése, és átvétele

a) A megfelelő kapacitás és a szükséges erőforrások elérhetősége érdekében előzetes tervezést és előkészületeket kell végrehajtani.

b) A rendszer(ek) túlterheltségével járó kockázatok mérséklése érdekében szükség van a kapacitások iránti várható igények előrejelzésére.

c) Meg kell határozni az új rendszerek üzemeltetési követelményeit, a rendszer átvétele és üzembe helyezése előtt el kell végezni a követelmények dokumentálását és le kell futtatni a szükséges teszteket.

8.2.1. Kapacitástervezés

A rendszer működtetéséhez, működéséhez szükséges adatfeldolgozó és adattároló kapacitásokról való gondoskodás feltételei:

a) Fel kell mérni, illetve nyomon kell követni a kapacitás iránti igények várható alakulását.
b) Figyelembe kell venni a környezet és a rendszer támasztotta igényeket.
c) Nyomon kell követni a rendszer erőforrásainak – processzorok, központi tárolóegységek, adatállományok tárolására rendszeresített eszközök, nyomtatók és egyéb kimenetek, adatátviteli rendszerek – felhasználását.
d) Meg kell határozni az üzleti alkalmazások és a vezetői információs rendszer eszközeinek felhasználását.
e) Ki kell szűrni és meg kell szüntetni a rendszer biztonságát és a felhasználói szolgáltatásokat veszélyeztető szűk keresztmetszeteket, illetve meg kell tervezni a rendszer helyreállításhoz szükséges intézkedéseket.

8.2.2. A rendszer átvétele

Az informatikai rendszerek átvételének alapvető követelménye az átadás-átvételi jegyzőkönyv, melynek tartalmaznia kell minden, az átvétellel kapcsolatos feladatot, kötelezettséget, dokumentációt. Az átvételi jegyzőkönyvben önálló fejezetben dokumentálni kell, hogy az üzemeltetéshez szükséges (8.6.4.g) pont szerinti dokumentáció átadásra került-e, hogy a (6.2) pont szerinti kiképzés megtörtént-e, hogy az (11.1.3) pont szerinti üzletfolytonossági- és katasztrófa tervek elkészültek-e. Ugyancsak az átadás-átvételi jegyzőkönyvben kell rögzíteni a hiánypontok esetén akár az átadó, akár az átvevő (viszontszolgáltatás esetén, akár a felhasználó) oldalán vállalt kockázatokat, az azok megszüntetésére rendelt intézkedéseket, feladatokat, felelősöket és határidőket.

8.3. Védelem rosszindulatú programok ellen

A programok és az adatfeldolgozó kapacitások ki vannak téve a rosszindulatú programok bevezetésével járó veszélyeknek. (Ebbe a kategóriába soroljuk a vírusokkal fertőzött termékeket, a hálózati férgeket, trójai lovakat, valamint a logikai bombákat.)

a) Megfelelő intézkedésekkel kell megakadályozni, illetve kiszűrni a rosszindulatú programok bevezetését.
b) A felhasználóknak ismerniük kell a rosszindulatú és engedély nélküli programok alkalmazásával járó veszélyeket.
c) A vezetőknek gondoskodniuk kell a rosszindulatú programok kiszűrésére és megelőzésére alkalmas különleges ellenőrző eszközök alkalmazásáról.

8.3.1. A rosszindulatú programokat ellenőrző eszközök

A rosszindulatú programokkal szembeni védekezést szűréssel és a programok bevezetése előtti ellenőrzéssel kell megvalósítani. A rosszindulatú program elleni védekezés részét kell, hogy képezze a felhasználók tájékoztatása és oktatása, a hozzáférés-védelem, továbbá a változtatások felügyelete és ellenőrzése. Ennek során szükséges:

a) Olyan eszközök alkalmazása, melyek megkövetelik a "jogtiszta" programok használatát és tiltják az engedély nélküli termékek alkalmazását.
b) Külső hálózatokból vagy azokon keresztül, illetve egyéb adathordozókról telepített adatállományok és programok felhasználásával járó kockázat elhárításához szükséges intézkedések bevezetése.
c) Vírusfelismerő és megsemmisítő programok telepítése és rendszeres aktualizálása.
d) A kritikus üzleti folyamatokat támogató rendszerek adattartalmának és programjainak rendszeres vizsgálata.
e) A bizonytalan eredetű adatállományok ellenőrzése, vírusok kiszűrése.
f) E-mail kiterjesztések, csatolt dokumentumok és letöltések használat előtti ellenőrzése.
g) A vírusokkal szembeni védelemre vonatkozó feladatok és eljárások meghatározása, alkalmazásuk oktatása, a vírustámadások naplózása és az eredeti állapot helyreállítása.
h) Megfelelő üzletmenet-folytonossági terv összeállítása, a szükséges adatállományok és programok back-up példányainak és a helyreállítás eljárásainak elkészítése.
i) A hamis, vagy hamisított programra vonatkozó összes információ ellenőrzése, a figyelmeztető tájékoztató kiadványok folyamatos frissítése, meglétének ellenőrzése. Fontos, hogy a felhasználókat a rendszerhibát okozó "láncievelekről", illetve az illegális programok használatának veszélyeiről értesíteni kell. A felhasználót a gépén tárolt illegális programokért felelősségre kell vonni. Az informatikai üzemeltetésnek - például körlevelek formájában - folyamatosan figyelmeztetnie kell a felhasználókat a frissen megjelent fenyegetésekről.

8.3.1.1. A vírusvédelmi rendszer kialakítása és működtetése

a) Központosított hálózati felhasználó adminisztrációt kell kialakítani – az egyenrangú hálózatokat fel kell számolni, a felhasználókat tartományba vagy szerverre kell bejelentkeztetni.
b) El kell készíteni a Vírusvédelmi Szabályzatot.
c) Vírusvédelmi felelősöket kell kijelölni.
Az összes érintett dolgozóra kiterjedő felhasználói oktatásnak ki kell térni a vírusvédelmi rendszer működésére

8.3.2. A felhasználók felelőssége, feladatai

A felhasználók kötelessége, hogy az általuk használt munkaállomásokon, hordozható eszközökön a vírusvédelmi rendszer telepítve legyen és ennek hiányát vagy működésképtelenségét a Vírusvédelmi rendszergazdának jelentsék. Kötelességük továbbá a vírusvédelmi előírások megismerése és betartása, valamint az erre vonatkozó nyilatkozat aláírása.

A felhasználó által átvett munkaállomáson a vírusvédelmet érintő változásokért a felhasználó a felelős, a vírusvédelmi rendszer konfigurációjának megváltoztatása szankciókat von maga után.

A felhasználó nem vonható felelősségre vírustámadással kapcsolatban abban az esetben, amennyiben a Vírusvédelmi szabályzatban foglaltakat betartotta.

8.3.2.1. Felhasználókra vonatkozó tiltott tevékenységek

1. A felhasználónak minden esetben be kell jelentkeznie a munkaállomásra. TILOS a munkaállomások bejelentkezési ablakát megkerülni
2. A felhasználónak TILOS a víruskereső szoftver konfigurációjának módosítása!
3. A felhasználónak TILOS a víruskereső szoftver futásának leállítása akár ideiglenesen is!
4. TILOS a munkaállomáson alkalmazott - az előző fejezetében felsorolt - biztonsági beállításokat megváltoztatni!
5. A felhasználó nem telepíthet, mozgathat állományokat a munkaállomásra olyan hordozható adathordozóról (CD, hajlékony mágneslemez, ZIP drive, stb.), mely nem-ellenőrzött forrásból érkezik.
6. A felhasználó nem telepíthet és használhat a munkaállomásán engedély nélküli, az üzemeltetés által nem támogatott szoftvereket.
7. TILOS a levelekben érkező csatolt állományokat dupla kattintással megnyitni! A felhasználónak kötelessége, hogy a csatolt állományokat először a diszkre mentse, majd az elmentett állományt nyissa meg!
8. TILOS vírustámadással kapcsolatos leveleket, másoktól hallott vírusokkal kapcsolatos információkat (kacsák) továbbítani! E szabály alól kivételt képez a Vírusvédelmi rendszergazda, akinek egy személyben joga és kötelessége vírusfertőzés gyanúja esetén az érintetteket értesíteni, melyre használhatja a levelező rendszert is
9. TILOS a munkaállomások között adatmozgatást megosztásokon keresztül végrehajtani, fájlmozgatásra minden esetben a fájlszerverek közös munkakönyvtárát kell használni!
10. TILOS üzleti dokumentumok akár munka, akár végleges példányát kizárólag a munkaállomáson tárolni! A felhasználónak feladata, hogy naponta legalább egyszer az állományt a hálózati meghajtóra mentse.
11. Mindenki számára TILOS vírusokat készíteni, módosítani (mutációkat létrehozni), víruskészítésre alkalmas eszközöket a szabályzat hatálya alá tartozó tárgyi eszközökön tárolni!
12. A munkaállomás felhasználóinak, TILOS adminisztrátori jogokkal tevékenykedniük!

8.3.2.2. Fertőzésgyanú kezelése

Fertőzés gyanúja esetén a felhasználónak nem kötelessége a rendellenességek értelmezése. Amennyiben a felhasználó rendellenes működést tapasztal, kapcsolatba kell lépnie az Ügyfélszolgálattal.

8.3.2.3. Hibabejelentés

A felhasználónak jogában áll a munkáját akadályozó esetben a vírusvédelmi rendszerrel kapcsolatban hibát bejelenteni. Ezt szintén az Ügyfélszolgálatnál teheti meg.

8.3.2.4. A vírusvédelmi szoftver frissítése

A vírusvédelmi szoftver frissítéséért a Vírusvédelmi rendszergazda a felelős, a felhasználónak a frissítéssel tennivalója nincsen! A munkaállomások frissítése automatikusan, a felhasználó beavatkozása nélkül történik.

8.4. Operátori tevékenységek

8.4.1. Az adatmentések tartalék példányai

a) A megtervezett mentési és visszaállítási eljárásokra üzemeltetési előírásokat kell készíteni és azok betartását rendszeresen ellenőrizni kell.

b) A biztonsági mentéseket a háromgenerációs elv betartása mellett, lehetőség szerint külön telephelyen, de minimum a követelményeknek megfelelő külön helyiségben kell tárolni, ennek részleteit az Üzletmenet-folytonossági Terv határozza meg.

c) A mentések nyilvántartását az erőforrásoknak megfelelően kell vezetni és azok helyességét rendszeresen ellenőrizni kell. Törekedni kell arra, hogy a mentések adminisztrációját önálló alkalmazás szolgálja ki, amely tartalmazza a végrehajtás ellenőrzés, keletkezéssel egyidejű karbantartás, az automatikus címkegyártás, frissítési és lejárati határidő figyelés, stb. automatizált funkcióit.

d) Az időszakos, archiválandó (pl. éves) mentéseket a jogszabályokban meghatározott ideig, de minimum 6 évig, bármikor visszakereshetően, helyreállíthatóan kell megőrizni.

8.4.2. Operátori naplók

Az elszámoltathatóság és auditálhatóság biztosítása érdekében olyan regisztrálási és naplózási rendszert kell kialakítani, hogy utólag megállapíthatóak legyenek az informatikai rendszerben bekövetkezett fontosabb események, különös tekintettel azokra, amelyek a rendszer biztonságát érintik. Egyúttal lehessen ellenőrizni a hozzáférések jogosultságát, meg lehessen állapítani a felelősséget, valamint az illetéktelen hozzáférés megtörténtét vagy annak kísérletét.

a) A rendszernek képesnek kell lennie minden egyes felhasználó vagy felhasználói csoport által végzett művelet szelektív regisztrálására. A minimálisan regisztrálandó események a következők:
   1. rendszerindítások, -leállások, leállítások,
   2. rendszerhibák és korrekciós intézkedések,
   3. programindítások és -leállások, leállítások,
   4. az azonosítási és hitelesítési mechanizmus használata,
   5. hozzáférési jog érvényesítése azonosítóval ellátott erőforráshoz,
   6. az adatállományok és kimeneti adatok kezelésének visszaigazolása,
   7. azonosítóval ellátott erőforrás létrehozása vagy törlése,
   8. felhatalmazott személy műveletei, amelyek a rendszer biztonságát érintik.

b) Az informatikai rendszer üzemeltetése során – az operátori tevékenységek dokumentálására - operátori naplót kell vezetni.

c) Ki kell alakítani a biztonság belső ellenőrzésének rendszerét, amely során meg kell határozni a felügyeleti és megelőzés tevékenységek eljárásrendjét.

d) Az informatikai rendszer üzemeltetéséről nyilvántartást kell vezetni, amelyet az informatikai vezető által kijelölt személynek rendszeresen ellenőriznie kell.

Törekedni kell arra, hogy a fenti funkciócsoportot egészben vagy részben automatizált Üzemviteli rendszer szolgálja ki.

8.4.3. Az üzemzavarok naplózása

Az üzemzavarok bejelentésekor / észlelésekor korrekciós intézkedéseket kell kezdeményezni, függetlenül attól, hogy a jelzés az Ügyfélszolgálaton- vagy az Üzemeltetésen keresztül érkezett. minden esetben kötelező a másik fél és az aktuális felhasználói kör értesítése. A felhasználók által jelentett, az adatfeldolgozás vagy átviteli rendszerek működésében észlelt hibákat naplózni kell.

Az üzemzavar kezelésének szabályai:

a) A hibanapló vizsgálata és a hiba kezelésének, elhárításának ellenőrzése
b) Korrekciós intézkedések vizsgálata, illetve ezek végrehajtásának és a kezdeményezett intézkedések engedélyezésének szabályosságának ellenőrzése.

8.5. Hálózatmenedzsment

A hálózatmenedzsment segítségével kell meghatározni a hálózatok adattartalmi biztonságát és az infrastruktúra védelmét, különös tekintettel a több szervezetet átfogó hálózatokra.

8.5.1. Hálózati ellenőrző eszközök

Olyan ellenőrző eszközökről kell gondoskodni, amelyek biztosítják a hálózatokban kezelt és továbbított adatok biztonságát, valamint a kapcsolt szolgáltatásokat megóvják az illetéktelen hozzáférésektől.

a) A hálózatok és a számítógépek működtetésének feladatait szét kell választani.
b) A nyilvános hálózatokon keresztül továbbított érzékeny adatok, illetve a kapcsolt rendszerek védelmére másodlagos ellenőrző eszközökre van szükség.
c) Pontosan definiálni kell a hálózat határait. A hálózat biztonságos szegmentálásának kialakításáért a cégvezetés által kijelölt személy (vezető) a felelős

8.6. Az adathordozók biztonságos kezelése

Az eszközök károsodásának megelőzése, és az üzleti tevékenységekben okozott fennakadás megakadályozása érdekében:

a) Gondoskodni kell az adathordozók ellenőrzéséről és fizikai védelméről.
b) A szigorú számadás elvei szerint meg kell előzni a dokumentumok, a számítástechnikai adathordozók (szalagok, lemezek, kazetták), az input/output adatok és a rendszerdokumentációk károsodását, eltulajdonítását és engedély nélküli törlését.
c) Szabályozni kell az adathordozók beszerzését, tárolását és kezelését.
d) Biztosítani kell, hogy az adathordozók kezelése – a vonatkozó iratkezelési szabályok szellemében – a tárolt adatok szempontjából egyenértékű legyen papír alapú dokumentumok kezelésével. Az adathordozókról és azok tartalmáról nyilvántartást kell vezetni.
e) A BVK Holding Zrt.-nél csak nyilvántartott és egyedi azonosítóval ellátott adathordozót szabad használni.
f) A BVK Holding Zrt.-en kívüli adatforgalomban használt adathordozók előállítása, kiadása és fogadása az ügyviteli (iratkezelési) szabályzat előírásai szerint a kijelölt helyeken, dokumentált és ellenőrzött módon történhet. Az adathordozókat

használatba venni csak az előírt ellenőrző eljárások elvégzése után szabad (pl., vírusellenőrzés).

g) Minden adathordozót újraalkalmazás előtt, felszabadítás, selejtezés után az adatok megsemmisítését eredményező megfelelő eljárással törölni kell.
h) Az adattípus (minősítés) felismerhető jelölését a számítástechnikai berendezéssel előállított adattároló és megjelenítő eszközökön biztosítani kell.
i) Az adatok sértetlen és hiteles állapotának megőrzését biztosítani kell.
j) Az adathordozók kivitelére, illetve a meghibásodott adathordozók cseréjére vonatkozó előírásokat a (8.7) pont tartalmazza.
k) PEN-drive használata esetén kizárólag a Társaság által beszerzett, és személyi használatra átadott/átvett eszközök használata megengedett. Az eszköz használatához USB port engedély szükséges.

8.6.1. Az adathordozók kezelése

Az adathordozókat biztonságos módon kell kezelni. Annak érdekében, hogy ezek az adathordozók ne kerülhessenek illetéktelen felhasználásra, a következők szerint kell eljárni:

a) Nem minősített adathordozókat az ügyviteli (iratkezelési) szabályzat előírásai szerint kell kezelni.
b) Érzékeny információt tartalmazó adathordozókat az ügyviteli (iratkezelési) szabályzat és a titokvédelmi szabályzat szerint kell tárolni és kezelni.

8.6.2. Az adathordozók biztonságos tárolása

Az adathordozókat – azokat is, amelyek használaton kívül annak – biztonságos helyen kell tárolni, vagy mennyiben ezek munkaközi példányok, meg kell semmisíteni.

a) Ezek a következők:
   a. kinyomtatott dokumentumok,
   1) hang- és egyéb adatrögzítés,
   2) nyomtatópapír,
   3) kimeneti jelentések,
   4) egyszer használatos nyomtatószalagok, ~ mágnesszalagok
   5) mobil diszkek és kazetták
   6) optikai tárolóeszközök (összes lehetséges formája, ideértve a telepítőkészleteket gyártó terjesztéséhez alkalmazott adathordozókat),
   7) programlisták,
   8) tesztadatok.
   9) rendszerdokumentáció
b) Az adathordozók tárolására vonatkozó fizikai védelem követelményeivel kapcsolatban a rendszerszintű IBSz-ekben meg kell határozni:
   1) a tárolók környezeti paramétereire vonatkozó előírásokat és a paraméterek normál értékeinek biztosítására, ellenőrzésére vonatkozó intézkedéseket,
   2) az elöregedésből fakadó adatvesztés elleni megelőző intézkedéseket (pl. rendszeres átírás),
   3) az adathordozók másodpéldányainak biztonságos tárolására vonatkozó előírásokat,
   4) az adathordozók kölcsönzésével kapcsolatos előírásokat,
   5) a rendszer- és a felhasználói szoftver törzspéldányok biztonságos tárolására, valamint a használati másodpéldányok készítésére vonatkozó előírásokat.

c) A fokozott biztonsági osztályba sorolt minősítésű adathordozók tárolása csak megbízhatóan zárt helyiségben, minimum 30 perces tűzállóságú tároló szekrényben történhet.

8.6.3. Adatkezelési eljárások

Az adatok illetéktelen közzétételének, illetve felhasználásának megakadályozása érdekében szükségesek az adatkezelést (-tárolást, -feldolgozást) szabályozó eljárások. Ezeknek az eljárásoknak – az adatok minősítésének megfelelően– igazodniuk kell az előírásokhoz, szabályzatokhoz, számítástechnikai rendszerekhez, hálózatokhoz, a használt számítástechnikai eszközökhöz, távközlési, hangátviteli és multimédiás, levelező- stb. rendszerekhez. Az adatkezelési eljárások előírása, meghatározása során a következőket kell figyelembe venni:

a) Az összes adathordozó kezelése és címkézése.
b) Az illetéktelen személyek kiszűrése, hozzáférésük megakadályozása.
c) A bemenő adatok teljeskörűségének, az adatfeldolgozás teljességének és a kimeneti adatok hitelesítésének ellenőrzése.
d) A be- és kimenő adatok védelme, a védettség mértékének az adatok érzékenységéhez való igazítása.
e) Az adatok elosztásának szabályozása, ellenőrzése és korlátozása.
f) Az adatok minősítését, kezelési jelzését kötelezően alkalmazni kell és a változásokat automatikusan naplózni kell.
g) Rendszeresen ellenőrizni kell az adatok minősítésének alkalmazását.
h) A biztonsági naplófájlokat az arra feljogosított személynek a rendszer minősítésének megfelelő, meghatározott módon kell kezelnie, illetve kiértékelnie.
i) Az észlelt eltéréseket (hibás kezelés, jogosultság megsértésének a kísérlete) haladéktalanul ki kell vizsgálni és az eredményt jegyzőkönyvben kell rögzíteni. Ezért az adott szervezeti egység vezetője a felelős

8.6.4. Az informatikai rendszer dokumentációjának biztonsága

Az informatikai rendszerek dokumentációja biztonságilag érzékeny adatokat is tartalmazhat, ilyen érzékeny adat lehet a felhasználás folyamatainak leírása, az eljárás, az adatszerkezetek, vagy az engedélyezési folyamatok ismertetése. Az illetéktelen hozzáférés megelőzése érdekében:

a) Gondoskodni kell a rendszerdokumentációk biztonságos tárolásáról.
b) Minimálisra kell csökkenteni azok számát, akik hozzáférhetnek a rendszerdokumentációkhoz.
c) Gondoskodni kell a nyilvános hálózaton keresztül elérhető, vagy azon keresztül továbbított dokumentáció védelméről.
d) Az informatikai rendszer biztonságával kapcsolatos dokumentációt az informatikai rendszer biztonsági fokozatának megfelelő módon kell kezelni.
e) Az informatikai rendszer (vagy annak bármely elemének) dokumentációját változások menedzselésének keretében kell aktualizálni és naprakészen tartani. Gondoskodni kell a változások menedzseléséről és a biztonságot érintő változások, változtatások naplózásáról.
f) A rendszerben feldolgozásra kerülő, a fokozott és a kiemelt biztonsági osztályba sorolt adatok és hozzájuk kapcsolódó jogosultságok nyilvántartását elkülönítetten kell kezelni.

g) Az informatikai rendszer beszerzéssel és/vagy fejlesztéssel történő kialakításához és üzemeltetéséhez, a rendszer funkcionalitásának és megbízható üzemeltetésének a biztosításához a következő dokumentációk szükségesek:

Késztermék	Fejlesztett termék
Szállítási dokumentáció, minőségi bizonyítvány	Architektúra és konfiguráció szintű dokumentáció
Rendszerelemek, egységek dokumentációi	Modul szintű dokumentáció
Teljes rendszerdokumentáció	Teljes rendszerdokumentáció
Rendszerteszt dokumentáció	Tesztkövetelmények és eljárások dokumentációja modul szinten
Üzemeltetési dokumentáció (normál üzemeltetés, hibaelhárítás, újraindítás	Tesztkövetelmények és eljárások dokumentációja rendszer szinten
Felhasználói dokumentáció	Felhasználói dokumentáció Átadás-átvételi dokumentáció
Biztonsági rendszer dokumentációja	Üzemeltetési dokumentáció (normál üzemeltetés, hibaelhárítás, újraindítás)
	Biztonsági rendszer dokumentációja

A biztonsági rendszerek, alrendszerek dokumentációjának tartalmaznia kell a biztonsági funkciók leírását, azok installációját, aktiválását, leállítását és használatát a fejlesztés, valamint az üzemeltetés során.

8.7. Adatok és programok átadása

A szervezetek között cserélt adatok és programok elvesztésének, módosításának vagy illetéktelen felhasználásának lehetőségét is meg kell akadályozni. Az adatok és a programok szervezetek közötti átadását, cseréjét ellenőrizni kell, a cserének meg kell felelni a hatályos törvényeknek. Mérlegelni kell az elektronikus adatcsere, az elektronikus kereskedelem és az e-mail üzleti és biztonsági kockázatát, annak következményeit és az ellenőrző eszközök alkalmazására vonatkozó követelményeket.

8.7.1. Megállapodások az adatok és programok cseréjéről

A BVK Holding Zrt. más szervezettel adat- és programcserét kizárólag írásbeli szerződés alapján bonyolíthat, melyben utalni kell az érzékeny információk kezelésére is.

A csere biztonsági feltételeire vonatkozó megállapodásokban meg kell határozni:

a) Az adatátvitel, feladás és átvétel ellenőrzésének és bejelentésének eljárási szabályait.
b) Az adatok biztonságos átvitele előkészítésének és tényleges átvitelének műszaki szabványait.
c) Adatvesztéssel kapcsolatos kötelezettséget és felelősséget.
d) Az adatátvitel során a biztonságos (szükség esetén rejtjelezett) környezet előírásait minden érintett félnél.
e) Az érzékeny adatok védelméhez szükséges speciális eszközök igénybe vételét (pl. kriptográfiai kulcsok).

8.7.2. Adathordozók szállítása

Az információ a fizikai szállítás során történő átvitel esetén ki van téve az illetéktelen hozzáférés és visszaélés veszélyének. A számítástechnikai adathordozók biztonsági szállítása érdekében az alábbi ellenőrző eszközök alkalmazását kell mérlegelni.

a) Szállítást – épületen kívül – csak a szervezeti egység vezetője rendelhet el.
b) A szállítást a szállított hordozók, adatok érzékenysége alapján mérlegelve szakcégre, vagy legalább két személyre kell bízni (különösen, ha a szállítás útvonala a cég telephelyein kívüli szakaszokat is tartalmaz).
c) Szállítás során átadás-átvételi bizonylat szükséges.
d) Épületen kívüli szállítás esetén a legrövidebb és leggyorsabb útvonalat kell kiválasztani.
e) Tömegközlekedési eszközön – lehetőség szerint – ne történjék adathordozó szállítása.
f) Épületen kívüli szállítás esetén – a MABISZ ajánlását figyelembe véve – megfelelő tárolóeszköz szükséges.
g) Elektronikusan rögzített adatokat tartalmazó mágneses adathordozó szállításkor elkerülendő a nyilvánvalóan erős mágneses tér (pl. nagyfeszültségű távvezetékek).
h) Szállítás során a vagyonbiztonság érdekében fokozott figyelemmel kell eljárni.
i) Az adathordozót tilos őrizetlenül hagyni.
j) Az adathordozókat óvni kell a fizikai sérülésektől.
k) Az adathordozókon a minősítést megváltoztathatatlanul kell feltüntetni.
l) Rendkívüli esemény esetén a szervezeti egység (a szállítást elrendelő) vezetőjét – szükség esetén a rendőrséget is – értesíteni kell. A vezetőnek haladéktalanul meg kell tennie a további károk elkerülése érdekében a szükséges lépéseket, valamint ezzel egy időben tájékoztatnia kell Az IT Igazgatót az eseményről és a megtett intézkedésekről.

8.7.3. Az elektronikus levelezés biztonsága

Az elektronikus levelezés biztonságának szabályozásakor a következő fenyegetettségeket kell figyelembe venni:

a) Az üzenetek illetéktelen elérésének vagy módosításának, illetve a szolgáltatás megtagadásának veszélye.
b) Emberi hibákból eredő veszélyeztető tényezők, pl. rossz címzés vagy irányítás.
c) Bizalmas adatok továbbításának lehetősége és ennek veszélyei.
d) A feladó és címzett hitelesítési problémák, illetve a levél átvételének bizonyítása.
e) A kívülről hozzáférhető címjegyzékek tartalmával való visszaélési lehetőségek.
f) Távolról bejelentkező felhasználó biztonsági problémái.

Az elektronikus levelezés biztonsági irányelvei:

a) A levelező rendszer vírusvédelmét folyamatosan frissíteni kell, valamint követni kell az új mail-vírusok megjelenését.
b) Az elektronikus levelező eszközök, elsősorban a szerverek fizikai és logikai védelméről folyamatosan gondoskodni kell. (pl. nyomon kell követni új szoftverfrissítések, service pack-ok és security-patch fájlok megjelenését.)
c) Az elektronikus levelező rendszeren keresztül történő támadások esetén, amennyiben a rendszer védelme átmenetileg nem biztosított, - pl. olyan vírus fenyegetettség esetében, amikor a vírusvédelmi rendszerek még nem nyújtanak kellő védelmet, - az intraneten kívül eső elektronikus levélforgalmat ideiglenesen le kell állítani. Ennek elrendelésére Az IT Igazgató jogosult.

d) Definiálni kell a felhasználók felelősségét, a BVK Holding Zrt. érdekeinek védelmében.
e) A külső partnereknek küldött bizalmas anyagokat (Auditjelentések, ajánlatok, szerződések, személyes és üzleti adatokat tartalmazó dokumentumok) titkosított mellékletként kell csatolni a levélhez.
f) Az elektronikus üzenetek bizalmasságának, illetve hitelességének védelme érdekében használt rejtjelező eszközt (PKI, kulcsok hosszát, tárolásuk módját) Az IT Igazgató engedélyezi.
g) Kilépéskor archiválni kell és a kilépés napjától számított 1 évig meg kell őrizni minden olyan felhasználó elektronikus levezését, akiknek munkaviszonya, illetve a jogosultság alapját képező megbízása, szerződése megszűnt. Megőrizendők továbbá azok az elektronikus levelek, amelyek peres eljárások alapját képezhetik.
h) A nem hitelesíthető, kétes forrásból származó üzeneteket ki kell vizsgálni.
i) Az elektronikus levelezés forgalmát tartalmilag szűrni kell, a bizalmas adatok kiszivárgásának elkerülése érdekében.
j) Minden felhasználót fel kell világosítani arról, hogy a BVK Holding Zrt. levelező rendszerén tárolt és továbbított levelek, a BVK Holding Zrt. tulajdonát képezik, ezért a BVK Holding Zrt. szabályzatokban és utasításokban feljogosított ellenőrző szerveinek ezekhez az állományokhoz, a vizsgálathoz szükséges mértékig betekintési joga van.
k) A BVK Holding Zrt. levelező rendszerét a cég üzletmenetétől idegen reklám, valamint egyéb üzleti célokra használni tilos.

A BVK Holding Zrt. elektronikus levelezési címjegyzéke nem szolgáltatható ki harmadik félnek, semmilyen célból.

9. Hozzáférés-menedzsment

9.1. A hozzáférés ellenőrzésének üzleti követelményei

Az adatok és az üzleti folyamatok elérését az üzleti és biztonsági követelmények alapján kell ellenőrizni. Ennek során meghatározásra kerültek az adatok elérésére, terjesztésére és engedélyezésére vonatkozó általános irányelvek.

9.1.1. Irányelvek és üzleti követelmények

Minden informatikai rendszer hozzáférési rendszerét a megvalósítási projekt során biztonsági osztálynak megfelelő követelményszinten kell megtervezni. Ebben pontos tartalmat kapnak a munkakörök, az objektumok és a hozzáférési módok, melyek meghatározásához a következőket kell figyelembe venni:

a) Az egyes üzleti alkalmazások biztonsági követelményeit.
b) Az üzleti alkalmazásokra vonatkozó összes adat azonosítását.
c) Az adatok terjesztésére és engedélyezésére vonatkozó irányelveket, azaz a "need to know" elvet, a biztonsági szinteket és az adatminősítés alkalmazását.
d) A különböző rendszerek és hálózatok hozzáférés ellenőrző eszközeit és az adat minősítésére vonatkozó irányelvek közötti összhang megteremtését.
e) Az adatok és szolgáltatások elérésének védelmére vonatkozó törvényi rendelkezéseket, társasági szabályzatokat és a szerződésekben rögzített szabályokat.
f) Azonos munkavállalói csoportokra vonatkozó egységes irányelveket.
g) Hozzáférési jogok kezelését a kapcsolatok összes típusát felismerő osztott és hálózatba szervezett környezetben.

9.1.2 A biztonságkritikus munkakörök szétválasztása.

Törekedni kell a rendszerek üzemeltetése során a least privilege elvre. amely a kockázatok csökkentésére a legkevesebb jogosultsággal működik

Erőforrások / Funkciók	Alkalmazás			Adatbázis hozzáférés			Program kódok		
	Éles	Teszt	Fejlesztői	Éles	Teszt	Fejlesztői	Éles	Teszt	Fejlesztői
Felhasználó	Igen	Igen	Nem	Nem	Nem	Nem	Nem	Nem	Nem
Rendszergazda	Nem	Nem	Nem	Nem	Nem	Nem	Igen	Igen	Nem
Programozó	Nem	Nem	Igen	Nem	Nem	Igen	Nem	Nem	Igen
Alkalmazásgazda	Igen	Igen	Nem	Nem	Nem	Nem	Nem	Nem	Nem
Adatbázis adminisztrátor	Nem	Nem	Nem	Igen	Igen	Igen	Nem	Nem	Nem

9.1.3. A hozzáférés ellenőrzésének szabályai

a) A szabad belátás elve (DAC) szerint kialakított hozzáférés-vezérlésnél a felhasználóknak az adatállományokhoz fűződő jogosultságai egyedi elbírálás alapján személyenként vagy csoportonként kerülnek meghatározásra.

b) Az előre meghatározott munkakörök (szerepkörök) szerinti hozzáférés jogosultság-vezérlés esetében az előre meghatározott felhasználói szerepkörökhöz, valamint az informatikai rendszer adatállományaihoz és erőforrásaihoz biztonsági címkéket kell hozzárendelni, amelyek tartalmát (adatcsoportok, adatvédelmi szintek, hozzáférési jogok) előre meghatározott módon kell kialakítani. Az egyes felhasználók eltérő szerepkörbe sorolhatók és megkapják a szerepkörhöz rendelt jogokat. A hozzáférés jogosságának elbírálása az adott szerepkör, illetve a hozzáférésre megcélzott adatállomány, erőforrás biztonsági címkéinek összehasonlításával történik. A szerepkör szerint meghatározott hozzáférés-jogosultság kiosztás (MAC) használata a fokozott és a kiemelt biztonsági osztályokban kötelező.

c) Mindegyik informatikai rendszernél a minimálisan használandó szerepköröket, valamint az azokhoz tartozó legjellemzőbb funkciókat külön-külön kell meghatározni. A szerepkörök tartalmát az SZMSZ-ben (Szervezeti és Működési Szabályzat) és más utasításokban előírt munkakörök, valamint ezeknek a szervezeti hierarchiában elfoglalt helye határozza meg.

d) A szerepkörök az informatikai rendszerek védelmi rendszerterveiben nyernek konkrét értelmezést és szükség esetén azok további rész-szerepkörökre oszthatók.

e) Az informatikai rendszerrel dolgozó minden munkatárs a védelmi rendszertervben konkrétan meghatározott szerepkörbe sorolandó és örökli a szerepkörre meghatározott hozzáférési jogokat.

f) A munkaköröktől történő eltérést a tervezés során a projekt vezetőjének, az üzemeltetés során Az IT Igazgatónak kell meghatározni és jóváhagyatni az adatgazdával.

9.2. A felhasználói hozzáférés menedzsmentje

Az információs rendszerek illetéktelen elérésének megakadályozása, érdekében megfelelő hozzáférési ill. hozzáférés ellenőrző rendszert kell kialakítani. Hozzáférés csak dokumentáltan kérhető.

Minden szerepkör engedélyezés esetén az engedély jogosultságot biztosít meghatározott fizikai, illetve logikai biztonsági zónába (pl. számítóközpont, szerverszoba, archiváló helyiség, illetve adott alkalmazás, hálózati szegmens, munkahelyi állomás stb.) történő belépésre és abban az engedélyezett fizikai, illetve logikai objektumokhoz való hozzáférésre.

Hivatalos eljárásokkal kell szabályozni az információs rendszerekre és szolgáltatásokra vonatkozó hozzáférési jogok kiosztásának ellenőrzését.
Az eljárásoknak ki kell terjedniük a felhasználói hozzáférés életciklusinak minden egyes szakaszára, az új felhasználók kezdeti bejelentkezésétől az olyan felhasználók kijelentkezéséig, akik többé már nem igénylik az információs rendszerek és szolgáltatások elérését. Külön figyelmet érdemel az elsőbbségi hozzáférési jogok kiosztása, melyek lehetővé teszik, hogy egyes felhasználók megkerüljék a rendszer ellenőrző eszközeit.

9.2.1. A felhasználók bejelentkezése

Szükség van olyan hivatalos be- és kijelentkezési eljárásra, amely alapján az összes többfelhasználós rendszerben és szolgáltatásnál lehet szabályozni a felhasználók hozzáférését. A felhasználó-azonosító olyan legyen az informatikai rendszerben, hogy az informatikai rendszert használó identitására vonatkozóan legyen egyedi, jellemző, ellenőrizhető és rendelkezzen hitelesítésre alkalmas megjelenítéssel. A felhasználók közé tartoznak a természetes személyek, folyamatok, vagy egyéb eszközök egyaránt. Az egyedi felhasználói azonosítót a hozzáférés szabályozására, az adatok és az információk védelmére, valamint a hitelesítés támogatására kell felhasználni. Biztosítani kell, hogy a felhasználó azonosítója az egyes erőforrásokhoz, folyamatokhoz és az adatokhoz való hozzáférést megfelelően szabályozza (korlátozza) és követhető, ugyanakkor a biztonsági funkciók működése során ez ellenőrizhető legyen a biztonsági rendszer számára.

a) A felhasználó-azonosítónak minden esetben egyedinek kell lennie, (azaz semmilyen körülmények között sem adható ki különböző felhasználók részére megegyező azonosító).
b) A felhasználói azonosítók képzésére központi névkonvenciós szabályt kell felállítani. A felhasználói azonosítók képzését a BVK Holding Zrt.-n belül, egy helyen kell végrehajtani
c) A felhasználói azonosítók és jogosultságok rendszerében bekövetkezett mindennemű változást (az ellenőrizhetőség érdekében) naplózni kell.
d) Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakör ellátásához szükséges minimális funkcióelérést biztosíthatják.
e) A felhasználói azonosítók nem örökérvényűek. Ennek megfelelően a következő szabályokat kell alkalmazni:
    1) A BVK Holding Zrt. munkatársai, illetve külső munkavállalói – amennyiben munkakörük, illetve beosztások alapján, az informatikai rendszer szolgáltatásait igénybe vehetik – munkába állásuk után haladéktalanul kapják meg felhasználói azonosítójukat. Az utasítási jogkört gyakorló vezető –

legalább 3 munkanappal– a munkába lépés előtt igényelje meg a felhasználói azonosítót a hozzáférési jogosultságok megjelölésével. Tilos, akár csak átmeneti jelleggel is, a saját azonosítójuk hiánya miatt más dolgozó azonosítóját használni. A kapott felhasználói azonosítót haladéktalanul érvényesíteni kell,

2) a BVK Holding Zrt. dolgozóinak felhasználói azonosítóját munkaviszonyuk megszűnésével, a külső munkavállalók felhasználói azonosítóját megbízatásuk lejártával, haladéktalanul le kell tiltani. Akinek munkaviszonya megszűnt a rendszer szolgáltatásait nem veheti igénybe, és erőforrásait nem használhatja.
3) a munkaviszonyukat huzamosabb ideig szüneteltető (pl. gyermek szülése), illetve a tartósan más okból távollévő (külföldi kiküldetés, elhúzódó gyógykezelés) dolgozók felhasználói azonosítóját le kell tiltani, illetve munkába állásukkal egy időben ismét engedélyezni kell,
4) a dolgozók áthelyezése kapcsán felmerülő jogosultsági változásokat (megszűnő felhasználói azonosítók letiltása, vagy a jogosultságok törlése, illetve új azonosítók vagy jogosultságok létrehozása) az áthelyezéssel egy időben haladéktalanul át kell vezetni,
5) harmadik személyek, akik valamilyen okból igénybe vehetik a BVK Holding Zrt. bármelyik rendszerének szolgáltatásait, csak meghatározott időre, és korlátozott lehetőségeket biztosító (pl. egy adott projekt keretein belül érvényes) felhasználói azonosítót kaphatnak. A részükre kiadott azonosító szerkezetileg feleljen meg a szervezeten belüli dolgozók azonosítójával, de legyen egyértelműen és könnyen megállapítható, hogy az adott felhasználói azonosító harmadik (külső) személyé.
6) azokban a rendszerekben, amelyek regisztrálják a felhasználó utolsó bejelentkezésének időpontját, ha egy felhasználó azonosító 30 napot meghaladóan inaktívnak bizonyul (azaz a felhasználó a rendszer szolgáltatásait ez idő alatt egyszer sem vette igénybe), azonosítóját le kell tiltani, és erről a dolgozó munkahelyi vezetőjét értesíteni szükséges, megjelölve az érvénytelenítés okát
7) a szervezeti egység vezetőjének haladéktalanul kezdeményezni kell Az IT Igazgatónál a kilépő dolgozó összes azonosítójának letiltását.

9.2.2. A jogosultságok kezelése

Az egyes biztonsági osztályokban a következő a standard jogosultságokat kell értelmezni:

Alapbiztonsági osztály

1) Ebben az osztályban minimálisan a következő jogokat kell megkülönböztetni:
   - olvasási jog (betekintés),
   - létrehozási jog,
   - módosítási jog,
   - törlési jog.
2) A hozzáférés-jogosultság vezérlésére a szabad belátás szerint kialakított hozzáférés (DAC) elvét kell alkalmazni.
3) Az adminisztrációs és naplózási jogoknak el kell különülni a felhasználói jogoktól.
4) A rendszernek alkalmasnak kell lennie a hozzáférési jogok egyedi vagy csoport szinten való megkülönböztetésére és szabályozására. A hasonló szerepű személyek csoportjai munkájának támogatására hozzáférési jogosultságcsoportokat kell kialakítani.

Fokozott biztonsági osztály

1) Ebben az osztályban minimálisan a következő jogokat kell megkülönböztetni:
   - olvasási jog (betekintés),
   - létrehozási jog,
   - módosítási jog,
   - törlési jog (selejtezés),
   - másolási jog.
2) A hozzáférés-jogosultság vezérlésére a szerepkör szerinti hozzáférés (MAC) elvét kell alkalmazni, valamint a biztonsági adminisztrátori szerepkört elkülönítetten kell létrehozni.
3) A biztonsági naplóállományokat a rendszer szintű IBSZ-ben meghatározott módon, két példányban, időszakosan, és elkülönítetten tárolt, egyszer írható adathordozóra kell archiválni.
4) A felhasználók azonosítására és hitelesítésére az egyedileg meghatározott jelszó használatán kívül – kötelezően az adott rendszerhez és a belépő személyhez kötött –kiegészítő azonosító-hitelesítő eszközt, pl. chipkártyát kell használni.

Kiemelt biztonsági osztály

1) Ebben az osztályban az informatikai rendszer objektumaihoz legalább a következő hozzáférési módokat kell hozzárendelni:
   - olvasási jog (betekintés),
   - létrehozási jog,
   - módosítási jog,
   - selejtezési jog,
   - törlési jog,
   - másolási jog.
2) A rendszerrel kapcsolatba kerülő személyekhez a következő hozzáférési módokat kell hozzárendelni:
   - engedélyezési jog,
   - visszavonási jog,
   - olvasási jog (betekintés),
   - létrehozási jog,
   - módosítási jog,
   - selejtezési jog,
   - törlési jog,
   - másolási jog,
3) A hozzáférés-jogosultság vezérlésére szerepkör szerint meghatározott hozzáférési jogosultság kiosztás (MAC) elvét kell alkalmazni.
4) A konkrét jogosultságokat és a hozzáférés-jogosultság vezérlésének konkrét megvalósítási módját az 1-3. pontban rögzítettek alapján az alkalmazásra kerülő hardver-szoftver termékek lehetőségeinek figyelembevételével kell kialakítani.
5) A munkakörökre a fokozott biztonsági osztálynál elmondottak érvényesek azzal a szigorítással, hogy a rendszeradminisztrátor, az operátor és a biztonsági adminisztrátor szerepköröket személyileg is szét kell választani.
6) A biztonsági naplóállományokat kettőzötten, az Üzemeltetési főosztályvezető és Az IT Igazgató által közösen meghatározott módon kell archiválni.
7) A felhasználók azonosítására és hitelesítésére az egyedileg meghatározott jelszó használatán kívül – az adott rendszerhez és a belépő személyhez elválaszthatatlanul kötött és minősített – kiegészítő azonosító-hitelesítő eszközt kell használni.

8) A BVK Holding Zrt. informatikai rendszereihez való hozzáférési jog megadása BVK Holding Zrt. dolgozók részére csak jóváhagyott igény esetén lehetséges.
8) A BVK Holding Zrt. informatikai rendszeréhez való hozzáférési jog megadása alvállalkozók részére csak előzetes írásbeli engedély alapján lehetséges

9.2.3. A felhasználói jelszavak kezelése

Az informatikai rendszerekben a felhasználók hitelesítésének alapvető módja a jelszó megadása.

A felhasználói jelszavak kezelésére a következő szabályok a mérvadók:

a) A felhasználónak kötelezően alá kell írnia egy nyilatkozatot, melyben felelősséget vállal személyes, (esetleg csoportos jelszavainak) bizalmas kezelésére.
b) Belépéskor megkapott, illetve – pl., elfelejtés esetén – ideiglenes jelszó átadása csak biztonságos csatornán történhet, a felhasználó előzetes (pl. Személyes) azonosítása után. Az ideiglenes jelszavak csak az adott munkanap végéig lehetnek érvényesek, megváltoztatásuk kötelező.
c) Telefonon, illetve elektronikusan aláíratlan e-mailen történő kérésre, jelszóváltoztatás nem kezdeményezhető.
d) A felhasználónak minden esetben vissza kell igazolnia új jelszavának az átvételét ellenőrizhető úton (pl., e-mail), vagy személyesen
e) A jelszónak minden felhasználó számára szabadon megváltoztathatónak kell lennie.
f) A felhasználói jelszavakkal kapcsolatban, (amennyiben az adott rendszerben erre lehetőség van) biztosítani kell a következő követelmények teljesülését.
   1) minimális jelszóhossz megadása
   2) a jelszó egyediségét (történeti tárolás),
   3) a központi jelszó megadás utáni első bejelentkezéskor a kötelező jelszó cseréjét,
   4) a jelszó maximális élettartamát,
   5) a jelszó minimális élettartamát,
   6) a jelszó zárolását,
   7) a jelszó képzési szabályainak meghatározását.
g) A számítógépes rendszerekben a jelszavakat tilos nyílt formában tárolni. A jelszófájlokat megfelelő rejtjelezés védelemmel kell ellátni.
h) A jelszavakat vagy a jelszófájlokat a hálózaton nyílt, olvasható formában továbbítani tilos.
i) A felhasználói jelszó szerkezeti szabályaival (bonyolultság) szemben támasztott követelményeket minden esetben az határozza meg, hogy milyen a kiszolgálón tárolt adatok érzékenységi besorolása és ebből következően a kiszolgáló informatikai biztonsági osztályba sorolása.

A felhasználó azonosítók és jelszavak rejtjelezetlen formában való tárolása a BVK Holding Zrt. rendszereiben szigorúan tilos! Felhasználói azonosítók, jelszavak, rejtjelező kulcsok és az ehhez tartozó jelszavak biztonsági másolatai lezárt, lepecsételt borítékban, minimum zárható lemez- vagy páncélszekrényben tárolhatók. A lezárt borítékot a lezárónak alá kell írni, a lezárás dátumának feltüntetésével.

9.2.4. A felhasználó hozzáférési jogosultságainak ellenőrzése

Az informatikai rendszerekben biztosítani kell, hogy a felhasználók tényleges hozzáférési jogosultsága a szerepkörüknek megfelelő legyen. Ennek érdekében

a) A jogosultságokat rendszeres időközönként ellenőrizni kell. Az általános felhasználók esetében ezt évente, míg a kiemelt jogosultsággal rendelkező felhasználók esetében legalább 3 havonta kell megtenni.
b) Rendszeresen ellenőrizni kell, hogy privilegizált jogokkal csak egyedileg azonosítható felhasználók, csoportok és eszközök rendelkezhessenek.
c) A szerepkörök változásakor a hozzáférési jogosultságokat felül kell vizsgálni és az új szerepkörnek megfelelően módosítani kell.
d) Az ellenőrzést a szervezeti egység vezetője által kijelölt személy végzi el, és az ellenőrzések eredményéről a negyedéves jelentésében számol be Az IT Igazgatónak.

9.3. A felhasználó feladatai

Meg kell akadályozni az illetéktelen felhasználói hozzáférést az informatikai rendszer erőforrásaihoz.

A biztonság hatékonyságához nélkülözhetetlen az engedéllyel rendelkező felhasználók együttműködése.
A felhasználóknak ismerniük kell a hozzáférés hatékony ellenőrzésére alkalmas eszközök használatát, különös tekintettel a jelszavak használatára és a felhasználó kezelésében lévő berendezések biztonságára.

9.3.1. A jelszó használata

A BVK Holding Zrt. informatikai rendszereit használó valamennyi felhasználónak a következő jelszóhasználati szabályokat kell betartania:

a) A jelszavakat bizalmasan kell kezelni, azok más személyeknek nem adhatók meg, nyilvánosságra nem hozhatók.
b) A jelszavakat – a biztonsági másolat kivételével – nem szabad felírni, papíron tárolni. Amennyiben ez elkerülhetetlen (pl. a kezdeti jelszó), ekkor gondoskodni kell a jelszó zárt, un Biztonsági borítékban történő tárolásáról. Ezektől eltérően a legmagasabb jogosultságot biztosító felhasználói azonosítók esetén a jelszavakat kötelező zárt borítékban, két példányban, azokat két különböző helyen, lemez- vagy páncélszekrényben tárolni.
c) Amennyiben a felhasználó azt gyanítja, hogy jelszavát valaki megismerte, azonnal le kell azt cserélnie.
d) A jelszó minimális hossza 8 karakter, rendszergazdák esetében 10 karakter.
e) A jelszónak tartalmaznia kell legalább egy kisbetűt, egy nagybetűt és egy számot, rendszergazdák esetében speciális karaktert is.
f) A jelszó kívülálló számára ne legyen egyszerűen kitalálható, ne tartalmazzon a felhasználó személyére utaló információkat (pl. neveket, telefonszámokat, születési dátumokat), összefüggő szövegként ne legyen olvasható.
g) Legalább 3 havonta rendszeresen cserélni kell a rendszerben használt felhasználói jelszavakat, kerülve a korábban használt jelszavak ismételt vagy ciklikus használatát.
h) Első bejelentkezés alkalmával a kötelező jelszócserét végre kell hajtani.
i) Automatikus bejelentkezési eljárások (pl., batch fájlok, vagy funkcióbillentyűhöz rendelt makrók) nem tartalmazhatnak felhasználói jelszót.
j) Amennyiben a munkaállomásokon a hitelesítési folyamatban a beírt jelszó olvasható (az alkalmazás nem rejti el megfelelően a jelszót), az alkalmazás üzemeltetőjének figyelmeztetése alapján, a felhasználó köteles gondoskodni arról, hogy más illetéktelen személy ne láthassa meg az általa beírt jelszót.

A biztonságos jelszóhasználat szabályait minden felhasználónak oktatni kell.

A felhasználókkal tudatosítani kell, hogy mindazon műveleteket, melyeket az ő azonosítójával és jelszavával mások hajtanak végre, az informatikai rendszer az ő "terhére' könyveli el, és azokért személyesen felel.

Amennyiben a felhasználó multiplatformos környezetet, vagy több hitelesítést igénylő alkalmazást használ, lehetőség van felhasználó számára egyetlen, kellő hosszúságú és bonyolultságú jelszó alkalmazására az összes rendszeren. (A multiplatformos rendszerekben használatos jelszó hossza min. 12 karakter, ezen kívül vegyesen tartalmaznia kell alfabetikus és numerikus karaktereket is.) Az ilyen jelszavaknál fokozottan ügyelni kell arra, hogy ne tartalmazzanak egymást követő azonos karaktereket.

9.3.2. Felügyelet nélküli informatikai berendezések védelme

A felhasználóknak gondoskodniuk kell a felügyelet nélkül hagyott eszközök megbízható védelméről. A felhasználó helyiségeiben felállított és a hosszabb időre felügyelet nélkül hagyott berendezéseknél – többek között munkaállomásoknál vagy szervereknél – külön védelem szükséges az illetéktelen hozzáférés megakadályozására. Mindegyik felhasználónak és harmadik személynek meg kell ismernie a felügyelet nélkül hagyott berendezésékre vonatkozó biztonsági követelményeket és eljárásokat, valamint a védekezés megvalósítására vonatkozó saját felelősségüket. A felhasználókat tájékoztatni kell a következőkről:

a) Az informatikai rendszerekhez csak olyan kihelyezett terminál funkció használata engedélyezhető, melynek működése az informatikai rendszerből menedzselhető (beleértve a jogosultságok vezérlését is), továbbá abból szükség esetén kizárható. A központi védelmi funkciók és a távoli csatlakozó berendezés védelmi funkcióinak együttes megléte alapvető feltétele a távoli hozzáférési jog engedélyezésének.
b) Azokban a rendszerekben, ahol lehetőség van rá, biztosítani kell a hosszabb ideig inaktív munkaállomások rendszer által kényszerített kijelentkezését, vagy a berendezés blokkolását (lock), például a PC-s munkaállomásoknál alkalmazni kell a jelszóval kombinált képernyővédő funkciót (A munkaállomáshoz történő visszatéréskor a képernyővédő funkció feloldása csak sikeres jelszó megadása után legyen lehetséges.)
c) A PC-s terminál használata esetén, a PC használatát a nem azonosított és hitelesített felhasználók számára tiltani kell.

9.4. A hálózati szintű hozzáférések menedzsmentje

A hálózatba szervezett szolgáltatások védelme érdekében a rendszerszintű IBSz-ekben szabályozni és ellenőrizni kell a belső és külső hálózatba szervezett szolgáltatások elérését annak érdekében, hogy hozzáférési jogosultsággal rendelkező felhasználók ne veszélyeztethessék a hálózatba szervezett szolgáltatások biztonságát. Ellenőrizni kell a belső és külső hálózatokban működő szolgáltatások elérését.

Az ellenőrzés és a menedzselés eszközei a következők:

a) Megfelelően biztonságos kapcsolatok létesítése a szervezet hálózata és más szervezetek tulajdonában levő hálózatok vagy nyilvános hálózatok között.
b) A felhasználók és az eszközök hitelesítésének mechanizmusa.

c) Az informatikai szolgáltatások felhasználóinak menedzselése, hozzáférésük vezérlése.

9.4.1. A hálózati szolgáltatások használatának irányelvei

A hálózatba szervezett szolgáltatásokhoz való nem eléggé biztonságos csatlakozások hatással lehetnek a szervezet egészére. A felhasználók közvetlenül csak azokhoz a szolgáltatásokhoz férhessenek hozzá, amelyekre engedélyük kifejezetten vonatkozik. Ez az ellenőrzés különösen fontos az érzékeny vagy kritikus alkalmazásokhoz való hálózati csatlakozások vagy a különösen nagy kockázattartalmú helyen tevékenykedő felhasználók – többek között olyan nyilvános vagy külső területek – esetében, amelyek kívül esnek a szervezet biztonsági irányításán és ellenőrzésén.

a) A hálózatok és a hálózati szolgáltatások használata során a következő tényezőkre kell figyelni:
   1) meg kell határozni az engedélyezett hálózatok, valamint az engedélyezett hálózati szolgáltatások elérési kritériumait,
   2) az engedélyezési eljárás során meg kell határozni az engedélyezett hálózatokat és hálózati szolgáltatásokat, valamint azokat a személyeket, eszközöket, alkalmazásokat, melyek valamiképpen kapcsolatba kerülnek a hálózatokkal és a hálózati szolgáltatásokkal.
   3) menedzselési és ellenőrzési eljárásokat kell kialakítani.

Az 1-3. alpontok a rendszerszintű IBSZ-ben kerülnek részletesen kidolgozásra.

b) Ezen pontoknak összhangban kell lenniük a már eddig megfogalmazott, azonosításra, hitelesítésre, hozzáférés szabályozására, bizalmasság-megőrzésre és az ellenőrzésre vonatkozó szabályokkal. Mindegyik igény esetében vagy a formalizált hálózati elérésekkel kapcsolatos szabályok, vagy pedig az adott esetre kidolgozott speciális elvárások alapján kell az irányelveket kidolgozni.
c) Az elektronikus úton továbbított üzenetek, állományok tekintetében is az ügyviteli (iratkezelési) szabályzatnak megfelelően kell eljárni.
d) A felhasználók számára a hálózati erőforrások használatát, a munkájukat nem veszélyeztető mértékig, korlátozni kell.
e) Az adatvesztés és sérülés elkerülése érdekében hibadetektáló és javító eljárásokat kell alkalmazni.
f) A hálózat elosztott és diszkrét elemeit rendszeresen ellenőrizni kell annak érdekében, hogy a hálózatban a hálózati forgalom monitorozására és rögzítésre alkalmas erőforrást ne használják illetéktelenül.

9.4.2. Felhasználó azonosítása, hitelesítése távoli kapcsolatnál

A külső kapcsolatok magukban rejtik az üzleti információk illetéktelen elérésének veszélyét, többek között a tárcsázás módszerével. Ezért a távoli felhasználók hozzáférését hitelesítéshez kell kötni. A kriptográfiai technikákra alapozott módszerek lehetővé teszik a felhasználók megbízható hitelesítését. Kockázatelemzés alapján fel kell mérni a védelem szükséges mértékét, annak érdekében, hogy kiválasztható legyen a hitelesítés megfelelő módszere.

Különös gonddal kell ügyelni arra, hogy a távoli felhasználó vagy eszköz hitelesítésére szolgáló eljárás saját védelme ne legyen a védett adatokénál magasabb, tehát ne a védelemi adat maga legyen a „legértékesebb" megszerezhető értesülés.

A távoli felhasználók hitelesítése megoldható többek között kriptográfiai technikával, gépi jelzéssel vagy kérdés/felelet protokollal. A csatlakozások forrásának ellenőrzése kiválasztott magánvonalakkal vagy hálózati felhasználói címek ellenőrzésére alkalmas eszközökkel is lehetséges.

Mindegyik felhasználói igény esetében vagy a formalizált hálózati elérésekkel kapcsolatos szabályok, vagy pedig az adott esetre kidolgozott speciális elvárások alapján kell az irányelveket kidolgozni. A felhasználókkal a szolgáltatások indítása, vagy az azokkal történő kommunikáció megkezdése előtt végre kell hajtani a hitelesítési eljárást.

Az adott hálózati alrendszer hitelesítési mechanizmusa nem érintheti a hálózat többi alrendszerének hitelesítési rendszerét.

A hálózati erőforrások használatát a felhasználók számára korlátozni kell.
Megosztott erőforrások csak azonosítás után legyenek elérhetők. Munkaállomások megosztását (azok védelmének nehézsége miatt) kerülni kell.

Csak a kellően biztonságos környezettel, technikákkal biztosított helyeken lehet a távoli elérést biztosítani. Távoli elérésre külön kezelt felhasználói csoportot kell kialakítani.

9.4.3. Távoli munkaállomás azonosítása, hitelesítése

Egy távoli számítógéphez való automatikus csatlakozás lehetősége egy üzleti alkalmazáshoz való illetéktelen hozzáférést tehet lehetővé, ezért a számítástechnikai rendszerekhez távolról való összes csatlakozást hitelesíteni kell. Ez különösen fontos akkor, ha a csatlakozás egy olyan hálózatot használ, amely kívül esik a szervezet biztonsági rendszerének ellenőrzésén.

9.4.4. A hálózatok biztonsági szegmentálása

A nagy hálózatok biztonságának ellenőrzésére alkalmas módszerek egyike a hálózatok felosztása önálló (belső és külső) logikai hálózati struktúrákra, ezek mindegyikét egy meghatározott biztonsági gyűrű (háló) védi. Ez kialakítható, többek között oly módon is, hogy a két összekapcsolható hálózat között egy biztonsági kapu ellenőrzi a hozzáférést és a két struktúra közötti információáramlást. Ennek a konfigurációnak alkalmasnak kell lennie a két struktúra közötti forgalom szűrésére, valamint – a BVK Holding Zrt. hozzáférést ellenőrzési irányelveinek megfelelően – az illetéktelen hozzáférés megakadályozására. Az ilyen kapu egyik jellemző példája a tűzfal.

A hálózatok elkülönítésének kritériumait a hozzáférés ellenőrzésére vonatkozó irányelvek és a hozzáférési igények alapján kell kialakítani: aminek során figyelembe kell venni a megfelelő hálózati útvonal-kiválasztási vagy kapuzási technológia tényleges és fajlagos költségeit és a teljesítményre gyakorolt hatását.

9.4.5. A hálózatra való csatlakozások ellenőrzése

Az osztott hálózati munka, különösen a több szervezet által használt hálózat biztonsága szükségessé teszi bizonyos ellenőrző eszközök alkalmazását a felhasználók csatlakozási lehetőségeinek korlátozására. (Ezeket a forgalomszűrő, ellenőrző lehetőségeket amennyiben szükséges, a gateway és operációs rendszeri beállításánál alkalmazni kell.)
Korlátozó rendelkezéseket többek között az alábbi esetekben célszerű alkalmazni:

a) Elektronikus levelezés.
b) Egyirányú adatállomány mozgatás (pl. mentési rendszerek esetében).
c) Adatállomány mozgatása mindkét irányban.
d) Meghatározott időponthoz kötött hálózati hozzáférés.

9.5. A hálózati szolgáltatások biztonsága

Mivel a különböző hálózatok szolgáltatásainak kínálata rendkívül széles, jelentős részük még számos többletszolgáltatással rendelkezik, ezért fontos, hogy a rendszer telepítése során csak azokat a hálózati szolgáltatásokat implementáljuk a rendszerbe, melyekre az üzemeltetéshez feltétlen szükség van. A feleslegesen felinstallált hálózati szolgáltatások, protokollok esetleges biztonsági rések előfordulását megnövelhetik. A rendszerüzemeltetőnek minden esetben fel kell mérnie, és minden részletre kiterjedően dokumentálnia kell az általa alkalmazott hálózati szolgáltatás egyedülálló, illetve összetett biztonsági jellemzőit. Amennyiben több hálózati szolgáltatás működik a rendszerben, úgy ezek egymásra gyakorolt hatását is elemezni kell biztonsági szempontból. A hálózati szolgáltatások biztonsági beállítása, valamint annak ellenőrzése, karbantartása a hálózatot üzemeltető Kommunikációs terület feladata.

9.5.1. Az operációs rendszer szintű hozzáférések ellenőrzése

Az informatikai eszközök illetéktelen elérésének megakadályozása érdekében az operációs rendszer szintjén rendelkezésre álló biztonsági lehetőségeket is fel kell használni a számítástechnikai erőforrásokhoz való hozzáférés korlátozásához. Ezeknek a következőket kell lehetővé tenniük:

a) Az engedéllyel rendelkező felhasználó személyének azonosítása és hitelesítése, szükség esetén a terminál vagy csatlakozási hely azonosítása.
b) A sikeres és az eredménytelen hozzáférési kísérletek rögzítése.
c) Megfelelő hitelesítési eszközök és – jelszókezelő rendszer használata esetén – minőségi jelszavak biztosítása.
d) Adott esetben a felhasználók csatlakozási idejének korlátozása.

Amennyiben az üzleti kockázatok alapján ez indokolt, más hozzáférést vezérlő módszerek (pl. ujjlenyomat, chipkártya, kérdés-felelet) is alkalmazhatók.

9.5.2. Bejelentkezési, hitelesítési eljárások

A számítógéprendszerbe való bejelentkezési folyamatnak minimumra kell csökkentenie az illetéktelen hozzáférés lehetőségét.

a) Ennek során csak a bejelentkezés eredményes befejezése után jelenhet meg a használni kívánt rendszerre vonatkozó adat, azonosító stb.
b) A bejelentkezés elfogadására vagy elvetésére csupán az összes szükséges adat megadása után kerülhet sor; sikertelenség esetén nem jelölheti meg a hibás, elrontott azonosítót, jelszót.
c) Korlátozni kell az eredménytelen bejelentkezési kísérletek számát, rögzíteni kell az eredménytelen kísérleteket, időtúllépés esetén meg kell szüntetni az adatátviteli kapcsolatot.

9.5.3. A felhasználó azonosítása, hitelesítése

Biztonságos bejelentkezési folyamatot kell kialakítani, melynek során

a) Az azonosítás és hitelesítés keretében a hozzáférési jogosultságot jelszavakkal kell ellenőrizni. A jelszómenedzselést úgy kell biztosítani, hogy a jelszó ne juthasson illetéktelenek tudomására, ne legyen megkerülhető, illetve könnyen megfejthető.
b) A felhasználók azonosítása egyedi, jellemző, ellenőrizhető és hitelesítésre alkalmas kell, hogy legyen.
c) A munkakör megváltozásakor a felhasználók hozzáférési jogosultságait felül kell vizsgálni, és ennek alapján módosítani kell.
d) Biztosítani kell a felhasználói azonosítók időszakos vagy végleges letiltásának lehetőségét.
e) A rendszer hozzáférés szempontjából meghatározó erőforrásaihoz (pl. fájlok, tároló területek, berendezések stb.) olyan egyedi azonosítókat kell rendelni, amelyek a hozzáférési jogosultság meghatározásának alapjául szolgálnak.

9.5.4. A jelszókezelő rendszer

A jelszavak rendszerszintű kezelését az adott operációs rendszer vagy alkalmazási rendszer beépített jelszókezelési rendszere végzi.

A jelszókezelő rendszerrel szemben támasztott alapvető követelmények:
a) A számonkérhetőség fenntartása érdekében ki kell, hogy kényszerítse az egyéni kulcsszavak használatát, és megadott időközönként azok cseréjét.
b) Minden felhasználó számára biztosítania kell, a szabad jelszóváltoztatás lehetőségét.
c) Kényszerítse ki a kellő biztonsági szintnek megfelelő jelszavak használatát.
d) Központi jelszó megadás utáni első bejelentkezéskor kötelező a jelszócsere.
e) Jelszó egyediségét valamint történeti tárolását biztosítani kell. (pl. a jelszókezelő rendszer nyilvántartást vezet az eddig alkalmazott jelszavakról, és megakadályozza a korábbiak felhasználását.)
f) Bejelentkezési folyamat során, a képernyőn rejtse el a jelszót.
g) A számítógépes rendszerben tárolt jelszavakat, jelszófájlokat az alkalmazások adataitól elválasztva, megfelelő rejtjelezési védelemmel ellátva kell tárolni.
h) Biztosítson lehetőséget a következők beállítására:
   1) minimális jelszóhossz megadása,
   2) a jelszavak képzési szabályainak meghatározása,
   3) jelszó élettartam,
   4) a jelszó felfüggesztés, letiltás.

A felhasználói jelszó szerkezeti szabályaival (bonyolultság) szemben támasztott követelményeket a rendszer szintű IBSz határozza meg.

9.6. Alkalmazás szintű hozzáférések vezérlése

Az illetéktelen hozzáférés megakadályozására a felhasználói rendszereken belül biztonsági eszközöket is kell alkalmazni. A programok és az adatok logikai hozzáférését minden esetben az engedéllyel rendelkező felhasználókra kell korlátozni. A felhasználói rendszerekben:

a) A mindenkori hatályos üzleti hozzáférési irányelveknek megfelelően ellenőrizni kell az adatokhoz és a felhasználói rendszer funkcióihoz való felhasználói hozzáférést.

b) Védelmet kell nyújtani az illetéktelen hozzáféréssel szemben minden segédprogram és operációs rendszerprogram számára ott, ahol meg lehet kerülni a rendszer vagy az alkalmazás ellenőrző eszközeit.
c) Nem szabad befolyásolnia olyan más rendszerek biztonságát, amelyekkel az adott rendszer megosztva használ különböző informatikai erőforrásokat.

9.6.1. Az adatelérés szabályozása

Abban az esetben, amennyiben azt a kialakított rendszer sajátossága szükségessé teszi, az alkalmazás szintjén is szabályozni kell az adatelérést (pl. megfelelő menük alkalmazásával, a dokumentációhoz és a rendszer funkciókhoz való hozzáférés szelektívé tételével stb.). További elvárások az operációs rendszerek felhasználóinak azonosításával, hitelesítésével kapcsolatos pontban részletezettek.

9.6.2. Érzékeny adatokat kezelő rendszer elkülönítése

Érzékeny adatokat csak azon személyek kezelhetnek, akiket erre az SZMSZ által kijelölt vezetők feljogosítanak, továbbá rendelkeznek a megfelelő jogosultságot biztosító felhasználói azonosítóval, a hitelesítést lehetővé tevő jelszóval és – szükség esetén – további azonosításra alkalmas eszközzel.

A különlegesen érzékeny adatok kezelésére – indokolt esetben – elkülönített informatikai eszközök is igénybe vehetők.

9.7. Hozzáférés a biztonsági monitoring rendszerhez és a rendszer használata

Az illetéktelen hozzáférések, a tiltott tevékenységek kiszűrése érdekében:

a) Figyelemmel kell kísérni a hozzáférési irányelvektől való eltéréseket, és rögzíteni kell a megfigyelhető eseményeket, hogy adott esetben bizonyítékul szolgáljanak a biztonsági események kivizsgálásához, és segítséget nyújtsanak a szabályzat aktualizálásához.
b) A rendszer nyomon követése tegye lehetővé az ellenőrző eszközök hatékonyságának ellenőrzését és egy, a hozzáférési irányelveknek való megfelelés hitelesítését.
c) A biztonsági monitorrendszert csak az arra feljogosítottak használhatják, és tevékenységüket naplózni kell.

9.7.1. Eseménynaplózás

A kivételes és a biztonságot fenyegető eseményeket eseménynaplóba kell bejegyezni és azt a hozzáférés nyomon követhetősége érdekében meg kell őrizni.

9.7.2. Az informatikai rendszer használatának nyomon követése

A felhasználók által elvégzett tevékenységeket – az ellenőrizhetőség érdekében – rögzíteni, naplózni kell.

a) Az informatikai rendszer üzemeltetéséről (a biztonsági napló mellett) üzemeltetési naplót kell vezetni, amelyet az üzemeltetés vezetőjének és Az IT Igazgatónak rendszeresen ellenőriznie kell.
b) Az informatikai rendszer üzemeltetéséről nyilvántartást (adatkérések, adatszolgáltatások, feldolgozások stb.) kell vezetni, amelyet az arra illetékes személynek (rendszergazda, csoportvezető) rendszeresen ellenőriznie kell.

9.7.3. A dátum és az idő beállítása

Kiemelt figyelmet kell fordítani az operációs rendszer és alkalmazás dokumentációjának figyelembevételével a rendszerdátum és -idő beállítására, mert minden tevékenység visszakereshetőségének alapja a hiteles, pontos dátum és idő. A rendszerdátum és idő beállítása központi időszerverek alkalmazásával történik. A központi időszerverek alkalmazása kötelező minden olyan rendszerben ahol ez lehetséges. Mobil informatikai tevékenység, távmunka

A mobil informatikai eszközön, illetve a távoli hozzáféréssel végzett munka esetén is meg kell teremteni az informatikai biztonságot.

A szükséges védelemnek összhangban kell lennie ennek a speciális munkavégzésnek a kockázataival. Mobil számítástechnikai eszközök használata során mérlegelni kell egyrészt a nem védett környezetben való munkavégzés kockázatait, másrészt a védekezés szükséges módját és eszközeit. A mobil számítástechnikai eszközökön a felhasználó szervezeti egység vezetőjének gondoskodni kell a rejtjelezett adattárolásról és adatátvitelről. Távmunka (távoli hozzáférés) esetén a BVK Holding Zrt. érintett szervezeti egységeinek gondoskodniuk kell a biztonságos adatkapcsolat létrehozásáról, a kapcsolatot tartó hely védelméről.

A mobil informatikai tevékenység és a távmunka szabályozását Az IT Igazgatónak jóvá kell hagynia.

9.8.1. Mobil számítástechnikai eszközök használata

A laptopok, notebookok, otthoni munkaállomások használóinak mind a fizikai biztonság, mind a logikai vedelem területén a jelen IBSz-ben és a rendszerszintű IBSz-ekben foglaltakat kell figyelembe venniük.

Ezek közül a legfontosabbak:

a) A távmunka során is be kell tartani a BVK Holding Zrt. szabályzatait.
b) A mobil eszközök nem hagyhatók felügyelet nélkül, amennyiben nem biztosítható azok előírt védelme.
c) Ki kell alakítani a mobil informatikai eszközök megfelelő fizikai védelmét, a háttértárolón csak titkosítással ellátott adatok tárolhatók.
d) A kommunikációhoz rejtjelezett csatornáról kell gondoskodni.
e) Vírus- és behatolás védelmi eszközöket kell biztosítani a mobil eszközökre.
f) A mobil eszközökön tárolt adatok bizalmasságának védelmére fokozott figyelmet kell
g) fordítani.
h) A mobil eszközön minősített adatot tárolni nem szabad
i) A távoli elérésre vonatkozó szabályokat kell alkalmazni.
j) A mobil eszköz eltűnését (elvesztését, ellopását, stb.) 24 órán belül jelezni kell a közvetlen vezetőnek és Az IT Igazgatónak.
k) Minden egyéb vonatkozásban az IBSz előírásait kell követni.

10.Az informatikai rendszerek fejlesztése és karbantartása

10.1. Az informatikai rendszerek informatikai biztonsági követelményei

Az informatikai rendszerek integrált biztonságának kialakítása a biztonságpolitika által meghatározott szempontok szerint kell, hogy történjen.

Ebbe beletartoznak az infrastruktúra, az üzleti alkalmazások és a felhasználó által kifejlesztett alkalmazások. A biztonság esetenként alapvető feltételeinek egyike az alkalmazást vagy szolgáltatást támogató üzleti folyamat megtervezése és megvalósítása. Az informatikai rendszerek kifejlesztése előtt szükség van a biztonsági követelmények meghatározására és egyeztetésére.
Egy projekt követelményeinek megfogalmazása során meg kell határozni az összes biztonsági követelményt. Ezeket a követelményeket és szükséges megoldásokat egy informatikai rendszer fejlesztésének részeként kell megindokolni, egyeztetni és dokumentálni.

10.1.1. Projektek informatikai biztonsági támogatása

A projektek végrehajtása során az informatikai biztonsági követelményeket kötelező érvényesíteni.
Minden informatikai, informatikai fejlesztéssel járó projekt során kötelező Az IT Igazgató bevonása a munkába, a bevonásért és az informatikai biztonsági követelmények betartásáért a projektvezető a felelős.

10.1.2. A biztonsági követelmények elemzése és meghatározása

a) A BVK Holding Zrt. informatikai beruházásai elkészítésének fázisában a fejlesztési tervek előkészítésére vonatkozó utasítások figyelembevételével az informatikai biztonsággal kapcsolatban a következőknek kell szerepelnie az elkészítendő dokumentum(ok)ban:
   1) az informatikai rendszer által kezelendő adatoknak az információvédelem és a megbízható működés szempontjából történő elemzése és a védelmi célkitűzések meghatározása,
   2) az informatikai rendszer várható informatikai biztonsági osztályba sorolása az információvédelem és a megbízható működés területén,
   3) a jogszabályokból és a belső szabályozásból eredő kötelezettségek bemutatása,
   4) a fizikai és a logikai védelem rendszer szintű bemutatása,
   5) a megvalósításhoz szükséges feltételrendszer meghatározása,
   6) a biztonsági rendszer teljes költségének becslése, ennek összehasonlítása a lehetséges kockázatokkal, károkkal.

b) Az informatikai biztonsági fejezetnek a tervezési dokumentumokba történő beállításáért a projektvezető, annak kijelöléséig. vagy hiánya esetén az előterjesztő a felelős.

c) A BVK Holding Zrt. minden informatikai projekt előterjesztésének tartalmaznia kell a létrehozandó (fejlesztendő, átalakítandó) informatikai rendszer fizikai, logikai és adminisztratív védelmi rendszerének – a projekt keretében történő – tervezési és megvalósítási lépéseit, költségeit, felelőseit.

d) Az informatikai projekt jóváhagyott költségvetésében szerepelnie kell a biztonsági rendszer tervezési és megvalósítási költségeinek.

Az előző pontokban megfogalmazott feltételek hiánya esetén a BVK Holding Zrt.-nél informatikai projekt nem indítható el. Ezért a projektvezető a felelős.

10.2. Biztonság a felhasználói rendszerekben

A felhasználói rendszerek integrált biztonsága kiterjed a rendszerekben tárolt felhasználói adatok illetéktelen hozzáférésének, módosításának, törlésének, nem megfelelő

felhasználásának stb. megelőzésére. A rendszertervek összeállítása során mérlegelni kell a rendszerbe beépítendő automatikus ellenőrző eszközök, valamint a biztonságot támogató manuális ellenőrző eszközök szükségességét.

A felhasználói rendszerek biztonságát a következő intézkedések szavatolják:

a) A felhasználói rendszerekben – többek között a felhasználó által kifejlesztett alkalmazásokban – meg kell tervezni a megfelelő ellenőrző eszközöket és eseménynaplókat, valamint a tevékenységek naplózását. Ezeknek tartalmazniuk kell a bemenő adatok, a belső adatfeldolgozás és a kimenő adatok hitelesítését.
b) Az érzékeny, értékes vagy kritikus adatok feldolgozását végző, vagy ilyen adatokat befolyásoló rendszereknél további ellenőrző eszközökre lehet szükség. Ezeket az ellenőrző eszközöket a biztonsági követelmények és a kockázatelemzés alapján kell kiválasztani.
c) Az a) és b) pontban meghatározott biztonsági intézkedéseket pontosan, minden részletre kiterjedően dokumentálni kell.

10.2.1. A bemenő adatok ellenőrzése

Az adatfeldolgozó rendszerekbe bevitt adatokat hitelesíteni, ellenőrizni kell.

A bemenő adatok ellenőrzésének eszközei:

a) Az ismételt adatbevitel és az ebből származó adat karbantartási anomáliák elkerülésére írt eljárások.
b) Időszakos adatmező és adatállomány vizsgálat, valamint a felvitt adatok hitelességének és integritásának ellenőrzése és igazolása.
c) Az adatbevitel alapját képező nyomtatott input dokumentumok ellenőrzése, illetve ezek engedély nélküli módosításának megakadályozása, valamint az engedélyezés kikényszerítésére írt eljárások. Fokozott és kiemelten Fontos besorolású rendszerek esetén gondoskodni kell az ilyen minősítést eredményező adatok forrásának és forrás-dátumának rögzítéséről is.
d) Adathitelesítési hibák kiküszöbölését elősegítő eljárások.
e) Adatbevitel során, a mezőtípus kompatibilitást biztosító, illetve adattartalom helyességét ellenőrző és kikényszerítő eljárások és függvények.
f) Az alkalmazáshoz történő hozzáférés naplózása.
g) A feldolgozásban részt vevő munkatársak feladatkörének és felelősségének rögzítése a munkaköri leírásokban.

10.2.2. Az adatfeldolgozás ellenőrzése

A pontosan és hiánytalanul beléptetett adatok biztonságát, integritását a feldolgozás ideje alatt a következő intézkedésekkel kell szavatolni:

a) Az adatfeldolgozás rendszerébe ellenőrzési, hitelesítési pontokat kell beépíteni, különös tekintettel az adatmódosító, adattörlő funkciók helyére.
b) Adatfeldolgozási hibák esetén: hibadetektáló, és a további rendszerfutást leállító eljárások beépítése a rendszerbe.
c) Korrekciós programok alkalmazása a feldolgozás során felmerülő hibák korrigálására.
d) A folyamatba épített ellenőrzés végrehajtásáért az üzemeltetés vezető a felelős.

10.2.3. Az üzenetek hitelesítése

Elvárások az üzenethitelesítés, valamint az elektronikus aláírás kialakítása kapcsán:

a) Az azonosítás és hitelesítés keretében a hozzáférést jelszavakkal kell ellenőrizni.
b) A hitelesítés legáltalánosabb módja, a jelszó megadása. Kezelésére a jelszókezelésre vonatkozó fejezetben részletezett általános szabályokat kell alkalmazni.
c) A hitelesítést a felhasználó és a rendszer között egy felhasználó által megnyitott, védett csatornán keresztül kell biztosítani.

10.3.9. 10.2.4. A kimenő adatok ellenőrzése

Az adatfeldolgozás rendszerében ellenőrizni, hitelesíteni kell a kimenő adatokat.

A kimenő adatok biztonsága érdekében a következő védelmi eljárásokat kell alkalmazni:

a) Integritásellenőrzés.
b) Adattartalom meglétének, értékének ellenőrzése.
c) A megfelelő minősítés meglétének ellenőrzése.
d) A kimenő adatok értékelésében és hitelesítésében részt vevő munkatársak feladatainak és felelősségének meghatározása.

10.3. Kriptográfiai eszközök

A BVK Holding Zrt. által kezelt minősített adatok, illetve olyan adatok esetében, ahol más védelmi eszközök nem nyújtanak kellő biztonságot, a BVK Holding Zrt. rejtjelező eszközökkel és technikákkal gondoskodik az adatvédelemről. A rejtjelező technológiákra, algoritmusokra és alkalmazásukra vonatkozó eljárásrendek az adott alkalmazás, rendszer „Üzemeltetési Szabályzat"- ában kerülnek kifejtésre, melyet az adott rendszer üzemeltetői készítenek el.

10.3.1. Kriptográfiai eszközök, módszerek

A BVK Holding Zrt. minősített adatainak, illetve olyan adatok esetében, ahol más védelmi eszközök nem nyújtanak kellő biztonságot, rejtjelező eszközökkel és technikákkal kell gondoskodni az adatvédelemről.
Kriptográfiai rendszerekkel és technikákkal kell gondoskodni az adatok rejtjelezéséről, amikor az adatokat illetéktelen személyek által is hozzáférhető helyen kell továbbítani vagy tárolni, valamint minden olyan esetben, ahol fennáll az adatok kompromittálódásának veszélye.

10.3.2. Felhasználható algoritmusok és technológiák

A gyakorlatban rejtjelezésre csak olyan algoritmusok használhatóak, melyek széles körben bizonyítottan megbízhatóak. Ezen algoritmusokat felhasználó alkalmazások közül került kiválasztásra azon eszközök köre, melyek, felhasználhatóak az adatok védelmére és rejtjelezésére a BVK HOLDING ZRT. rendszerein belül.
A National Institute of Standards and Technology (NIST) tartja karban az aktuálisan elfogadható biztonságot nyújtó algoritmusok listáját (http://csrc.nist.gov/groups/STM/cavp/index.html), melyet a BVK Holding Zrt. is elfogadhatónak és alkalmazhatónak minősít:

- Szimmetrikus
- Advanced Encryption Standard (AES),
- Triple-DES (3DES)
- Skipjack Algoritmus
- Aszimmetrikus
- Digital Signature Algorithm (DSA2),

- RSA /RSA2 , Elliptic Curve DSA (ECDSA2),
- Secure Hash Standard (SHS) (SHA-224, SHA-256, SHA-384, and SHA-512)
- Random Number Generators (RNG)
- Deterministic Random Bit Generator (DRBG)
- Key Management -Key Agreement Schemes and Key Confirmation (KAS)
- Message Authentication (MAC)
- Counter with Cipher Block Chaining-Message Authentication Code (CCM)

A nem megengedett algoritmusok használata a BVK Holding Zrt. rendszereiben tilos. Jelenleg az NIST által elfogadott algoritmusok:

Erősség	Kulcshosszúság (bit)					
Szimmetrikus kulcsú **AES** **3DES** **Skipjack**	56	80	112	128	192	256
SHS (SHA-224, SHA-256, SHA-384, SHA-512)	-	224	256	256	384	512
MAC	64	160	256	256	384	512
Aszimmetrikus kulcsú **Digital Signature Standards (DSA2, RSA2)**	512	1k	2k	3k	7,5k	15k
Elliptikus görbén alapuló **Elliptic Curve DSA2**	160	160	224	256	384	512

Jelmagyarázat:
fejlesztés alatt
nem biztonságos

10.3.3. Kriptográfiai eszközök alkalmazásának irányelvei, módszer kiválasztása

Az adatgazda felelős az általa kezelt adatok bizalmasságának, integritásának védelméért, az adat osztályba sorolásával együtt az azokat megfelelően védő kriptográfiai módszer kiválasztásáért és alkalmazásáért is. Az adatgazda feladata, hogy az IBSZ „Kriptográfiai adatlap" mellékletét legjobb tudásának megfelelően kitöltse, és azt az Információbiztonsági megbízottnak eljuttassa.

A BVK Holding Zrt. informatikai rendszereiben alkalmazandó rejtjelező rendszer üzembe helyezése csak Az IT Igazgató engedélyével lehetséges. Amennyiben egy adott az alkalmazás esetében a szabályzatnak megfelelő algoritmus nem alkalmazható, Az IT Igazgató egyedi

elbírálással dönthet a kockázatarányos védelmet biztosító technológia alkalmazásáról. Amennyiben az elvárt védelmi szint nem megvalósítható az adott alkalmazásban (például: túl nagy fejlesztést igényel, vagy egyéb technológiai korlátjai vannak), a kockázat lehetséges kezeléséről, vagy annak felvállalásának szükségességéről a vezetőséget írásban tájékoztatja.

Új fejlesztések esetén az alábbi kiválasztási módszer irányadó:

- Milyen biztonsági osztályba sorolható a védendő adat (alap, fokozott, kiemelt, üzleti titok, banktitok)
- Mi az adatkezelés formája (adattárolás vagy adattovábbítás)
- Milyen eszközöket/alkalmazásokat lehet alkalmazni a BVK Holding Zrt.nál rejtjelezés céljára
- Az Információbiztonsági Megbízott jóváhagyása szükséges a kiválasztáshoz és bevezetéshez

A BVK Holding Zrt. által az alább felsorolt eszközök támogatottak az adatok tárolása, vagy fájlként történő továbbítás esetén (például email csatolmány, USB kulcson történő átadás...):

- TrueCrypt
- 7Zip

A felsorolt eszközök biztonságosan alkalmazható verzióját az eljárásrendek definiálják, mivel ezek verziója gyakran változhat.

Az eszközöket minden számítógépre telepíteni kell. Ennek biztosítása érdekében ezeket a desktop image-ekbe el kell helyezni, valamint a már használatban lévő gépeken is gondoskodni kell ezek telepítéséről.

10.3.4. Rejtjelezés algoritmusának meghatározása

A BVK Holding Zrt. az adat rejtjelezéséhez használt algoritmust az adat információbiztonsági csoportjához köti. Amennyiben az előírt algoritmus nem érhető el, az információbiztonsági felelős jóváhagyása szükséges.

Az adatok tárolásánál és folyamatos továbbításánál felhasznált algoritmusok eltérhetnek, így ezeket értelem szerűen a felhasználás módjának megfelelően kell az alábbi táblázatból kiválasztani.

Az adatokhoz osztályozásuk alapján rendelt kriptográfiai algoritmusok:

Minősítés	Hálózat	Titkosítás	Kulcshossz
Osztályozás nélküli	**Belső/Külső**	**opcionális**	-
Alap	**Külső/Külső**	**opcionális**	-
Fokozott	**Belső/Külső**	**opcionális**	-
Kiemelt	**Belső/Külső**	**opcionális**	-

Üzleti titok	**Külső**	**szükséges**	**Szimmetrikus: 80 -112** **Hash: SHA -254, SHA – 256** **MAC: 160 – 256** **Aszimmetrikus: 1024**
Üzleti titok / Banktitok	**Belső**	**szükséges**	**Szimmetrikus: 80 -112** **Hash: SHA1** **MAC: 160 – 256** **Aszimmetrikus: 1024**
Banktitok	**Külső**	**szükséges**	**Szimmetrikus: 128 – 256** **Hash: SHA -256, SHA – 512** **MAC: 256 - 384** **Aszimmetrikus: 2048**

10.3.5. Jelszókezelés

A jelszókezelésre vonatkozóan az IBSZ 9.3.1 pontja az irányadó.

Rejtjelezés esetén a jelszavakra vonatkozóan mindezeken túl alábbi követelmények érvényesek:

- Minimális jelszóhossz: 12 karakter
- Jelszó nem lehet szótári szó, nem lehet könnyen kitalálható szó, tartalmaznia kell kis-, és nagybetűt, számot, speciális karaktert (például: -_„"+!%/=)( )

Jelszavak kiadása

A jelszókezelésre vonatkozóan a BVK Holding Zrt. mindenkori jelszó kezelési rendje az irányadó.

Jelszavak tovább adása

A jelszókezelésre vonatkozóan a BVK Holding Zrt. mindenkori jelszó kezelési rendje az irányadó.

Jelszavak tárolása

A jelszókezelésre vonatkozóan a BVK Holding Zrt. mindenkori jelszó kezelési rendje az irányadó.

Jelszavak megsemmisítése

A jelszókezelésre vonatkozóan a BVK Holding Zrt. mindenkori jelszó kezelési rendje az irányadó.

10.3.6. Elektronikus aláírás

A BVK Holding Zrt. a következő esetekben írja még elő digitális aláírás használatát:

a) Elektronikus kereskedelmi tevékenységek során (e-business, e-commerce, e-banking stb.), ahol azonosítani és hitelesíteni kell az elektronikus kifizetéseket, kötelezettségvállalásokat aláíró személyét, valamint meg kell vizsgálni az aláírt dokumentum integritását.
b) Elektronikus eszközökkel feldolgozott pénzátutalásoknál, szerződéseknél és megállapodásoknál.

Ügyelni kell a magánkulcs bizalmas kezelésére. A magánkulcs kezelését végző (a kulcsgeneráló eszközöket, alkalmazásokat kezelő) személyek fontos és bizalmas munkakört betöltőnek minősülnek. Az elektronikus aláírás kulcsa és a rejtjelkulcs nem lehet azonos.

Az elektronikus aláírás algoritmusát, valamint az alkalmazható kulcsok hosszát az IT Igazgató hagyja jóvá.

10.3.7. Kulcsmenedzsment

A kulcsmenedzsmentet kötelező jelleggel ki kell alakítani minden elektronikus aláírással, rejtjelezéssel rendelkező rendszerben. A kulcsmenedzsment kialakítása során a hatályos jogi szabályozást, és a PKI-ra vonatkozó nemzetközi szabványokat kell figyelembe venni.

10.3.7.1. Kriptográfiai kulcsok védelme

A rendszerben használt kriptográfiai kulcsok védelme:

a) A kriptográfiai kulcsok fizikai, valamint speciális, illetve fokozott biztonságot igénylő esetben rejtjelezéssel megvalósított logikai védelméről is gondoskodni kell.
b) Szükség esetén a kulcs-felek megosztásával kell biztosítani a rejtjelkulcsok védelmét.

10.3.7.2. Szabványok, eljárások és módszerek

A kulcskezelési rendszer kialakításánál a következő szabványok, szempontok és módszerek egyeztetett rendszerét kell figyelembe venni:

a) Kulcsgenerálási rendszer.
b) Nyilvános kulcs hitelesítési eljárások
c) A felhasználói kulcsok eljuttatására, valamint az átvett kulcsok aktiválására vonatkozó módszerek.
d) Kulcstárolási illetve hozzáférési szabályok.
e) Kulcsmódosítási, aktualizálási szabályok.
f) Hamisított kulcsok kezelése.

g) Kulcsvisszavonási szabályok. (A kulcsok visszavonásának és használaton kívül helyezésének módja többek között abban az esetekben, amikor a kulcsokat hamisítják vagy a kulcs tulajdonosa elhagyja a szervezetet.)
h) Kulcsok archiválási rendje.
i) Elveszett kulcsok helyreállítási szabályai. (Az elveszett kulccsal rejtjelezett állományok visszaállítása az üzletmenet-folytonosság terv része kell, hogy legyen.)
j) Kulcsok megsemmisítésének szabályai.
k) Kulcskezelő rendszer eseménynaplózása.

A kulcshamisítás kockázatának csökkentése érdekében, előzetesen meg kell határozni a kulcsok aktiválásának és visszavonásának dátumait. A kulcs élettartama függ a vélelmezett kockázat mértékétől.

A nyilvános kulcsokkal való esetleges visszaélések kockázatának csökkentése érdekében, csak hitelesített nyilvános kulcsok használhatók a rendszerben.

A kriptográfiai szolgáltatók külső szállítóival, például egy hitelesítő hatósággal kötött, a szolgáltatás mértékét meghatározó megállapodásoknak vagy szerződéseknek szabályozniuk kell a felelősség kérdését.

10.3.8. Monitorozás, megfelelőség

A rejtjelező szoftverek telepítése, karbantartása az informatikai üzemeltetés feladata.

A megfelelőség biztosítása érdekében automatikus vagy manuális (audit jellegű) ellenőrzések történhetnek a rendszereken.

A rejtjelezéssel kapcsolatos problémák, incidensek (jelszavakkal kapcsolatos problémák, elvesztés, megszerzés, ellopás) jelentése minden alkalmazott kötelessége

10.3.9. Kulcskezelés és a rejtjelezés visszafejtése

A rejtjelezés visszafejtésének biztosítása alapvető a BVK Holding Zrt. számára, melyhez szükséges a felhasználók által használt kulcs ismerete amennyiben arra szükség van. A felhasználónak kötelessége az általa rejtjelezett információk eredeti „titkosítatlan" formába történő visszaállítása, amennyiben azt a BVK Holding Zrt. Vezérigazgatója és az információbiztonsági megbízott írásban felszólítja.

A kulcskezeléssel szemben az alábbi kritériumokat támasztja a BVK Holding Zrt.:

Kulcs integritás:

- Megbízhatóság – a kulcs nem lehet egyszerűen kitalálható és kihasználható rosszindulatú támadó által
- Rendelkezésre állás – a kulcs információ rendelkezésre kell hogy álljon, amennyiben szükséges

Kulcs elérhetősége:

- Bizalmasság: A kulcs információ bizalmassága nem sérülhet annak kiadása, kezelése során.
- Jóváhagyás: A kulcs információ megszerzésére csak a jogosult személyek lehetnek képesek megfelelő jóváhagyás után.

Kulcs visszaállítás:

- Korlátozott információ visszaállítás: A visszaállítás tárgyához szükséges minden információt vissza kell állítani, azonban kizárólag a tárgyhoz tartozó kulcs visszaállítási információk tehetők elérhetővé a jóváhagyott személy számára.
- Időablak: A kulcs visszaállítási időablak kezdő és végdátuma is kötelezően meghatározandó.

10.3.9. Definíciók

Kifejezés	Értelmezés
Autentikáció	**Olyan eljárást jelent, amelynek során meggyőződünk arról, hogy valamely információ (legtöbbször egy felhasználó azonosságára vonatkozó állítás) megfelel a valóságnak.**
Rendelkezésre állás	**Azt a valószínűséget jelenti, amellyel egy definiált időintervallumon belül az alkalmazás vagy rendszer a tervezéskor meghatározott funkcionalitási szintnek megfelelően a felhasználó által használható.**
Bizalmasság	**Az információk vagy adatok esetében, csak az arra jogosítottak és csak az előírt módokon férhetnek hozzá, és nem fordulhat elő úgynevezett jogosulatlan információszerzés.**
Kriptográfia	**Az információ rejtjelezése, az illetéktelen hozzáféréssel szembeni védelem módszere, mely biztosítja az információ hitelességét, módosíthatatlanságát és meggátolja az illetéktelen hozzáférést.**
Kriptográfiai kulcs	**Olyan paraméter, melyet a kriptográfiai algoritmus használ a transzformáláshoz, hitelesítéshez, autentikációhoz, rejtjelezéséhez és/vagy visszafejtéshez.**
Kriptográfiai módszer	**Lehet kriptográfiai technika, eljárás, szolgáltatás, rendszer, termék.**
Adat	**Az információ olyan megjelenési formája, melyet tárolunk, továbbítunk vagy feldolgozunk.**
Titkosítás / rejtjelezés	**Az adatok rejtjelezésére használt eljárás, mely biztosítja, hogy a rejtjelezett adat mások számára nem értelmezhető, abból az eredeti információ nem állítható elő a kriptográfiai kulcs ismerete nélkül.**
Visszafejtés	**A rejtjelezés inverz eljárása, mellyel a rejtjelezett üzenetből az eredeti üzenet visszaállítható.**
Integritás	**Az információ nem változhat meg (például tárolás, feldolgozás vagy továbbítás során sem).**
Mobilitás	**A kriptográfiai eljárások technikailag több helyen is**

	alkalmazhatóak, más infrastruktúrákkal kompatibilisek.
Adatgazda, adatkezelő	**Az a munkatárs, aki az adatkezelés célját, az adatok elkészítésének, módosításának, törlésének szabályait valamint a jogosult felhasználói kört (mint felhasználói csoportokat) meghatározza, tevékenységükért felelősséggel tartozik, továbbá azok, akiknek a munkaköri leírása adott adatokra ezt a felelősséget meghatározta.**
Nem megengedett algoritmus	**Olyan algoritmus, mely nem szerepel a BVK Holding Zrt. által alkalmazhatónak minősített algoritmusok listáján.**
Szimmetrikus rejtjelezés	**A rejtjelezéshez és kódoláshoz ugyanaz a kulcs használatos, melyet biztonságosnak vélt úton kell eljuttatni a másik félhez.**
Aszimmetrikus rejtjelezés	**Az algoritmus két különböző kulcsot használ a rejtjelezéshez és a visszafejtéshez (például nyilvános kulcsú titkosítás). A két kulcs egymásból nem számítható ki, vagyis nem állítható elő a nyilvános kulcsból a titkos kulcs.**

10.4. Informatikai biztonság a fejlesztési és a karbantartási folyamatokban

a) Szükség van a projekt és a támogatási környezetek szigorú ellenőrzésére.
b) Az alkalmazói rendszerekért felelős vezetőknek vállalniuk kell a felelősséget a projekt és a támogató, környezetének biztonságáért. Gondoskodniuk kell arról, hogy megvizsgálják a rendszerben javasolt összes változtatást és megállapítsák, mennyiben befolyásolják ezek a rendszer vagy működési környezete biztonságát.
c) Fejlesztési szabályokat és az elfogadott BVK HOLDING Zrt. szabványokat kell kialakítani.

10.5.1. Változásmenedzsment eljárások

Az informatikai rendszer sérülékenységének minimalizálása érdekében a változtatásokat csak szigorú ellenőrzéseken keresztül lehet megvalósítani.
A változtatás ellenőrzésének eljárását a Változásmenedzsment Szabályzatban kell szabályozni.

Az eljárással kapcsolatban:

a) Szabályozni kell a változtatást végrehajtó személyek körét.
b) A szükséges módosítás érdekében az összes szoftver, információ, adatbázis és hardver azonosítását el kell végezni.
c) A munka elkezdése előtt részletes, formalizált elfogadási eljárásra van szükség.
d) Biztosítani kell, hogy a megvalósítás során az üzleti folyamatok ne sérüljenek.
e) A rendszerdokumentációkban a változásokat át kell a vezetni, és a régi dokumentációkat archiválni kell.
f) Karban kell tartani a változásmenedzsment segítségével az összes szoftverfrissítést.
g) Biztosítani kell minden változtatás ellenőrzését.
h) Biztosítani kell, hogy az üzemi dokumentumokon is átvezetésre kerüljenek amennyiben szükségesek a változtatások.
i) Biztosítani kell, hogy a változtatások kellő időben és az üzleti eljárás zavarása nélkül kerüljenek megvalósításra.

10.5.2. Az operációs rendszer változtatásainak ellenőrzése

a) Amennyiben a külső vagy belső tényezők szükségessé teszik az operációs rendszer változtatását, az operációs rendszer alapértelmezett átvizsgálása után az applikációs rendszert ellenőrizni és tesztelni kell annak biztosítása érdekében, hogy a változtatás a működőképességgel és a biztonsággal ne ütközzön.
b) Éles rendszerbe történő beillesztés előtt a változásokat az alkalmazásokkal kell tesztelni.

10.5.3. Vásárolt programok változtatására vonatkozó szabályok

A BVK Holding Zrt. munkavállalói munkavégzésük során csak jogtiszta szoftvereket használhatnak. Ha a vásárlási (licenc, fejlesztési) szerződés másként nem rendelkezik a szerzői jogról szóló törvény alapján kell eljárni. Ennek megfelelően a szerző kizárólagos joga nem terjed ki:

a) a többszörözésre,
b) az átdolgozásra,
c) a feldolgozásra,
d) a fordításra,

e) a szoftver bármely más módosítására – ideértve a hiba kijavítását is – valamint
f) ezek eredményének többszörözésére annyiban, amennyiben e felhasználási cselekményeket a szoftvert jogszerűen megszerző BVK Holding Zrt. a szoftver rendeltetésével összhangban végzi.

10.5.4. A programfejlesztés kihelyezése

A programfejlesztés kihelyezése esetén a BVK Holding Zrt. adat- is információvédelmére vonatkozó szabályok szem előtt tartásával kell eljárni.

a) Biztosítani kell a forrásprogram, illetve a továbbfejlesztés lehetőségét a BVK Holding Zrt. részére a fejlesztőtől függetlenül is.
b) A fejlesztés során az üzemi rendszerekhez a fejlesztő részére távoli hozzáférés nem engedélyezhető.
c) A fejlesztő "éles" adatokkal tesztelést nem folytathat.
d) Biztosítani kell, hogy a BVK Holding Zrt. illetékesei a Fejlesztési környezetet, az adat- és információvédelmi szabályok betartását ellenőrizhessék.

11.Üzletmenet-folytonosság menedzsment

Az üzleti tevékenység megszakítása (megszakadása) esetén kezdeményezni kell a szükséges intézkedések megtételét.

11.1. Üzletmenet-folytonosság menedzsment területei

A kritikus üzleti és informatikai folyamatok védelme érdekében a meghibásodások és a rendellenességek elhárítása során:

a) Az üzletmenet-folytonosságának fenntartását szolgáló eljárás a megelőző és helyreállítást vezérlő eljárások (üzletmenet-folytonossági terv, katasztrófa-elhárítási terv) együttes alkalmazásával mérsékelni kell a különböző rendellenességek és a biztonsági rendszer meghibásodása által okozott fennakadásokat. (Ezek lehetnek többek között természeti katasztrófák, balesetek, berendezésekben keletkezett hibák, vagy szándékos cselekmények következményei.)
b) Elemezni kell a meghibásodások, fennakadások és üzemzavarok következményeit.
c) Az üzletmenet-folytonosságának irányítása ki kell, hogy terjedjen – többek között – a kockázatok azonosítására és csökkentésére alkalmas ellenőrző eszközökre, a kárt okozó események következményeinek korlátozására, valamint a lényeges tevékenységek időben történő újraindítására.

11.1.1. Üzletmenet-folytonosság menedzsment folyamata

Az üzletmenet-folytonosság tervezését – méreteire való tekintettel – projektszerűen kell megvalósítani.

Az üzletmenet-folytonosság biztosítási folyamatának kialakítása során a következőket kell figyelembe venni:

a) Az informatikai biztonsági kockázatok felmérése, és a bekövetkezési valószínűségek elemzése.
b) A folytonosság megszakadásából (megszakításából) következő hatások, következmények felmérése és elemzése.

c) Az üzleti céloknak és az informatikai biztonságpolitikának megfelelő üzletmenet folytonossági stratégia meghatározása.
d) Az előzőekben megfogalmazottaknak megfelelő üzletmenet-folytonossági tervek kidolgozása.
e) Az elfogadott tervek rendszeres felülvizsgálata és aktualizálása.
f) Kulcsfontosságú rendszerek kizárólag megfelelő és kipróbált katasztrófa-elhárítási terv alapján működhetnek éles üzemben.

11.1.2. Az üzletmenet-folytonosság és a hatásvizsgálat

a) A megfelelő üzletmenet-folytonosság az informatikai rendszer folyamatos üzemi működésének az a szintje, amely során a kiesés kockázatának szintje a BVK Holding Zrt. számára még elviselhető.
b) Az elviselhetőség határát az üzletmenet - támogatás szempontjából kritikus rendszereinek-egy meghatározott (maximált) kiesési ideje határozza meg.
c) Az üzletmenet-folytonosság megfelelő szintjét a szükséges megelőző, illetve (a kiesés bekövetkezése után) visszaállító intézkedésekkel kell biztosítani, amely intézkedéseket előre meg kell tervezni (üzletmenet-folytonossági terv, katasztrófa-elhárítási terv).
d) Az üzletmenet-folytonosság tervezés eredménye az üzletmenet-folytonossági terv, amely részletesen meghatározza a kívánt üzletmenet-folytonosság fenntartásához szükséges feltételeket, szervezeti és szervezési lépéseket, valamint szabályozza a megvalósítás módját.

11.1.3. Az üzletmenet-folytonossági terv kidolgozása

Alapvető célja az, hogy a BVK Holding Zrt. üzleti folyamatait támogató informatikai erőforrásai a rendelkezésre álló üzemidőben a lehető legjobb időkihasználással és a legmagasabb funkcionalitási szinten működjenek annak érdekében, hogy az üzleti folyamatok zavarai által okozott közvetlen és közvetett károk minimálisak legyenek.

Az üzletmenet-folytonossági tervnek részletesen meg kell határoznia a kívánt üzletmenet-folytonosság fenntartásához szükséges megelőző, helyettesítő, illetve visszaállító intézkedések megvalósításához szükséges feltételeket, szervezeti es szervezési lépéseket és a megvalósítás módját.

A tervezés egyik lényeges eleme a kiesési kockázatok elemzése, amelynek során mérlegelni kell az okozott kár nagyságát és az üzemzavari események, a veszélyhelyzetek bekövetkezésének gyakoriságát.

Az üzletmenet-folytonosság terv fő részei:

a) Kockázatfelmérés és értékelés
    1) Projekt előkészítő megbeszélés (feladat behatárolás, humán és eszköz erőforrás, illetve az adminisztrációs feltételek tisztázása, projekt-terv megbeszélése, felhasználandó dokumentumok előzetes meghatározása).
    2) Részletes projektterv elkészítése.
    3) Projektindító megbeszélés (célok, feladatok, várható eredmények prezentációja; pontos feladatmeghatározás; projekt szervezet összetétele; felhasználandó dokumentumok listája; projekt megkezdése).
    4) Előzetes helyzetfelmérő interjúterv elkészítése és véglegesítése (területek, személyek).

5) Az interjúk megszervezése (személyek és időpontok egyeztetése), tematikák elkészítése.
6) Interjúk elkészítése és feldolgozása dokumentumokban (kritikus üzleti folyamatok és az ezeket támogató alkalmazások; a kiesések következményei, kockázatai és rangsorolása az eredményes működés szempontjából, rendelkezésre állás követelményei potenciális üzemzavari és katasztrófa események palettája, tartalékolási és visszaállítási stratégiák és megoldások).
7) Projekt-team teszteli a meghatározott tartalékolási és visszaállítási megoldások megvalósíthatósági feltételeit, majd ennek alapján helyzetfelmérő és értékelő jelentést készít.
8) A projekt-team a helyzetfelmérő és értékelő jelentését a BVK Holding Zrt. vezetésének átadja, ahol megtörténik a jelentés ellenőrzése és elfogadása.

b) Az üzletmenet-folytonossági terv elkészítése
c) Itt történik meg az üzletmenet-folytonossági terv kidolgozása, melynek fő részei:
1) Megelőzési terv és intézkedések
- Tartalmazza mindazon szabályzatokat, dokumentumokat és intézkedéseket, amelyek az informatikai rendszer folytonos üzemét valamilyen módon veszélyeztető tényezőkkel kapcsolatosak.
- Alapvető szerepe van a megelőzésnek, mind a nagyobb üzemzavarok vagy katasztrófa események, mind a nagyszámú, de kisebb üzemeltetési és felhasználási problémák miatt sérülő alkalmazások rendelkezésre állásával kapcsolatban.
- A megelőzési terv a következőkre terjed ki:
  - Az informatikai rendszer megbízható üzemeltetésére és az üzemeltetésre vonatkozó intézkedésekre.
  - Az informatikai rendszer kritikus elemeinek üzemi és katasztrófa tartalékmegoldásaira és ezek üzemkészségét biztosító intézkedésekre.
  - Az informatikai rendszer üzemét biztosító környezeti rendszerek karbantartási, illetve az ezekkel kapcsolatos biztonsági intézkedésekre.
  - Az üzemeltetési dokumentáció és dokumentumok rendszerezett és biztonságos tárolására.
  - Adathordozók rendszerezett és biztonságos tárolására.
  - Az üzemeltető, a karbantartó és a kárelhárító személyzet rendelkezésre állását és bevethetőségét biztosító intézkedésekre.
  - A külső szervizre, a tartalékképzési megoldásokra vonatkozó, és a biztosítási szerződésekkel kapcsolatos intézkedésekre.
  - Mentési tervre, amely meghatározza a mentési rendszer generációit és hierarchiáját.
  - Az üzemelő rendszer konfigurációjában, az üzemelő szoftverben megvalósítandó változások szabályozott kivitelezésére, valamint a szoftverfejlesztések elkülönített kivitelezésére és a fejlesztett szoftverek rendszerbe történő integrálására vonatkozó legfontosabb intézkedésekre.
  - Vírusvédelmi és vírusmenedzsment intézkedésekre, figyelembe véve a BVK Holding Zrt. hatályos vírusvédelmi szabályzatát.
  - Megelőzésben fontos szerepet játszik az alkalmazói rendszerek használatára történő rendszeres oktatás, illetve az informatikai biztonság olyan szintű oktatása, amely kiterjed az informatikai rendszerekben kezelt adatok bizalmasságának, hitelességének,

sértetlenségének, rendelkezésre állásának megőrzése érdekében betartandó szabályokra és az érvényesítendő védelmi intézkedésekre.
    - Tesztelési és tréning tervre, amely meghatározza a tesztelés formáit. Két formája javasolt: audítálás jellegű check-listás teszt, amelyet egy előre elkészített ellenőrzési lista alapján független belső vagy külső auditorok végeznek el, illetve valós üzemzavari vagy katasztrófa események szimulációjával.

2) Visszaállítási terv
- A visszaállítási terv alapvető célja az, hogy az üzemzavari vagy katasztrófa események bekövetkezése esetén zárt módszertan alapján a lehető leghamarabb bekövetkezzék az esemény azonosítása, az esemény kezeléséhez előírt emberi és eszköz erőforrások haladéktalan mozgósítása, és a tervben rögzített módon végbemenjen visszaállítás minden részfolyamata.
- A visszaállítási terv a következőket tartalmazza:
    - A visszaállítási terv célját és használatát.
    - Az üzemzavari és katasztrófa események meghatározását.
    - Az események bekövetkezési és kezelési időszakait.
    - Az eseménykezelő team összetételét, feladatait és hatáskörét.
    - Visszaállítási intézkedéseket a következő lépésekre:
        - azonnali válasz (riadóterv),
        - futtató környezet helyreállítás,
        - funkcionális helyreállítás,
        - üzemeltetési szintű helyreállítás,
        - áttelepülés (katasztrófa esetén),
        - normalizáció az áttelepülés után.
- Az intézkedések átfogják a központi erőforrások, azok fizikai és személyi környezetét, a végponti munkaállomások és a kommunikációs rendszer területeit.
- Véglegesítésre kerül az előzetes intézkedési terv, amely tartalmazza mindazon feltételek biztosítására vonatkozó intézkedéseket, amelyek megléte nélkül az üzletmenet-folytonossági terv nem működőképes.

d) Oktatás, tréning és tesztelés
- Az oktatás célja az üzletmenet-folytonosság jelentőségének tudatosítása, az üzletmenet-folytonosság tervezés alapismereteinek átadása.
- A megelőzési és visszaállítási tervben foglaltak megismerése és elsajátítása.
- Az üzletmenet-folytonossági terv tesztelése és tréningje akkor válik elindíthatóvá, ha a BVK Holding Zrt. által az üzletmenet-folytonossági tervben a végrehajtáshoz rendelt intézkedések olyan szinten megvalósultak, hogy az üzletmenet-folytonossági terv tesztje és tréningje az egyes üzemzavar vagy katasztrófa eseményekre kivitelezhető.
- Az üzletmenet-folytonossági terv tesztje szimulált esemény bekövetkezésével és a terv szerinti visszaállítással kerül megvalósításra. A teszt keretében az eseménykezelő team (+ esetleg az üzemeltető személyzet és a felhasználók) a valós körülményeket megközelítően gyakorolják a visszaállítási terv utasításainak végrehajtását.

11.1.3.1. Katasztrófa-elhárítási terv

A katasztrófa-elhárítási terv globális helyettesítő megoldásokat ad megelőző és elhárító intézkedésekre, amelyekkel a bekövetkezett katasztrófa esemény után az informatikai rendszer funkcionalitása degradált vagy eredeti állapotába visszaállítható.

A katasztrófa-elhárítás tervezés célja a kiesési idő, a rendszer normál állapotának lehető legrövidebb időn belül történő visszaállításán túl az, hogy ezt a kockázatokkal arányosan lehessen megvalósítani.

A vészhelyzetekből eredő károk megelőzésének, mérséklésének alapvető követelménye a részletes terv (Megelőzési és Visszaállítási terv) elkészítése, tesztelése és a végrehajtás rendszeres gyakorlása.

A katasztrófa-elhárítási terv eljárások és/vagy tevékenység lépések sorozata annak biztosítására, hogy a BVK Holding Zrt. kritikus adatfeldolgozó képességeit – a szükséges aktuális adatokkal – a bekövetkezett katasztrófa után elfogadhatóan rövid időn belül helyre lehessen állítani.

a) A katasztrófa-elhárítási tervben a következők kerülnek meghatározásra:
   1) a rendelkezésre állási követelmények megadása;
   2) a katasztrófa vagy vészhelyzet események definíciója;
   3) a korlátozott informatikai üzem fogalma (visszaesési fokozatok) és a hozzájuk tartozó funkcionalitási szintek;
   4) javaslat a felelősségek szabályozására veszély vagy katasztrófa esetén;
   5) a riadóterv vázlata;
   6) kiválasztott esetekre konkrét intézkedési terv, különösen a következő területen:
      - a szükségüzem esetére a minimális hardver- és szoftverkonfiguráció rögzítése (beleértve az adatokat is),
      - a szükségüzem esetére – amennyiben az lehetséges – manuális póteljárás rögzítése,
      - szükség esetén backup-rendszer (pl. saját vagy külső tartalék központ igénybevétele),
      - adatrekonstrukciós eljárások bevezetése,
      - az újra alkalmazhatóságot lehetővé tevő intézkedések;
   7) az olyan informatikai rendszerek védelme, amelyeknek állandóan elérhetőeknek kell lenniük (pl. redundancia intézkedésekkel és a hibákat toleráló hardverekkel és szoftverekkel),
   8) az adatbiztosítási intézkedések megvalósítási szabályainak összeállítása (pl. háromgenerációs elv),
   9) az üzemi szempontból szükséges adatok biztonsági kópiáinak elkészítése meghatározott időszakonként.
   10) a biztonsági másolatoknak más biztos helyen (a munkaterületen, illetve a számító-központon kívüli) raktározása,
   11) az installált rendszerszoftverek és a fontosabb alkalmazói szoftverek referenciamásolatainak biztonságos raktározása.
   12) a fontosabb dokumentációk megkettőzése és raktározása,
   13) a megvalósított adatbiztosítás ellenőrizhető dokumentációja;
   14) visszaállítási terv, amely magában foglalja az informatikai alkalmazások prioritásainak kijelölését és célkitűzések megállapítása (pl. az X alkalmazás újraindítása Y napon belül);
   15) a beszállítói (szolgáltatói) szerződésekre vonatkozó – katasztrófa események bekövetkezése esetében érvényes – követelmények meghatározása (annak

érdekében, hogy katasztrófahelyzetben is biztosítani lehessen a rendelkezésre állást);

16) javasolt biztosítások katasztrófák, káresemények esetére,

17) a terv készítésének, felülvizsgálatának, tesztelésének időpontja.

b) A katasztrófa-elhárítási terv részei:

1) a katasztrófa-elhárítási terv definíciója,

2) a mentési (megelőzési) terv:

- Azon lépések sorozata, amelyeket azért hajtanak végre (a normál üzem során), hogy lehetővé tegyék a szervezet hatékony reagálását a katasztrófára.
- A mentési terv elmentett eszközöket (adatokat, szoftvereket) biztosít a helyreállításhoz. Így például a számítógép, a háttértárak tükrözése és az optikai tárolók használata sokkal könnyebbé teheti adatbázisok, illetve nagy tömegű papíralapú dokumentumok helyreállítását.

3) a helyreállítási és újraindítási terv:

A helyreállítási terv olyan eljárások sorozata, amelyeket a helyreállítás fázisában hajtanak végre annak érdekében, hogy helyreállítsák:

– az informatikai rendszert a tartalék központban vagy

– az adatfeldolgozó központot.

A helyreállítási terv szakaszai:

– azonnali reakció: Válasz a katasztrófahelyzetre, a veszteségek számbavétele, az előre tervezett és alkalmas munkatársak értesítése és a katasztrófaállapot megállapítása.

– környezeti helyreállítás: Az adatfeldolgozó rendszer (operációs rendszer, programtermékek és a távközlési hálózat) helyreállítása.

– funkcionális helyreállítás: Az informatikai rendszer alkalmazásainak és adatainak helyreállítása, az adatok szinkronizálása a tranzakció naplóval. Az elvesztett vagy késleltetett tranzakciók ismételt bevitele. Az üzemeltetők, a rendszeradminisztrátorok, a felhasználók együtt munkálkodnak azon, hogy helyreállítsák a normál feldolgozási rendet.

– áttelepülés: Az informatikai rendszer kiépítése és telepítése a hidegtartalék létesítményben (ha a melegtartalék létesítmények használata időben korlátozott).

– normalizáció: Az állandó informatikai rendszer újra kiépítése és arra az üzemelő rendszer áttelepítése.

4) tesztelési terv:

A tesztelési terv azokat a tevékenységeket tartalmazza, amelyek ellenőrzik és biztosítják a katasztrófa-elhárítási terv működőképességét.

5) a karbantartási (üzembentartási) terv:

A szervezet változása esetén a karbantartási tervet kell felhasználni a katasztrófa-elhárítási terv aktuális állapotban tartására.

6) az érintett személyek elérési adatai.

c) Intézkedni kell:
   1) A kár megelőzésére és a károk minimalizálására az IBSz alapján (pl. belső vagy külső háttér-, illetve tartalék számítógép-kapacitás előkészítése szükségüzem esetére az elégséges hardver- és szoftverkonfiguráció rögzítésével);
   2) a katasztrófák, veszélyhelyzetek bekövetkezésekor;
   3) a rendszer (folytonosságának) visszaállítására a katasztrófákat és a káreseményeket követően;
   4) a veszélyhelyzetek és a katasztrófák esetszimulálására, begyakorlásra, intézkedések modellezésére, illetőleg kipróbálására.

11.1.4. Az üzletmenet-folytonossági tervek vizsgálata, karbantartása és újraértékelése

11.1.4.1. Tervek tesztelése

A tervek tesztelését egy szimulált esemény bekövetkezésével és a tervszerinti visszaállítással kell megvalósítani. Ennek keretében az eseménykezelő szervezet, az üzemeltető személyzet és a felhasználók a valós körülményeknek megfelelően gyakorolják a visszaállítási terv utasításainak végrehajtását.

11.1.4.2. A tervek karbantartása és újraértékelése

A teszt értékelése során az üzletmenet folytonosságát biztosító terveket módosítani, aktualizálni kell, és gondoskodni kell azok egymáshoz való illesztéséről.
A terveket a folytonosan változó helyzethez, körülményekhez (személyzet, stratégia, infrastruktúra), követelményekhez (szabályok, kockázatok) is hozzá kell igazítani.

12. Megfelelés a jogszabályoknak és a belső biztonsági szabályzatoknak

12.1. A jogszabályi előírások betartása

a) Az informatikai rendszerek tervezésére, fejlesztésére, üzembe helyezésére, működtetésére, használatára és kezelésére különböző törvények, jogszabályok, szabványok, ajánlások, valamint az egyes szerződésekben rögzített biztonsági követelmények vonatkoznak. Ezek szervezeti szintű érvényesítése érdekében a BVK Holding Zrt. informatikai tevékenységének végzésére vonatkozó biztonsági szabályok rögzítése, a szabályozás hazai gyakorlatának és a nemzetközi szabványok előírásainak való megfeleltetése, továbbá az ehhez szükséges személyi és tárgyi feltételek meghatározása elengedhetetlen.

b) Fentieknek megfelelően a Szabályzat a hatályos jogszabályok, szabványok és ajánlások figyelembevételével készült el. Kétség esetén konkrét követelményekről ki kell kémi a BVK Holding Zrt. IT Igazgató véleményét.

12.1.1. A vonatkozó jogszabályok, szabványok és ajánlások

12.1.1.1. Jogszabályok:

1) 2001. évi XXXV. törvény az elektronikus aláírásról,
2) 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról,
3) 1995. évi CXIX. törvény a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről,
4) 1995. évi LXVI. törvény a közokiratok, közlevéltárak és a magánlevéltári anyag védelméről,

5) 1995. évi LXV. törvény az államtitokról és a szolgálati titokról,
6) 1992. évi LXIII. törvény a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról,
7) 1992. évi XXII. törvény a Munka Törvénykönyvéről,
8) 1978. évi IV, törvény a Büntető Törvénykönyvről,
9) 1959. évi IV. törvény a Polgári Törvénykönyvről,
10) 218/1999. (VI. 30.) Korm. rendelet az egyes szabálysértésekről,
11) 79/1995. (VI. 30.) Korm. rendelet a minősített adat kezelésének rendjéről,
12) 43/1994 (III. 29.) Konn. Rendelet a rejtjel tevékenységről,

12.1.1.2. Szabványok és ajánlások:

1) ISO/IEC 17799:2000 Information Technology - Code of pratice for information security management (Az informatikai biztonság kezelési kézikönyve),
2) ISO/IEC 15408:1999 Information Technology Security techniques (Informatikai biztonsági technikák) (Common Criteria)
3) Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 8. számú ajánlás - Informatikai Biztonsági Módszertani Kézikönyv,
4) MeH ITB 12. számú ajánlás - Informatikai Rendszerek Biztonsági Követelményei,
5) MeH ITH 16. számú ajánlás-Common Criterie (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertana,
6) Trusted Computer System Evaluation Criteria (TCSEC - Biztonságos Számítógépes Rendszerek Értékelési Kritériumai - "Narancs Könyv'),
7) Information Technology Security Evoluation Criteria (ITSEC - Információtechnológiai Biztonsági Ércékelési Kritériumok),
8) Control Objectives for Information and Related Technology (COBIT-ISACA ajánlás),
9) Az Adatvédelmi biztos ajánlása (2001. II. 1.) az intemettel összefüggő adatkezelések egyes kérdéseiről,
10) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal dara and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communication)

13.Irodalom:

[1] Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság (továbbiakban MeH ITB) *"Az informatikai rendszerek biztonsági követelményei"* című 12. számú ajánlása

[2] *'A Code of Practice for Information Security Management"* (Az informatikai biztonság menedzsmentjének gyakorlati kódexe) ISO/IEC 17799:2000 szabvány

III. Mellékletek

1.sz. melléklet: Titoktartási nyilatkozat

2.sz. melléklet: Kockázatvállalási nyilatkozat

3.sz. melléklet: Alkalmazás kriptográfiai adatlap

....§ (2) A jelen utasítás 2012. szeptember .....án lép hatályba, amelyet a helyben szokásos módon a munkavállalókkal ismertetni kell, illetve a szervezeti egységek vezetői részére át kell adni.

2012. október 10

.....

Szarvas Ferenc
vezérigazgató
BVK HOLDING Zrt.