Nemzeti Fejlesztési és Stratégiai Intézet Kft.

Informatikai Biztonsági Szabályzat

Verziószám: 1.

Hatályos: 2016. július 4.

Jóváhagyta:

Tartalom

1. Általános rendelkezések

1.1 Az Informatikai Biztonsági Szabályzat célja

A Nemzeti Fejlesztési és Stratégiai Intézet Kft. (a továbbiakban: Szervezet) Informatikai Biztonsági Szabályzatának (a továbbiakban: IBSZ) célja, hogy a vonatkozó jogszabályokkal összhangban meghatározza azokat az alapelveket, amelyeket a Szervezet informatikai rendszere által kezelt, informatikai eszközökön tárolt adatok bizalmassága, sértetlensége és folyamatos rendelkezésre állása igényel, mindemellett meghatározza a vezető és a biztonságért felelős személyek jogosultsági szintjét, feladatait, illetve kötelezettségeit.

A szabályzat célja továbbá, hogy közvetetten elősegítse a társaság stratégiai feladatainak megvalósítását azzal, hogy ahhoz biztosítja az informatikai biztonságot. További cél, hogy egységes elvek, keretszabályok kerüljenek megalkotásra és ezek értelmezése is egységes legyen a rendszer fejlesztői, üzemeltetői és felhasználói számára biztonsági tevékenységük összehangolása érdekében.

További feladat, hogy egységes irányelvek kerüljenek meghatározásra az új alkalmazások/ rendszerek elkészítéséhez, kialakításához, illetve a régiek felülvizsgálatához.

Tekintettel arra, hogy a kockázatok teljes körű megszüntetése nem lehetséges - azt csupán megelőzni, vagy kezelni lehet –, ezért a veszélyekkel számolni kell és a kockázati tényezőket kontroll alatt tartva minimalizálni szükséges, biztosítva ezáltal az informatikai rendszerek zavartalan működését.
A kockázatok kezelése során figyelemmel kell arra lenni, hogy a különböző kockázatok különböző szintűek (magas, közepes, alacsony) és a megfelelő kockázati szinthez a megfelelő védelmi szintet szükséges rendelni.

Jelen IBSZ kiemelt célja tehát, hogy a Szervezet működésében résztvevő informatikai rendszerekre specializálva, a megelőző kontrollok meghatározásával minimum szintre csökkentse az informatikai biztonsági kockázatok bekövetkezésének valószínűségét, valamint a kockázati szintnek megfelelő intézkedéssel megvizsgálja a lehetséges veszélyeket és javaslatot tegyen, valamint feltételrendszert alakítson ki azok kezelésére.

A megelőző kontrollok közé azon technikákat soroljuk, amelyekkel megkísérelik elkerülni valamilyen vészhelyzet bekövetkezését. Többek között jelen szabályzat is ide sorolható, tekintettel arra, hogy jelen szabályzat is megelőző intézkedésekre irányul.

Jelen IBSZ feladata továbbá, hogy

- társasági szinten határozza meg a jogszabályokkal összhangban a biztonsági eljárásokat, a felelősöket, az ellenőrzések rendjét és az esetleges szabálysértésekre vonatkozó alapelveket.
- térjen ki a fejlesztés, karbantartás, beszerzés, karbantartás és üzemeltetés általános biztonsági szabályaira,
- rögzítse az informatikai rendszerek fejlesztése területén a biztonsági rendszerek tervezésére, megvalósítására, tesztelésére, bevezetésére, követésére és a minőségbiztosítására vonatkozó általános szabályokat,
- foglalkozzon a vírusvédelemmel, a hálózatok, a külső hozzáférések, az üzletmenet-folytonosság, a változásmenedzsement, a biztonságmenedzsment és az ellenőrzések általános szabályaival,
- részletezze az IT rendszerek fejlesztésével, beszerzésével, karbantartásával és üzemeltetésével érintett külső és belső szervezetek (felhasználók, partnerek, szállítók, együttműködő egyéb partnerek) együttműködésének szervezésével, kiszolgálásával kapcsolatos biztonsági szabályokat, különös tekintettel az outsource szervezésmóddal összefüggő biztonsági előírásokra.

Az IBSZ fő célkitűzése továbbá, hogy a Szervezet speciális tevékenységéből adódóan az alábbi Pályázat kezelői Informatikai Rendszerek biztonsági előírásait megfelelően szabályozza és kijelölje azon szervezeti egységeket, amelyek ezen szabályok betartásáról gondoskodni kötelesek:

- "Otthon Melege Program" - "Háztartási nagygépek (hűtő és fagyasztó) energia megtakarítást eredményező cseréje alprogram"
- "Otthon Melege Program" - "Háztartási nagygépek (mosógép) energia megtakarítást eredményező cseréje alprogram"
- "Otthon Melege Program" - "Társasházak energia megtakarítást eredményező korszerűsítésének, felújításának támogatása alprogram"
- "Otthon Melege Program" - "Fűtéskorszerűsítés (kazáncsere), Háztartási nagygépek energia megtakarítást eredményező cseréje, valamint a Homlokzati nyílászárócsere alprogramjai"

A jelen szabályzat előírásai alapján az érintett szervezeti egységek az általuk használt informatikai rendszerre vonatkozóan – amennyiben a rendszer használatához kiemelt kockázatok tartoznak – köteles rendszerszintű IBSZ megalkotására. A rendszerszintű szabályozások a jelen IBSZ elveit kell, hogy kövessék, azt kell, hogy lebontsák az adott rendszerre vonatkozóan. Konkrét, az adott területre, illetve rendszerre érvényes és értelmezhető szabályokat tartalmaznak. Megnevezik az egyes feladatok végrehajtásában kompetens beosztásokat, szervezeteket (felelős, irányító, végrehajtó, ellenőrző).

A részletes szabályok kialakítása függ az egyes informatikai rendszerek jellegétől. Az elkészített rendszerszintű IBSZ-ek, mint a technikai feladatokat részletesen meghatározó szabályzatok az

egyes, érintett alkalmazások, illetve szervezeti egységekre kerülnek kiadásra és az adott területen a jelen IBSZ-vel együttesen kerülnek alkalmazásra, azzal együtt érvényesek.

1.2 Az Informatikai Biztonsági Szabályzat hatálya

1.2.1 Informatikai Biztonsági Szabályzat hatálya személyekre

Az IBSZ személyi hatálya közvetlenül kiterjed a Szervezet valamennyi teljes vagy részmunkaidős, valamint egyéb szerződéses jogviszonyban dolgozójára. Az IBSZ hatálya közvetetten kiterjed továbbá a Szervezet informatikai rendszerének, valamint ahhoz kapcsolódó üzemeltetési és karbantartási feladatokat ellátó cégekre, vállalkozókra, magánszemélyekre (a továbbiakban: Szerződéses partnerek). Az informatikai biztonság szempontjából elengedhetetlenül fontos tényező, hogy az érintettek megismerjék az IBSZ megfelelő pontjait és eleget tegyenek az IBSZ rájuk vonatkozó előírásainak, és maradéktalan betartsák azt.
Ezen feladatról a beszerzésekben közreműködő valamennyi szervezeti egységet, vagy közbeszerzéssel foglalkozó ügyvédet is értesíteni szükséges annak érdekében, hogy a kötelezettség teljesítését, már az ajánlati felhívás is tartalmazza a prudens eljárás érdekében.

Az IBSZ hatálya kiterjed minden olyan magánszemélyre, valamint gazdasági szervezetre, aki munkavégzése során bármilyen informatikai eszközzel a Szervezet informatikai infrastruktúrájához csatlakozik, illetve azt igénybe veszi.

1.2.2 Informatikai Biztonsági Szabályzat hatálya időben

Az Informatikai Biztonsági Szabályzatot évente, vagy jelentősebb infrastrukturális változás esetén időközben felül kell vizsgálni és szükség esetén módosítani kell, mind Szervezeti, mind informatikai szakmai szempontok szerint. Jelen szabályzat határozatlan időre jött létre és elfogadásának napjától visszavonásig hatályos.

1.2.3 Informatikai Biztonsági Szabályzat hatálya eszközökre

Az IBSZ tárgyi hatálya kiterjed:

- a védelem alatt lévő elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és fizikai megjelenési formájuktól függetlenül,
- a Szervezet teljes számítógépes hálózatára és annak valamennyi elemére;
- a számítógépes hálózathoz illeszthető eszközre (pendrive, mobiltelefon, router, stb.)
- a Szervezet tulajdonában lévő vagy az általa bérelt valamennyi informatikai berendezésre és azok környezetére, legyenek azok informatikai eszközök vagy sem
- az informatikai eszközök összes műszaki dokumentációjára,

- az informatikai folyamatban szereplő fejlesztési, szervezési és programozási dokumentációra,
- a rendszer- és felhasználói programokra,
- az adatok felhasználására vonatkozó utasításokra,
- az adathordozók tárolására és felhasználására.

A szabályozás tárgyi hatálya kiterjed a társaság által üzemeltetett valamennyi informatikai eszköz teljes életciklusára (előkészítés, megvalósítás, üzemeltetés és a rendszerből való kivonás fázisaira), az egyes informatikai elemekre és azok környezetére, az egyes informatikai rendszerek infrastruktúrájára és alkalmazási szintjeire, a központi és a munkahelyi számítástechnikai erőforrásokra.

1.3 Az Informatikai Biztonsági Szabályzatban használt fogalmak

Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

Adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Adattovábbítás: ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Adatkezelő: az a természetes vagy jogi személy, aki, vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: az a természetes vagy jogi személy, aki, vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

Adatvédelem: A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról szóló törvény hatálya alá eső adatkörök védelme.

Adatbiztonság: az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Aktív hálózati eszköz: kapcsolók (switch-ek), forgalomirányítók (router-ek), vezeték nélküli hozzáférési pontok és egyéb eszközök, amelyek segítségével a hálózat üzemvitele biztosítható.
BCP: Business Continuity Plan – Üzletmenet (működés) folytonossági terv, az üzletmenet (működés) fenntartása érdekében teendő intézkedések összessége. Részletes akciótervek kidolgozását jelenti arra az esetre, ha az adott üzleti folyamat vagy alkalmazás végrehajtása, működtetése valamilyen természeti vagy ember által okozott katasztrófa miatt akadályokba ütközik (például hosszabb időre kiesik egy rendszer). Ekkor alternatív módszereket kell kidolgozni a munkavégzésre (például telefonos vagy papír alapú üzenet továbbítás email helyett).

Bizalmasság: az adat és az adathordozó azon tulajdonsága, amely arra vonatkozik, hogy az adatot csak a jogosultak ismerhessék meg, illetve rendelkezhessenek azok felhasználásáról.

Biztonsági esemény: Az informatikai rendszer védelmi állapotában beállt illetéktelen változás, melynek hatására az informatikai rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása, vagy rendelkezésre állása elvész, illetve megsérül.

Csomópont: szerver feladatokat ellátó eszközök és aktív eszközök csoportja, az informatikai szolgáltatások ellátására.

DNS (Domain Name Service): a domainneveket és IP vagy más hálózati címeket egymáshoz rendelő szolgáltatás.

DRP: Disaster Recovery Plan – Katasztrófa utáni helyreállítási terv, magába foglalja az üzletmenet (működés) szempontjából kritikus adatok, hardver, és szoftver működésének újraindítását természeti vagy ember által okozott katasztrófák esetén. Részletes akciótervek kidolgozását jelenti, melyeknek célja hogy a rendszerek újra működőképesek legyenek (például hardver beszerzés, üzembe helyezés, installálás stb.).

Felhasználó: az a személy, aki az informatikai rendszer valamely szolgáltatását igénybe veszi.

Felhasználói azonosító: Az intézményi címtárban tárolt egyedi azonosításra szolgáló rövid karaktersorozat.

Funkcionalitás: az informatikai rendszer megfelelő tervezésének és üzemeltetésének köszönhetően az adat tartalmi és formai használhatóságának biztosítása a funkcionális használat követelményeinek megfelelően.

Hálózat: felhasználói számítógépek és/vagy szerverek közötti adatátvitelt biztosító passzív és aktív eszközökből álló infrastruktúra.

Hitelesség: az adat és az adathordozó azon tulajdonsága, amely arra vonatkozik, hogy az adat bizonyíthatóan az elvárt forrásból származik és megfelel a rá előírt valamennyi alaki és tartalmi követelménynek.

IBSZ: Informatikai Biztonsági Szabályzat, a jelen dokumentum rövidítése.

Incidens: A szolgáltatás standard működésétől eltérő esemény, mely fennakadást vagy minőségcsökkenést okoz, vagy okozhat a szolgáltatásban.

Informatikai Biztonsági Szabályzat (IBSZ): A Szervezet informatikai biztonsági szabályzata minden munkatárs és választott tisztségviselő számára egységes értelmezésben azt határozza meg, hogy az informatikai rendszerek által kezelt adatok bizalmasságának, hitelességének, sértetlenségének, és rendelkezésre állásának megőrzésével kapcsolatosan milyen elveket kell követni, illetve milyen követelményeket szükséges teljesíteni.

Informatikai biztonság: Az informatikai biztonság az az állapot, amikor az informatikai rendszer által kezelt adatok védelme — bizalmasság, hitelesség, sértetlenség, rendelkezésre állás és funkcionalitás szempontjából — zárt, teljes körű, a kockázatokkal arányos és folyamatos.

Informatikai biztonsági ajánlások: Jelen szabályzatban az Informatikai Biztonságpolitika alapján az Európai Közösség ITSEC, valamint a logikai védelem szempontjából ezzel harmonizáló Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 12. számú ajánlása (továbbiakban: MeH ITB 12. ajánlás) meghatározó jellegű.

Információ-technológiai (IT) rendszer: (information technology (IT) system) információs rendszer (hardver és szoftver) nemzetközi szakkifejezése.

IT szolgáltatás: bármilyen, a Szervezetnél használt vagy bevezetni szándékozott IT rendszerrel összefüggő, azzal kapcsolatos szolgáltatás.

Információ védelem: Az informatikai rendszerekben kezelt adatok által képviselt tartalom (emberi értelmezés=információ) bizalmasságának, hitelességének és sérthetetlenségének védelme.
Informatikai erőforrások: a hardver, szoftver eszközök összessége.

Informatikai biztonság: Az informatikai biztonság a védelmi rendszer olyan, a Társaság 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.

Információvédelem: az informatikai rendszerek által kezelt adatok által hordozott információk védelme a bizalmasság, a hitelesség és a sértetlenség sérülése, elvesztése el-len. Az információvédelem az informatikai biztonság egyik alapterülete.

IP telefónia: olyan számítógép-hálózati alkalmazás, amely dedikált eszközök (készülék és központ) segítségével telefonszolgáltatást tesz lehetővé. Ez a hagyományos telefonközpontokat felváltó számítógépes rendszer.

ITIL: Information Technology Infrastructure Library – egy olyan nemzetközileg elfogadott keretrendszer (de facto szabvány), mely a magas szintű IT szolgáltatások nyújtását a „legjobb gyakorlatok gyűjteménye" elv mentén szabályozza. Az ITIL olyan üzleti (működési) folyamatokat ír le, melyek mind a minőségi mind a gazdaságos szolgáltatás elérését támogatják az informatika területén.

Kockázattal arányos védelem: Ha egy kellően nagy időintervallumban a védelem költségei arányosak a potenciális kárértékkel.

Kockázat: A fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázatot a kárnagyság és a bekövetkezés gyakoriság szorzataként definiáljuk egy megadott időtávon.

Központi címtár: az egyetem dolgozóinak felhasználói adatit tároló LDAP adatbázis.

Központi szolgáltatások: levelezés, címtár, fájl kiszolgálás, Web szolgáltatás, névszolgáltatás, stb.

Least privilege (legkevesebb jog): alapelv, amely szerint minden szubjektumnak azt, 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.

LDAP (Light Weight Directory Access Protocol): nyílt szabványú címtár struktúra leíró nyelv.

Megbízható működés: Megbízható a működés, ha az illető informatikai rendszer(ek) és az általuk kezelt adatok folyamatosan rendelkezésre állnak és funkcionalitásuk önmagával azonos marad.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

Passzív eszközök: hálózati kábelezés és csatlakozók. Probléma: A probléma egy állapot, mely gyakran több hasonló tünetet produkáló incidens alapján ismerhető föl. A probléma azonosítható lehet egyetlen jelentős incidens alapján is, mely valamilyen hibára utal, melynek oka nem ismert, de hatása jelentős.

Rendelkezésre állás: az informatikai rendszer elem – 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.

SLA: Service Level Agreement – Szolgáltatási szint megállapodás egy olyan írásos megállapodás, mely két fél között jön létre: a szolgáltató (a jelen szabályzat alkalmazása során a szolgáltatásért

felelős szervezeti egység) és a szolgáltatás felhasználója között. Az SLA meghatározza a két fél között nyújtandó szolgáltatás tartalmát és fel-tételeit.

Számítógép: olyan informatikai eszköz, amelyet a felhasználó a napi munkája során használ, és amellyel igénybe veheti a hálózat szolgáltatásait.

Szerver feladatokat ellátó eszköz: olyan számítógépek, szoftverek, vagy speciális eszközök, amelyek különböző szolgáltatásokat biztosítanak más számítógépek számára.

Szerverszoba: fokozottan védett, naplózott bejutású, klimatizált, zárt helyiség, ahol a folyamatos működés feltételei az informatikai erőforrások számára biztosítottak.

Teljes körű védelem: teljes körű a védelem, ha az illető informatikai rendszer valamennyi elemére kiterjed.

Szolgáltatásért felelős szervezeti egység: az IT és telekommunikációs szolgáltatás nyújtására alkalmas infrastruktúrával rendelkező önálló szervezeti egység, mely az adott szolgáltatás nyújtásának feltételeit a felhasználók számára nyilvánosságra hozza.

Tűzfal: olyan kiszolgáló eszköz (számítógép vagy program), amelyet a lokális és a külső hálózat közé, a csatlakozási pontra telepítenek, annak érdekében, hogy az illetéktelen behatolásoknak ezzel is elejét vegyék. Ezzel együtt lehetővé teszi a kifelé irányuló forgalom ellenőrzését is.

Üzletmenet-folytonosság és katasztrófa-elhárítás tervezés: Az informatikai rendszer és a benne kezelt adatok, valamint a környezetüket képző összes rendszerelem csoportra vonatkozó védelmi intézkedések meghatározására irányuló tervezési tevékenység üzemzavarok és katasztrófa esetére. A védelmi intézkedések érvényesítésével az adatok védelme és/vagy visszaállíthatósága valósítható meg üzemzavar vagy katasztrófa események estén. Angol nyelvű elnevezése: Business Continuity Planning (rövidítése: BCP) és Disaster Recovery Planning (rövidítése: DRP).

VLAN: a hálózat egy meghatározott része a feladatoknak megfelelően, logikai csoportba van szervezve.

VPN szolgáltatás: speciális hálózati elérés, amely az egyetem hálózatához titkosított, és hitelesített kapcsolatot tesz lehetővé a világ bármely részéről.

WiFi (Wireless Fidelity): olyan szabványos vezeték nélküli adatátviteli technika, amely a 11-54 Mbps-os tartományban működik. A szabad frekvenciatartományt használó rendszer átviteli sebessége nagymértékben függ a rádióhullámok terjedési környezetétől (akadályok, távolság). Legtöbb notebook, laptop, palmtop számítógép gyárilag rendelkezik ilyen kapcsolódási lehetőséggel.

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

2. Az Informatikai Biztonsági Szabályzat elhelyezkedése a Szervezetben

Az Informatikai Biztonsági Szabályzatot az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat,
- Leltározási és selejtezési szabályzat,
- Adatvédelmi Szabályzat,
- Számviteli politika
- 2003. évi C. törvény
- 2013. évi L. törvény és kapcsolódó 77/2013 NFM rendelet
- NAIH -72534/2014

3. Az Informatikai Biztonsági Szabályzat által védett javak

A biztonsági szempontokat és védelmi intézkedéseket a Szervezet informatikai rendszerének egymással összefüggő és együttműködő elemei határozzák meg az alábbi tényezők alapján:

- rendszerelemekkel kapcsolatba kerülő valamennyi személy
- hardver- és szoftverelemek
- adathordozók, adatok

3.1 A védelem tárgya

A biztonsági intézkedések kiterjednek az alább felsoroltakra:

- személyhez fűződő vagyoni jogok,
- adatok és adathordozók a megsemmisítésükig,
- informatikai eszközök üzemeltetéséhez szükséges dokumentumok és okmányok
- adatfeldolgozó programrendszerek, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységek előírásszerű felhasználása, reprodukálhatósága,

- a rendszer elemeinek elhelyezésére szolgáló helyiségek,
- az alkalmazott hardver eszközök és azok működési biztonsága.

4. Az Informatikai Biztonsági Szabályzatban alkalmazott védelmi eszközök

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

4.1 A védelem eszközei

Az IT üzemeltetésre szerződött szakcég (a továbbiakban: IT szakcég), illetve az elektronikus információs rendszer felhasználói információbiztonsági kérdésekben közvetlenül a Szervezet vezetőjének tartozik beszámolási kötelezettséggel. Ahhoz, hogy az érintett személyek felkészülhessenek a lehetséges informatikai veszélyhelyzetekre, fenyegetésekre alapvető biztonsági követelményekről és azok betartásáról szóló képzést kapnak.

Az IT szakcég feladata és felelőssége az információbiztonság szintjének folyamatos ellenőrzése, a biztonsági incidensek megelőzése, illetve a bekövetkező incidensek hatásának mérséklése, valamint az okok feltárása, a felelősök azonosítása, továbbá a későbbi beszerzések, az informatikai fejlesztések során a biztonsági követelmények érvényre juttatása. Az IT szakcég feladatai, elvégzendő munkái IT biztonság szempontjából az alábbiak:

- az informatikai rendszereket fenyegető veszélyforrások következtében fellépő kockázatok meghatározása, illetve csökkentése,
- a védelmi rendszer tervezésében való részvétel,
- biztonsági szabályok meghatározása és betartatása,
- védelmi rendszer működtetése,
- az IT biztonság rendszeres felülvizsgálata,
- az informatikai hálózat biztonságának folyamatos ellenőrzése,
- informatikai rendszer változásainak nyomon követése,
- adatvédelmi felelőssel egyeztetve és együttműködve részt vesz a biztonsággal összefüggő szakmai munkában,
- felhasználói bejelentések kivizsgálása, illetve javaslattétel a további intézkedésekre,

- időszakos ellenőrzés az IT Biztonsági Szabályzat betartása kapcsán,
- a szabályzatban foglalt előírások ellen vétkezőkkel szembeni felelősségre vonási eljárás kezdeményezése.

Az IT üzemeltető feladatait a vállalkozási szerződésében kell részletesen szabályozni, pontosan rögzítve a hatásköröket és vállalt felelősségeket. Az üzemeltetési szerződésben rögzíteni kell, hogy az IT üzemeltető felelős a következő biztonsági szempontból fontos feladatokért:

- az informatikai rendszer üzemeltetéséhez szükséges erőforrások biztosításáért,
- az informatikai rendszer folyamatos működéséért,
- az informatikai rendszer biztonságának folyamatos felülvizsgálatáért,
- Disaster Recovery Plan kidolgozásáért és frissítésért,
- informatikai és informatikai biztonsági ajánlásokat tegyen a szervezet felé,
- Szervezet **ITIL** könyvtárának karbantartása és fejlesztése a szervezet változásait követve.

Az IT üzemeltetési szerződésben pontosan meg kell határozni a Rendszergazda feladatait, hatáskörét és felelősségi köreit. A rendszergazda felelőségi köreinek ki kell terjedjenek a következő pontokra:

- biztonsági kockázatának minimalizálásáért a hálózat és az eszközök tekintetében,
- szervezet informatikai hálózatának fizikai és informatikai felügyelete,
- aktív hálózati eszközök felügyelete és frissítése,
- rádiós és WiFi hálózatok felügyelete,
- az üzemeltetési feladatokat veszélyeztető és akadályozó tényezők felismeréséért és jelentéséért, a **BCP**-nek megfelelő infrastruktúra biztosítása,
- felhasználók kezelése, LDAP szerver karbantartása,
- az informatikai szabályok betartásáért, incidensek azonnali jelentésért,
- új hardver eszközök informatikai biztonsági politikának megfelelő beállítása,
- biztonsági javítócsomagok telepítése,
- biztonsági beállítások helyességének sértetlenségének folyamatos biztosítása,
- a személyes használatba adott számítógépek és informatikai eszközök esetében a:
  - biztonsági frissítések, javítócsomagok telepítése,
  - személyes jogosultság beállítása,
  - rábízott érzékeny adatok védelme.
- informatikai csomópontok, Szerverszoba fizikai és informatikai, Tűzfal zárása védelme,

- DNS szerverek és lokális DNS nevek karbantartása és naprakész frissítése,
- felhasználók és külső kapcsolatok védelme és felügyelete a központi címtárban,
- IP és analóg vonalas telefonok üzemeltetése, kapcsolatok intaktságának felügyelete.

A fenti feladatok megvalósítása érdekében folyamatosan át kell tekinteni:

- az irányelvek biztonsági hatékonyságát zártság és teljesség szempontjából (vagyis: minden lényeges kockázatot, minden védeni való rendszerelemet meghatároztunk-e és csak azokat határoztuk-e meg?),
- az ellenőrző és biztonsági eszközök, eljárások érvényességét, költséghatékonysági szempontból (kockázati arányosság, illetve folytonossági szempontból),
- a technológiai változások hatását.

4.2 Az Informatikai Biztonsági Szabályzatban kezelt kockázatok és kezelésük

4.2.1 Környezeti infrastruktúra kockázatai

Védett helyiségnek kell tekinteni azokat a helyiségeket, ahol a bizalmas adatok feldolgozására, tárolására alkalmazott informatikai erőforrások találhatók. A védett területek zárt területnek minősülnek, ezért védelmükről ennek megfelelően kell gondoskodni.
Védett területnek minősül a szerverszoba (szerver, központi szünetmentes áramforrás és az aktív hálózati elemek), valamint az irodai szobák.
A szolgáltatásokat biztosító, szerver feladatokat ellátó eszközöket közös helyiségben, szerverszobában kell elhelyezni. A szerverszoba biztonsági szempontból fokozottan védett helyiségnek minősül, melyekbe kizárólag ellenőrzött módon, az arra kijelölt személyek juthatnak be.

A szerverszobával szemben támasztott követelmények:

- zárt helyiség,
- behatolás elleni védelem biztosítása, csak arra feljogosított személyek léphetnek be naplózott beléptetés mellett,
- légkondicionált helyiség, az üzembiztonság és a megfelelő hőmérséklet fenntartása érdekében,
- megfelelő szünetmentes áramforrás biztosítása, az üzembiztonság fokozása érdekében,
- előírásnak megfelelő és hatóság által ellenőrzött füst-, és tűzérzékelő, a vagyonvédelem és az üzembiztonság érdekében.

A szerverszobában történő munkavégzés előírásai:

- a szerverszobába csak arra feljogosított személy léphet be,
- szerverszobában munka csak feljogosított személy által vagy annak jelenlétében végezhető.

A szerverszoba zárt helyisége zárt, a zárt helyiség kulcsa, a Központi Titkárság megőrzésében van, kizárólag az arra jogosult személy veheti át.

Általános alapelvek a számítógép használatra vonatkozólag:

- a Szervezetnél működő számítógépek csak rendeltetésszerűen, munkavégzés céljából használhatók,
- a munkavállalók csak a munkájuk végzéséhez szükséges rendszerekhez kaphatnak jogosultságot,
- a számítógépek használata során fokozott figyelmet kell fordítaniuk a tűz-, érintés- és munkavédelmi szabályokra,
- nem szabad letakarni a számítógépek, monitorok szellőzőnyílásait,
- kiemelt figyelmet kell fordítani az elektromos csatlakoztatások használata során az áramütés veszélyének,
- nem szabad megbontani az IT hálózat csatlakoztatásait,
- a számítógépekre csak az érvényes szabályozás mellett telepíthetők szoftverek, melyet a megbízott informatikai személynek kell elvégeznie. Azokban az esetekben, amikor a számítógép személyes használatban van, a felhasználó felelőssége, hogy gépére illetéktelen szoftver ne kerüljön fel, és az elemi biztonsági feltételeknek a számítógép megfeleljen.

A számítógépes munkaállomások használata során a felhasználóknak a következő általános szabályokat be kell tartaniuk:

- személyes használatban lévő számítógépen felhasználói jogokkal kell rendelkeznie,
- felhasználói jogaihoz tartozó jelszóval védeni tudja számítógépe integritását,
- illetéktelen személynek felhasználói jogát át nem adhatja,
- közepes vagy magas biztonsági kockázattal járó feladatvégzésekor a számítógépét senkinek nem engedheti át, információbiztonsági kockázatot nem idézhet elő,
- biztonsági frissítésről gondoskodnia kell,
- vírusvédelmi szoftver telepítéséről és frissítéséről gondoskodnia kell,
- működő számítógépet csak jelszóval védett képernyővédő használatával hagyhatja magára.

4.2.2 Humán kockázatok

4.2.2.1 Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

4.2.2.2 Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

4.2.3 Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

4.2.3.1 Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

4.2.3.2 A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

4.2.3.3 A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

4.3 Az Informatikai Biztonsági Szabályzatban általánosan kezelt védelmi eszközök

4.3.1 A számítógépek és szerverek védelme

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:

- menteni a még használható anyagot,
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

4.3.2 Hardver védelem

- a berendezések hibátlan és üzemszerű működését biztosítani kell,
- a működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése,
- az üzemeltetést, karbantartást és szervizelést a Rendszergazda végzi,

- a munkák szervezésénél figyelembe kell venni a gyártó előírásait, ajánlatait, illetve a tapasztalatokat,
- alapgép megbontását (kivéve a garanciális gépeket) csak a Rendszergazda végezheti el.

4.3.3 Az adatrögzítés védelme

- adatbevitel hibátlan műszaki állapotú berendezésen történjen,
- tesztelt adathordozóra lehet adatállományt rögzíteni,
- a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani,
- az adatrögzítő szoftver védelme. Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is,
- hozzáférési lehetőség:
  - a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá),
  - az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti,
  - a szerverek rendszergazda jelszavát az Rendszergazda kezeli,
- az adatrögzítés folyamatához kapcsolódó dokumentációk:
  - adatrögzítési utasítások,
  - ellenőrző rögzítési utasítások,
  - tesztelő és törlő programok kezelési utasításai,
  - megőrzési utasítások,
  - gépkezelési leírások.

4.3.3.1 Az adathordozók nyilvántartása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

4.3.3.2 Adathordozók tárolása

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

4.3.3.3 Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani.

4.3.3.4 Selejtezés, sokszorosítás, másolás

A selejtezést a vállalkozás selejtezésének szabályzata alapján kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni.
Biztonsági illetve archív adatállomány előállítása másolásnak számít.

4.3.3.5 Leltározás

A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

4.3.3.6 Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését.
A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata.

A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak.

A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért és az adatmegőrzési idők betartásáért az IT üzemeltető szakcég illetve a rendszergazda a felelősek.

4.3.4 Szoftver védelem

4.3.4.1 Rendszerszoftver védelem

Az informatikai vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

4.3.4.2 Felhasználói programok védelme

4.3.4.2.1 Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.
Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

4.3.4.2.2 Programok megőrzése, nyilvántartása

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni.

A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a vállalkozásoknak az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 évig meg kell őrizni.

A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.

A programok nyilvántartásáért és működőképes állapotban való tartásáért a vezetők a felelősek.

4.3.5 A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

4.3.5.1 Központi gépek

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.
A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni.

Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

A vásárolt szoftverekről biztonsági másolatot kell készíteni.

4.3.5.2 Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.
Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.
Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

A vállalkozás informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

4.3.5.3 Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.

A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.

Szükséges és elégséges ismeret elvének betartásával kell alkalmazni a hozzáférés védelmi és a jogosultságkezelési intézkedéseket. Minden, az IBSZ hatálya alá eső adatot, a központi informatikai rendszerben, a központi logikai, fizikai rendszerek védelme alatt, központi hozzáférés-védelmi és jogosultság-kezelési rendszer ellenőrzése mellett kell menedzselni az egyedi elszámoltathatóság elvének érvényre juttatásával. A hozzáférés védelmi követelmények a Szervezet informatikai rendszereiben alkalmazandó rendszertől függnek.

Az információkhoz való hozzáférési lehetőséget (jogosultságot) a felhasználó által betöltött munkakör (szerepkör) alapján kell meghatározni (szerepkör alapú hozzáférés). A szerepkörök definiálása a Szervezet munkafolyamatain, szervezeti struktúráján, a hierarchikus és funkcionális kapcsolatokon alapul.

A Szervezetbe újonnan belépő felhasználók informatikai rendszerhez történő hozzáférését az erre szolgáló igénylőlapon az érintett szervezeti egység vezetője kezdeményezi. A felhasználói hozzáférést és az indokoltan kért jogosultságokat a Szervezeti egység vezetője engedélye után a rendszer adminisztrátora hozza létre illetve adja meg.

A Szervezet informatikai rendszereiben működő szolgáltatások (pl.: megosztott könyvtárak) esetén a szolgáltatás indítását engedélyező dokumentumban meg kell jelölni a szolgáltatásért (logikailag) felelős irodavezetőt, és a szolgáltatás tulajdonosát. Amennyiben a feldolgozott adatok, illetve a szolgáltatás jellege alapján a szolgáltatás jellemzően valamelyik szakterületekhez kapcsolható (pl. gazdálkodási adatokról szóló kimutatások, pénzügy, személyügy, stb.), úgy annak a területnek a vezetőjét kell szolgáltatás tulajdonosnak kijelölni. A szolgáltatás tulajdonos által definiált hozzáférés-védelem elve szerint a szolgáltatás tulajdonosa által meghatározott szabályok (engedélyezés) alapján kell az adott szolgáltatáshoz történő hozzáférési jogosultsági kört kialakítani. A szolgáltatás tulajdonosa által megfogalmazott szabályok alapján kell beállítani a megfelelő (pl.: könyvtárak esetén: olvasás, írás, törlés; hálózati nyomtató esetén: hozzáférés) hozzáférési módot. A jogosultságok beállítását az informatikai rendszerben az Üzemeltetői csoport végzi el.

A munkaállomásokon és a szervergépeken technikailag is korlátozni kell az „alternatív" bootolási lehetőségeket (pl.: CD, DVD, USB, ethernet, stb.). Ezekre az eszközöket csak üzemeltetési / karbantartási / javításai célból lehet olyan rendszerrel működtetni, amely nem az üzemszerűen rátelepített operációs rendszer.

A munkaállomásokon és szervereken telepített szoftverek / alkalmazások és szakalkalmazások esetében kiemelt figyelmet kell fordítani az automatikusan létrejövő felhasználókra, hozzáférésekre, jogosultságokra (administrator, guest, root, stb.), ezek kezdeti jelszavát meg kell változtatni és/vagy zárolni kell a használatát. Szintén kiemelt figyelmet kell fordítani a „teszt jelleggel" létrehozott felhasználókra, hozzáférésekre. Ezeket a felhasználókat, hozzáféréseket, amikor használatuk már nem szükséges és indokolt meg kell szüntetni. Amennyiben a hozzáférések szükségesek (pl.: valamilyen rendszerszolgáltatás miatt), úgy legalább a magasabb szintű biztonságukról gondoskodni kell, így vagy át kell őket nevezni, vagy a nem szükséges jogosultságokat el kell venni ezektől a felhasználóktól. Az ilyen felhasználók alapértelmezett jelszavait meg kell változtatni megfelelő erősségű jelszavakra. Szakalkalmazások esetében a fejlesztőknek kerülniük kell az automatikusan felhasználói, alapértelmezett jelszóval működő hozzáférések használatát!

A felhasználó szerepkörének megváltozása esetén (pl.: más osztályra kerül, munkaköre megváltozik) a szervezeti egység vezetőjétől kapott információk alapján a régi szerepkörhöz tartozó jogosultságot a felhasználótól elveszi, majd a szükséges új szerepkörnek megfelelő jogosultságokat megadja neki.

A felhasználó jogviszonyának megszűnése esetén a IT üzemeltető szakcég illetve a rendszergazda által a szervezet vezetőjének kérésére a hozzáférési jogok törlésre kerülnek, a felhasználó az eszközökkel az üzemeltetés felé elszámol.

Az informatikai rendszerhez, alrendszerekhez történő hozzáférési engedélyeket évenként felül kell vizsgálni (pl.: távoli hozzáférések, internet elérés, külső levelezés, stb.). Az esetlegesen már nem indokolt jogosultságokat, hozzáféréseket meg kell szüntetni.

4.3.5.4 Felhasználói fiókok kezelése

A felhasználók kizárólag felhasználói jogosultsággal dolgozhatnak a munkaállomásokon, rendszergazdai jogosultságokat nem kaphatnak. Kivételt képeznek e szabály alól azon szakalkalmazások munkaállomásai, ahol a szoftver működéséhez szükségesek az emelt szintű jogok, itt a zavartalan munkavégzés miatt ez engedélyezett. Az így rendelkezésre álló jogokat a felhasználó nem használhatja semmilyen üzemeltetői feladatra (pl.: programok telepítése, leállítása, stb.), csak és kizárólag a szakalkalmazás használata miatt birtokolhatja ezeket! A munkaállomásokon a felhasználóknak tilos hálózati szolgáltatásként mappákat/fájlokat megosztani. Amennyiben a megosztás szakmailag indokolt, úgy a közvetlen vezető kezdeményezésére az IBF jóváhagyásával a megosztást a munkaállomás adminisztrátora hozza létre. Valamennyi megosztás esetén szigorúan kell meghatározni a hozzáféréseket, törekedni kell arra, hogy ne legyenek általános megosztások. Csak azok a felhasználók/munkaállomások kaphatnak jogot az erőforrások elérésére, amelyeknek ez a munkájukhoz valóban szükséges.

A Szervezet minden szobájában biztosítani kell a hálózati csatlakozás lehetőségét. A hálózati erőforrásokhoz való hozzáférést különböző szintű hálózati jogosultságok biztosítják.

Ezek a jogok az alábbi tevékenységek elvégzését tehetik lehetővé:

- hálózat kezeléséhez szükséges programok közös használata,
- közös nyomtató használata,
- internet böngészés,
- elektronikus levelezés,
- adatbázisok elérésének biztosítása,
- programok, illetve adatok elérésének biztosítása.

A hálózaton található fájlokra, könyvtárakra (mappákra) kioszthatő jogosultságok:

- olvasási jog,
- írási jog,
- törlési jog,
- módosítási jog.

A Szervezeti informatikai rendszerben az egyes számítástechnikai rendszerek, szoftverek készítői által gyárilag a felhasználók részére biztosított védelmi eljárásokat (pl. a WORD jelszavas védelme) a felhasználók – a Szervezeti adatok rendelkezésre állásának biztosítása érdekében – nem használhatják!

A felhasználók számára tilos nem engedélyezett erőforrások, szolgáltatások, jogosultságok megszerzése, vagy ennek kísérlete. Tilos más felhasználó munkájának zavarása, anyagaikhoz történő bármilyen illetéktelen hozzáférés vagy annak kísérlete.

A hozzáférés-védelmi és jogosultság-kezelési elemek, alrendszerek megbízható adminisztrálása érdekében a felhasználói hozzáféréseket megvalósító rendszerek működtetését (ahol a technológia lehetővé teszi) megbízható módon naplózni, és a naplótartalmat az engedélyezett jogosultság igénylések alapján ellenőrizni kell.

A rendszer adminisztrátorát (vagy a rendszer üzemeltetéséért felelős személyt) értesíteni kell, ha:

- a felhasználói fiókokra már nincsen szükség,
- a felhasználók kiléptek vagy áthelyezésre kerültek,
- csoport felhasználói fiókok esetén, ha a csoport tagjai megváltoznak,
- az elektronikus információs rendszer használata vagy az ehhez szükséges ismeretek megváltoztak.

A felhasználói fiókok a fiókkezelési szabályokkal összhangban rendszeres időközönként, legalább évente felülvizsgálandók.

További feladatok:

- meghatározza és azonosítja az elektronikus információs rendszer felhasználói fiókjait, és ezek típusait;
- kijelöli a felhasználói fiókok fiókkezelőit;
- kialakítja a csoport- és szerepkör tagsági feltételeket;
- meghatározza az elektronikus információs rendszer jogosult felhasználóit, a csoport- és szerepkör tagságot és a hozzáférési jogosultságokat, valamint (szükség esetén) az egyes felhasználói fiókok további jellemzőit.

4.3.5.5 Azonosítás és hitelesítés nélkül engedélyezett tevékenységek

A számítógépes munkahely kialakítását követően a számítógépen dolgozók azonosítására, valamint a jogosultságok meghatározására van szükség. A számítógép használatakor egyedi azonosítókat kell alkalmazni, melyek hiányában a munkaállomásra belépés nem lehetséges, így az elektronikus információs rendszeren belül semmilyen tevékenységre nincs lehetőség.

4.3.5.6 Nyilvánosan elérhető tartalom

Nyilvánosan hozzáférhető rendszerként definiálja a Szervezet a publikus weboldalát. Az oldal üzemeltetéséért felelős szervezeti egység vezetőjének gondoskodni kell az azon publikált információk törvényi megfelelőségéről és valódiságáról, sértetlenségéről. Tilos hatályos törvénybe, jogszabályba ütköző, vagy a jó ízlést és közerkölcsöt sértő tartalmat közzétenni. A felkerülő tartalmakat minden esetben ellenőriznie kell a szervezeti egység vezetőjének és csak a jóváhagyása után publikálhatóak az információk. A publikus weboldalnak gondosan szegmentáltnak kell lennie a Szervezet belső hálózatától arra alkalmas eszközzel. Gondoskodni kell a weboldal jogosult használata közben kieszközölhető jogosulatlan elérések megakadályozásáról.

4.3.5.7 A hálózat használatának szabályai

A Szervezet hálózata az alábbi tevékenységekre nem használható:

- a mindenkor hatályos magyar jogszabályokba ütköző cselekmények előkészítése vagy végrehajtása, tiltott haszonszerzésre irányuló tevékenység vagy a szerzői jogok megsértése,
- direkt üzleti célú tevékenység, illetve reklám,
- a hálózat, illetve annak erőforrásainak rendeltetésszerű működését és biztonságát megzavaró, illetve veszélyeztető tevékenység,
- a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, megsemmisítésére vagy bármely károkozásra irányuló tevékenység,
- másokra nézve sértő, vallási, etnikai, politikai vagy egyéb, zaklató tevékenység.

4.4 Internet használatához kapcsolódó biztonsági szabályok

A Szervezet Internet használati jogokkal rendelkező dolgozói a munkájukkal kapcsolatban használhatják a Szervezet által biztosított Internet szolgáltatást.

A belső hálózaton Internet-kapcsolatot létesíteni kizárólag tűzfalon keresztül lehet. Nem megengedett a Szervezet informatikai hálózatába kapcsolt hordozható és asztali munkaállomásokról modemes, mobiltelefonos vagy egyéb kapcsolat létrehozása Internetszolgáltatókkal.

Az Internet szolgáltatás magán célú használata nem megengedett! Az Internet forgalom automatikusan szoftveres alapon szűrésre kerül, így bizonyos tartalmak nem látogathatóak, technológiai eszközzel is tiltásra kerültek.

A technikai szűréstől függetlenül a felhasználóknak az internetes elérés szolgáltatás használatának folyamán az alábbi szabályokat kell betartaniuk:

- Az interneten csak a Szervezeti munkával kapcsolatos oldalakat lehet látogatni. Tilos a pornográf, on-line játék, fogadási oldalak, csevegő oldalak, letöltő oldalak és törvénybe ütköző tartalmakat szolgáltató oldalak látogatása, ezekről letölteni, ilyen tartalmakat és helyeken publikálni, adatokat cserélni, adatot tárolni!
- Az Internetről programok letöltése, telepítése és futtatása nem megengedett. Igény esetén az Üzemeltetői csoport vezetője, előzetes bevizsgálás után engedélyezheti az ilyen programok letöltését és futtatását.
- A bevizsgálás során ellenőrizni kell:
  - a letölteni kívánt program vírusmentességét,
  - a letölteni kívánt program képes-e működni abban a környezetben, amelybe a letöltést tervezik,
  - hogy a letöltés nem sért-e szerzői jogot.
- Informatikai biztonsági megfontolásokból tilos a Szervezetben a nem engedélyezett csevegő programok használata. Ezen programok rezidens futtatása tilos! Ezen programok Szervezeti érdekből történő használatára (pl.: skype – kommunikációs költségek csökkentése) az Informatika vezetője adhat dokumentált módon engedélyt.
- Amennyiben az Interneten keresztüli kommunikáció (főként levelezés) nem titkosított és egyértelműen azonosítható formában (digitális aláírás, fokozott biztonságú elektronikus aláírás) kerül lebonyolításra, nem megengedett bizalmas vagy annál magasabb minősítésű, védett információt kizárólag az Interneten keresztül azonosított feleknek továbbítani mindaddig, amíg a másik fél megbízható, az Internettől független azonosítása meg nem történik.
- Tilos a Szervezettel kapcsolatos belső információk nyilvános oldalakon való bárminemű közzététele.

Informatikai biztonsági vizsgálat, auditálás illetve hibakeresés céljából a Szervezet informatikai rendszereinek teljes hálózati forgalma megfigyelhető és rögzíthető. A felhasználó az IBSZ ismeretéről és elfogadásáról szóló nyilatkozatával elfogadja, hogy a rendszer használata egyben a felhasználó beleegyezését is jelenti a figyelésbe és rögzítésbe. Elektronikus levelek esetén a vizsgálat illetve megfigyelés nem terjed ki a levelek tartalmára. A levelek az alábbi technikai tulajdonságok alapján kerülnek vizsgálatra: kéretlen levelek, vírusokat tartalmazó levelek, informatikai támadásokat megvalósító üzenetek, adathalászatot megkísérlő üzenetek.

Ha a dolgozó Internet használata a munkája elvégzésének rovására megy (pl.: Szervezeti munkához nem kapcsolódó vagy nagy hálózati terhelést okozó tevékenységet folytat vagy biztonsági fenyegetést jelentő oldalakat látogat), az Üzemeltetői csoport vezetője jelzi a dolgozó közvetlen vezetőjének, aki megteszi a szükséges intézkedéseket. Amennyiben az intézkedés

eredménytelen marad, az érintett munkatárs vezetője utasítására a felhasználó Internet hozzáférését az Üzemeltetői csoport részlegesen, vagy teljesen letiltja.

Az Internet-kapcsolatok üzemeltetéséért felelős vezetőnek joga van az Internet-hozzáférés tartalmi, időbeli, sávszélességbeli és szolgáltatásbeli korlátozásához, amennyiben ez az Internet üzleti célú használatának biztosításához szükségessé válik. A korlátozásról a felhasználókat előzetesen tájékoztatni kell.

4.5 E-mail rendszer használatához kapcsolódó biztonsági szabályok

Az e-mail szolgáltatás a Szervezet által a felhasználók részére a Szervezeti elektronikus levelezés céljaira biztosított eszköz. Az e-mail rendszer, valamint a rendszerben előállított, elküldött és megkapott levél is a Szervezet felügyelete alá tartozik.

A Szervezet elektronikus levelezési rendszere korlátozott mértékben, és a szabályzatban rögzített feltételek betartása mellett használható nem Szervezeti levelezés céljára. Az elektronikus levelező rendszer felhasználója a rendszer használatával automatikusan aláveti magát ezeknek a korlátozásoknak.

A Szervezet e-mail rendszerén mindennemű jogszabályellenes tartalom továbbítása és tárolása tilos!

A Szervezet nevében folytatott elektronikus levelezésre kizárólag az erre a célra biztosított elektronikus levelezési cím, a rendszeresített levelező (kliens) program, illetve ezen csak az Üzemeltetői csoport vezetője által engedélyezett levelezési szolgáltatás használható. A beállítások (működési paraméterek) meghatározásáért és beállításáért a Rendszergazda a felelős.

Az elektronikus levelező rendszerben tárolt és továbbított dokumentumok elektronikus kezelésénél is be kell tartani az érvényben lévő ügyviteli, iratkezelési és adatkezelési szabályokat. Minden elektronikus postaládával rendelkező felhasználó köteles elektronikus postaládájának tartalmát figyelemmel kísérni oly módon, hogy legalább a munkakezdéskor és a munkavégzés befejezését megelőzően meggyőződjön róla, hogy érkezett-e új üzenete, és amennyiben igen, akkor azokat érkeztesse, kezelje (tekintse meg, tegye meg a szükséges egyéb intézkedéseket).

Az elektronikus levelező rendszer használata során nem megengedett:

- nagy mennyiségű és méretű, személyes jellegű üzenetek küldése;
- kéretlen reklámok és hirdetések közzététele;
- lánclevelek terjesztése, továbbítása;

- a felhasználóknak a Szervezeti e-mail címüket nem hivatalos minőségben használni (pl.: regisztráció, letöltési weboldalak, on-line játék oldalak, stb.);
- a levelek fejlécének megváltoztatása, hamis levelek küldése;
- olyan üzenetek, illetve csatolt fájlok küldése, továbbítása, amelyek törvénytelenségeket vagy arra való felhívást tartalmaznak, fenyegetőek, összességében sértik a Szervezet jó hírét, általánosan elfogadott erkölcsi szabályba vagy jogszabályba ütköznek;
- a tévesen címzett, másnak szóló levelek felhasználása;
- a Szervezet által biztosított e-mail címre érkező üzenetek átirányítása külső (nem a Szervezet elektronikus levelező rendszerében létrehozott) e-mail címre.

A levelezési rendszer személyes célokra, az elektronikus levelezésre vonatkozó szabályok betartásával és csak akkor használható, ha az nem sérti a Szervezet érdekeit.

Az elektronikus levelek címzése során minden felhasználónak körültekintően kell eljárnia az alábbiak figyelembevételével:

- Csoportos levelező, elosztási lista (pl. „mindenki", „x osztály", „Szervezeti dolgozók") alkalmazása során meg kell győződni arról, hogy valóban szükséges-e minden, a csoportba tartozó címzett részére elküldeni az üzenetet.
- Titokvédelmi vagy egyéb biztonsági, bizalmassági okokból, amennyiben a levelek címzettjei nem szerezhetnek tudomást egymásról vagy egymás e-mail címéről, akkor a levél „Titkos másolat" („BCC": Blind Carbon Copy) kategóriáját kell alkalmazni a címzés során.

A Szervezet a levelező rendszer működését akadályozó mennyiségű és méretű adat elektronikus levélként való továbbítását korlátozza.

4.5.1 A postaládára vonatkozó korlátozások:

Az e-mail felhasználó postaládájának mérete korlátos, melynek méretét a Rendszergazda határozza meg a technikai lehetőségek figyelembe vételével. A meghatározottnál nagyobb postaládára vonatkozó igényt a szervezeti egység vezetőjének jóváhagyásával a Rendszergazdához kell eljuttatni, amely a szükséges vizsgálatok, egyeztetések elvégzését követően dönt az igény kielégítéséről és intézkedik annak beállítása érdekében.

Amennyiben a Szervezeti levelezésben – pontos címzés mellett – az elektronikus levelező rendszertől a kézbesítés során kézbesíthetetlenségre utaló hibajelzés érkezik, akkor a felhasználónak – szükség szerint a Rendszergazda megkeresésével – fel kell tárnia ennek okát annak érdekében, hogy üzenete ne veszhessen el.

Az elektronikus levelek méretét, valamint a levélhez csatolt fájlok típusát a Rendszergazda korlátozhatja a rosszindulatú kódok terjedésének megakadályozása céljából és azért, hogy biztosítsa a Szervezeti levelezés megfelelő szolgáltatási szintjét. A korlátozás miatt nem továbbított levelekről, csatolt fájlokról a küldő értesítést kell, hogy kapjon.

Ismeretlen feladótól érkező, gyanús, csatolt fájlt tartalmazó, vagy ismeretlen linket ajánló (pl.: idegen nyelvű, láthatóan reklámcélú, olyan dokumentumra hivatkozó, amiről a címzett nem tud) elektronikus üzenetek csatolmányait illetve a kapott linkeket nem szabad megnyitni, e leveleket törölni kell.

4.6 Jelszókezelés

A jelszó az informatikai biztonság fontos eleme, ezért az informatikai rendszer valamennyi felhasználójának tisztában kell lennie a megfelelő jelszó használatára vonatkozóan.
Nem szabad egyszerűen megfejthető, az adott személyre jellemző jelszavakat használni, és azokat minden esetben titokban kell tartani.
A jelszót nem szabad leírni és más személy részére továbbítani sem.

4.7 Szankciók

Az IBSZ megsértésének gyanúja esetén kötelezően ki kell vizsgálni az esetet, és a Szervezet vezetőjének, vagy a kijelölt felelősnek meg kell tennie a szükséges intézkedéseket az alább felsoroltak figyelembevételével:

- Az IBSZ előírásainak nem ismerete nem mentesíti az elkövetőt a következmények vállalásának kötelességétől.
- Az IBSZ megszegése esetén az elkövetőt figyelmeztetésben kell részesíteni.
- Az IBSZ-nek egy figyelmeztetést követő ismételt megsértése szándékos elkövetésnek minősül és az eset súlyosságától függően fegyelmi eljárás folytatható le az elkövető ellen.Az IBSZ előírásainak szándékos megsértése esetén az elkövető a Polgári Törvénykönyv előírásai szerint köteles megtéríteni az általa okozott károkat.

5. Záró rendelkezések

Jelen szabályzat határozatlan időre jött létre és elfogadásának napjától visszavonásig hatályos.
Az IBSZ-ben előírt feladatokkal valamennyi érintett dolgozó munkaköri leírását ki kell egészíteni.