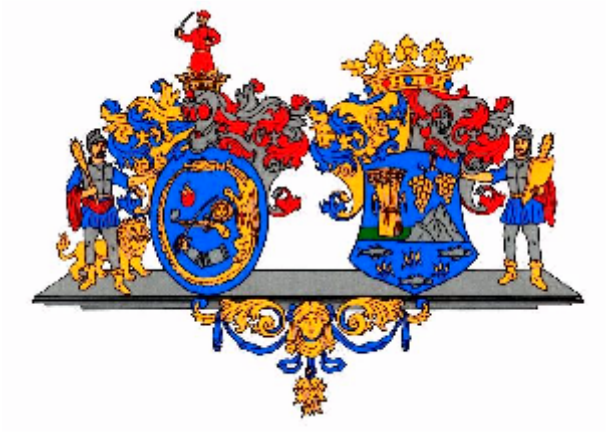


Hajdú-Bihar Megyei Önkormányzat Hivatala

Informatikai Biztonsági Szabályzat

Debrecen

2008.

Bevezető, általános rendelkezések

Az **Informatikai Biztonsági Szabályzat** (a továbbiakban: IBSZ) a Hajdú-Bihar Megyei Önkormányzat Hivatalára (a továbbiakban: Hivatal) általános érvénnyel meghatározza az információ technológiai (a továbbiakban: IT) rendszerekkel és IT eszközökkel kapcsolatos üzemeltetési-, adatvédelmi- és állagmegóvási szabályokat, valamint intézkedéseket.

Az **IBSZ kiadásának célja,** hogy a Hivatal tulajdonában lévő, illetve az általa üzemeltetett IT rendszerek védelmét, valamint az IT rendszerekkel kezelt adatok bizalmasságát, hitelességét, sértetlenségét, rendelkezésre állását a fenyegető veszélyekkel szemben – az IBSZ által előírt intézkedésekkel, szabályozással – biztosítsa.
A Hivatal számítástechnikai rendszereinek adat- és vagyonvédelme a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló módosított 1992. évi LXIII. törvény (a továbbiakban: adatvédelmi törvény) alapján került szabályozásra.

Az IBSZ hatálya

Az IBSZ személyi hatálya kiterjed:

- A Hivatal minden olyan munkatársára, illetve a Hivatallal polgári jogi jogviszonyban álló személyre, aki a munkavégzés, feladat-ellátás során IT eszközökkel, valamint az általuk kezelt adatokkal kapcsolatba kerül, ezekkel az eszközökkel, adatokkal munkát végez.
- A Hivatal informatikai rendszerével, szolgáltatásaival polgári jogi jogviszony alapján vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre a velük kötött szerződésben rögzített mértékben, illetve titoktartási nyilatkozat alapján.

Az IBSZ hatálya a következő területekre terjed ki:

- az adatokra és azok hordozóinak végleges megsemmisítéséig, a közlésre szánt adatoknak a felhasználásáig,
- a személyhez fűződő és vagyoni jogokra,
- a számítástechnikai berendezések, azok környezete, működésük biztonsága és a dokumentációk, a mágneses adathordozók (hajlékony lemezek, kazetták, CD és DVD, illetve merevlemezek, stb.) hiánytalan meglétére, a rajtuk tárolt programok és adatok használhatóságára,
- a számítástechnikával összefüggő műszerek, eszközök meglétére és használhatóságára,
- a számítástechnikai berendezésekhez tartozó okmányokra, programokra és azok dokumentációira,
- az alkalmazott biztonsági intézkedésekre, azok terveire, tartalmi előírásaira és eljárási szabályaira.

Üzemeltetési szabályok

1. IT eszközök fizikai védelme

1.1. Rendészeti védelem

A Hajdú-Bihar Megyei Önkormányzat Hivatala területén a stratégiai fontosságú hardver eszközöket (szerverek, routerek, telefonközpont) külön zárható helyiségben kell elhelyezni. Erre a külön elhelyezésre szolgál a Hajdú-Bihar Megyei Önkormányzat Informatikai Központja (a továbbiakban: IK) által működtetett gépterem, a második emeleti szerver szoba (a továbbiakban szerver szoba), valamint azok a Hivatali helyiségek, amelyekben azok az adatszerverek kerültek elhelyezésre, amelyek a Hivatal működése során használatosak.

A gépterembe, valamint az adatszerverek Hivatali helyiségeibe csak az arra illetékes személyek léphetnek be.

A gépterem, valamint az adatszerverek Hivatali helyiségeinek ajtaját munkaidőn kívül külön kulccsal zárni kell. Kulcsot (kulcsokat) csak az arra illetékes személyek tarthatják maguknál. A géptermek kulcsának egy példányát lezárt borítékban jól őrzött helyen kell elhelyezni (páncélszekrény, annak hiányában pénzkazetta vagy biztonságosan zárható szekrény), az IK által működtetett géptermek esetében az IK által használt helyiségek valamelyikében, a szerver szoba esetében a Fejlesztési Főosztályon az osztályvezető által meghatározott helyen.
A boríték esetleges felbontását jegyzőkönyvben rögzíteni kell.

1.2. IT eszközök üzemeltetésére vonatkozó szabályok

Az IT eszközök rendeltetésszerű működéséért a használatra kijelölt személy (a továbbiakban: felhasználó) a felelős.
A felhasználó köteles a rábízott eszközt a jó gazda gondosságával kezelni, állagmegóvással működtetni, valamint a szándékos és vétlen károkozást elkerülni.
Az eszközök burkolatát felnyitni, azon bármilyen javítást végezni csak az arra kijelölt szakembernek (rendszergazda) van joga.
A felhasználó köteles a részére átadott eszköz üzemeltetési leírását, valamint a hozzá tartozó floppy, CD és DVD adathordozókat az eszköz közelében elhelyezni, esetleges javítás esetén a javítást végző szakember részére rendelkezésre bocsátani, amennyiben ezekre a felhasználónak továbbiakban nincs szüksége a rendszergazdának megőrzésre átadni. Ez alól kivételt képez a licence konstrukcióban vásárolt szoftver, szoftverek tárolása, biztosítása. Ezen szoftverek a javítást végző szakemberek részére rendelkezésre állnak.

1.3. IT eszközök meghibásodására vonatkozó szabályok

A eszközök működése során tapasztalt működési zavarokat a felhasználó köteles azonnal a Lotus Notes rendszerben teendő kiadásával a rendszergazdát értesíteni. **A hibás eszközzel a hiba elhárításáig további munkavégzés nem folytatható.**

1.4. Illetéktelen felhasználás

A Hivatal tulajdonában lévő IT eszközök használata külső személyek számára csak a Hivatal vezetése (megyei főjegyző, aljegyző) által meghatározott engedéllyel és nyomon követhető módon (eszközátadási-bizonylat kíséretében) lehetséges.
Eszközöket javításra átadni csak átvételi elismervény ellenében szabad.
Az értékesítés, selejtezés céljából átadott eszközökön tárolt adatok védelméről az eszközt használó szervezeti egység vezetője gondoskodik.

1.5. Munka- és tűzvédelmi szabályok

A Hivatalon belül egyéb szabályzatban rögzített munka- és tűzvédelmi előírások a kötelező érvényűek.

1.6. A számítógépes hálózattal kapcsolatos szabályok

A Hivatal számítógépes hálózata Cat 5 kábelezésű, strukturált hálózat. A hálózat felügyelete, karbantartása az IK feladata.
A hálózat védelmét Internet irányából Microsoft ISA tűzfalszerver látja el (lásd 2.5.1 Microsoft ISA szerverismertető**).**
A Hálózat és az IK által felügyelt szerverek elvi ábrája az *1. számú mellékletben* található. A szerver szobában található rendszergazda által felügyelt eszközök ábrája az 1/2 számú mellékletben található. Ezen eszözök az 1. számú ábrán található belső hálózathoz csatlakoznak.

1.7. Hardver eszközök beszerzése, selejtezése

Számítástechnikai eszközök beszerzése csak a rendszergazda által jóváhagyott paraméterek alapján történhet.
Selejtezéshez, kiárusításhoz a rendszergazda írásos javaslata szükséges, melyből kiderül a selejtezés - kiárusítás oka, az eszköz állapota illetve becsült értéke.

1.8. Üzemen kívüli eszközök tárolása

Az ideiglenesen üzemen kívüli számítástechnika eszközök tárolása a szerver szobában történik, illetve az erre kijelölt helyen. Ezen helyekre, helyekről a számítástechnikai eszközök áthelyezése a rendszergazda tudtával történhet.

2. Szoftver és adatvédelem

2.1. Hozzáférési jogosultságok

A Hivatalban működő felhasználói rendszerek jogosultságai a *2. számú mellékletben* kerülnek meghatározásra, így a felhasználók változása esetén csak a melléklet kerül módosításra. A 2. számú mellékletben meghatározott rendszerek esetében a jogosultságokat minden esetben a szervezeti egység vezetőjének kezdeményezése alapján a Hivatal vezetője határozza meg.

A hálózati jogosultságok kezelése a Microsoft Active Directory struktúráján keresztül történik. Ennek menedzselése az IK munkatársának, a hivatal megbízásából a rendszergazdának, valamint az általa delegált személyeknek a feladata.
Az ún. administrator jelszavak tárolása zárt borítékban, páncélszekrényben történik. Ennek felbontása csak indokolt esetben, jegyzőkönyv kiállításával történhet.
Az esetleges elfelejtett jelszavak újragenerálását csak a rendszergazda végezheti.
A felhasználóneveket, jelszavakat más, arra illetéktelen személy tudomására hozni tilos.
A hálózaton adatok megosztása csak ellenőrzött módon, a megfelelő felhasználói jogosultságok beállítása mellett történhet.
A rendszergazda, valamint a felhasználó köteles a jelszavát megváltoztatni, amennyiben az illetéktelen személy tudomására jut.

Az Active Directory-ba történő felvétel, törlés, módosítás csak a szervezeti egység vezetőjének kezdeményezése alapján a Hivatal vezetőjének engedélyével történhet.
A felvételkor és módosításkor meg kell határozni, hogy a felhasználónak mely hálózati mappákhoz, illetve, mely rendszerekhez van hozzáférési jogosultsága. A kezdeményezést az erre rendszeresített, a Közérdek mappában közzétett nyomtatvány (*3. számú melléklet*) kitöltésével kell elvégezni.
Törlésre a Hivatalból történő kikörözéskor kerül sor. Ebben az esetben a kikörözés nyomtatvány alapján kerül törlésre a felhasználó.

A Hivatal munkatársai esetében a felvételt, törlést, módosítást a renszergazda végzi. Törlés esetében a felhasználó csak tiltásra kerül, és az IK munkatársa végzi el a tényleges törlést.

A 3. és 4. számú melléklet másolati példányai az erre rendszeresített dossziéban kerülnek tárolásra a szerver szobában.

A Hivatal számítógépein működő operációs rendszerek és irodai szoftverek nyilvántartása a Tárgyi eszköz-nyilvántartó program által történik.

A számítógépeken működő operációs rendszerek, irodai programcsomagok, valamint bármilyen felhasználói programok ellenőrzése történhet szúrópróba szerűen, valamint az éves leltározás kapcsán is. Az ellenőrzésre jogosult személy a rendszergazda, aki minden ellenőrzést dokumentálni köteles. Az így elkészített dokumentumot az elkészítést követő munkanapon köteles a szervezeti egység vezetőjén keresztül a Hivatal vezetője részére eljuttatni.

2.1.1. Active Directory

Címtárszolgáltatás, amely a hálózaton található objektumok adatait tárolja, és hozzáférhetővé teszi ezt az információt a felhasználók és a rendszergazda számára. Az Active Directory lehetővé teszi, hogy a felhasználók egyszerű bejelentkezési eljárás után hozzáférhessenek a hálózat bármely részén található, részükre engedélyezett erőforrásokhoz. Az Active Directory a rendszergazda részére szemléletes hierarchikus képet ad a hálózat felépítéséről, és lehetővé teszi, hogy egyetlen helyről felügyelje az összes hálózati objektumot.

Active Directory - felhasználók és számítógépek
Az Active Directory napi felügyeleti feladatok végrehajtására szolgáló eszköz. Ilyen feladat például a címtárban tárolt objektumok létrehozása, törlése, módosítása, áthelyezése és az azokra vonatkozó engedélyek beállítása, az érintett objektumok pedig a szervezeti egységek,

felhasználók, kapcsolatok, csoportok, számítógépek, nyomtatók és megosztott fájlobjektumok.

Active Directory adatmodell
Egy, az LDAP adatmodellből származó modell. A címtár tartalmazza a különböző egységeket képviselő, attribútumok által leírt objektumokat. A címtárban tárolható objektumokat és objektumosztályokat a séma határozza meg. A séma minden egyes objektumosztály számára meghatározza, hogy azoknak milyen attribútumokkal kell rendelkezniük, milyen további attribútumokkal rendelkezhetnek, és mely osztály töltheti be a szülő szerepét.

2.2. Az adattárolók védelme

Adattároló eszköznek kell tekinteni a hajlékony, cserélhető merev mágneslemezeket, optikai lemezeket, kazettákat, stb. Az adattárolók megóvása a Hivatal minden dolgozójának kötelezettsége. Adattárolót illetéktelen személynek átadni, még megtekintés idejére sem lehet. Az adattárolók megóvása érdekében tárolásukra egy külön vagy erre a célra kialakított helyet kell használni.

2.3. A szoftverek védelme

A Hivatalon belül csak hivatalosan beszerzett, írásbeli igazolással (számla, licence-szerződés) ellátott szoftvereket lehet használni. A szoftverekről – az eszközök nyilvántartásához hasonló módon - számítógépes nyilvántartást kell vezetni, amit a mindenkori helyzetnek megfelelően aktualizálni szükséges.
A beszerzett és használatban lévő programok védelme a Hivatal minden dolgozójának feladata. A Hivatal rendszereiben használatos alkalmazásokat, adatokat külső illetéktelen személyekkel megismertetni, azt átadni, lemásolni tilos. Az alkalmazás során a megszokottól történő eltérés esetén azonnal értesíteni kell arendszergazdát aki köteles a továbbiakról intézkedni. A számítástechnikai rendszerekbe, alkalmazásokba illetéktelen személynek behatolni, bármilyen idegen programot telepíteni, bemásolni tilos.
Biztosítani kell a felhasználók részére a felhasználói programok leírását. Új alkalmazás bevezetésekor biztosítani kell az alkalmazást használó munkatárs továbbképzésen történő részvételét.

2.4. Vírusvédelem

A Hivatalon belül a számítógépek vírusvédelme a VírusBuster szoftvertermékkel valósul meg. A vírusvédelmi szoftver adatfrissítése automatikusan központi menedzsmenttel történik. A felhasználó köteles ellenőrizni, hogy számítógépén mindenkor a legfrissebb vírusdefiníció van-e. Amennyiben eltérést tapasztal, akkor köteles ezt a rendszergazda felé jelezni. A rendszergazda kötelessége a központi menedzsment rendszer ellenőrzése, és szükség esetén beavatkozás annak működésébe.
A felhasználó külső adathordozó használata esetén köteles azon vírusvédelmi vizsgálatot végezni.
Amennyiben a felhasználó vírusra utaló jelenséget tapasztal, köteles azt jelezni a rendszergazdának. Munkavégzés az adott eszközön csak a megfelelő és alapos vírusvédelmi átvizsgálás után lehetséges.
Nem írtható vírus esetén a rendszergazda kötelessége felvenni a kapcsolatot a vírusvédelmi szoftver terméktámogatási osztályával.

Az elektronikus levelezés védelme a Sibary Antigen szoftvertermékkel történik. Ennek felügyelete az IK ilketékes munkatársának feladata.

2.4.1. VirusBuster Professional ismertető

- Kezelhetőség
  Az áttekinthető, komponensekre épülő kezelői felület és az átlátható opciók megkönnyítik a vírusvédelem üzemeltetését.
- Állandó védelem
  A háttérben működő rezidens védelem folyamatosan őrködik a számítógépek vírusmentessége fölött.
- Teljes körű támogatás
  A megszokott VirusBuster minőséget és megbízhatóságot a magas szintű támogatás és kiegészítő szolgáltatások biztosítják.
- Automatikus frissítések
  A védelem naprakészségét az automatizálható vírusadatbázis- és programfrissítő garantálja.
- Kiterjesztett állományvédelem
  A program lehetőséget nyújt az állományok írás-, átnevezés- és törlésvédelmére, amely számos vírus esetében az egyetlen megoldást jelenti.
- Áttekinthető naplózás
  A program egyes részei egy központi adatbázisba gyűjtik az eseményeket, így minden információ könnyen és gyorsan hozzáférhető.

2.4.2. Sybari Antigen for Microsoft Exchange ismertető

- Megelőző védelem
  Míg a hagyományos vírusvédelmi termékek csak azután ellenőrzik a leveleket, amikor azok már elérték a hálózat érzékeny pontjait, az Antigen újszerű megoldást alkalmazva az üzeneteket még az Information Store-ban átvizsgálja, mielőtt azok elérnék a postaládákat, és visszafordíthatatlan károkat okoznának.
- Figyelemreméltó sebesség hihetetlen teljesítménnyel ötvözve
  Az Antigen egyedülálló memórián belüli ellenőrzési technológiája lehetővé teszi az ellenőrzés gyorsabbá tételét, mialatt minimális hatást gyakorol a levelezőszerver teljesítményére.
- Kifinomult keresési opciók:
  - valós idejű, ütemezett, illetve manuális keresés a tárcsoportokban (Storage Groups), illetve azok adatbázisaiban,
  - SMTP levelezésvédelem,
  - az Exchange 2000 szerver Web Storage System teljes védelme,
  - az Exchange MTA csatlakozóin (X.400, MS Mail, CC Mail, stb.) keresztülhaladó minden üzenet ellenőrzése.
- A Virus Scanning API (VS API) 2.0 integrálása az Exchange 2000-hez
  Az Antigen támogatja a Microsoft VS API 2.0 vírusvédelmét, így összetett rendszerek számára is átfogó védelem biztosítható.
- Hét keresőmotor
  Hét vezető keresőmotor, közöttük a VirusBuster engine teljesen integrált, párhuzamos alkalmazásának támogatása a még hatékonyabb vírusvédelem érdekében. A keresőmotor

menedzser minden Antigen keresési funkció esetére külön-külön beállíthatóvá teszi, hogy mely motorokat alkalmazza szoftver.

- Maximális teljesítmény biztosítására kialakítva
  Az erőforrások használatának minimalizálása és a gyorsabb ellenőrzés érdekében a levél csatolmányok a memóriában kerülnek ellenőrzésre, ahelyett, hogy ehhez valamely háttértárra mentenénk őket.
- Távadminisztráció
  Az Antigen könnyen telepíthető egyetlen számítógépről minden Exchange szerverre. Ezen felül a beállítások és minden Antigen tevékenység ellenőrzése is elvégezhető egy kiválasztott központi helyről, akár a weben keresztül is.
- Read-only Client Access jogosultságok
  Az Antigen kliensekhez Read-only jogosultság rendelhető, ami által kevesebb felhasználó jut teljes körű kezelési jogosultsághoz az adott intézményben. Ezzel biztonságosabbá és konzisztensebbé tehető az Antigen működése.
- Központi menedzselési lehetőség Antigen karantén menedzserrel (Antigen Quarantine Manager, AQM)
  A karantén menedzser további lehetőségekkel bővíti a szolgáltatásokat. Távoli karanténállományok és vírusjelentéstételi adatbázisok központilag kezelhetők.
- Antigen állományszűrés (Antigen File Filtering (TM), AFF)
  Az AFF minden csatolmánnyal rendelkező beérkező és kimenő üzenet szűrését elvégzi fájlkiterjesztés, típus, név vagy wild card (csonkolt beírás) alapján. A csatolmányok fogadását vagy küldését azok mérete alapján is be lehet állítani.
- Tartalomszűrés
  A tárgysor, a küldő vagy a küldő domain alapján is blokkolhatók a beérkező és a kimenő levelek. Az Antigen 7.0 igény szerint törli, vagy karanténba helyezi a szűrőn fennakadt leveleket.
- Automatikus féregirtás
  A Worm Purge (TM) lehetővé teszi az ismert férgekkel fertőzött üzenetek teljes irtását, mielőtt azok az Information Store-ba érnének.
- Automatikus frissítés
  A vírusleíró adatbázisok automatikusan, egyetlen szerveren történő letöltés segítségével kerülnek frissítésre.
- Értesítő- és karantén szolgáltatások
  Az Antigen személyre szabott Exchange üzeneteket használ, hogy a rendszeradminisztrátort értesítse a vírusincidensekről.
- Értesítések beillesztése a kimenő levelekbe
  Az SMTP-n keresztül lehetővé vált, hogy a rendszergazdák testre szabott üzeneteket illesszenek minden kimenő elektronikus levélbe.

2.5. Adatvédelem, adatok mentése

Az IT rendszerekben található, illetve velük kapcsolatos adatokra a Hivatal Adatvédelmi Szabályzatában foglaltak vonatkoznak.
A felhasználók kötelesek az általuk kezelt rendszerek adatait a rendszerek belső mentési mechanizmusa segítségével rendszeresen menteni mágneses, illetve optikai adathordozóra.
Ezen felül a rendszergazda, a kijelölt informatikusok, munkatársak kötelesek heti rendszerességgel, illetve szükség szerint mentést végezni az általuk felügyelt területekről.

Az IT rendszer kapcsolatban áll az Internettel, ezért az Internet irányába tűzfalas védelem (Microsoft ISA) került kialakításra. A tűzfal működésének felügyelete az IK illetékes munkatársának feladata.

2.5.1. Microsoft ISA szerver ismertető

Az ISA Server az ICSA által minősített vállalati tűzfal és biztonságos alkalmazásátjáró, amely alkalmazásszintű szűrők használatával megvédi a hálózatot a hackertámadásoktól és a rosszindulatú férgektől. Az ISA Server többek között csomagszűrést, állapot-nyilvántartáson alapuló (stateful) csomagellenőrzést, alkalmazásszintű szűrést és fejlett proxyarchitektúrát biztosít.
Az ISA Server különféle operációs rendszereket tartalmazó környezetben is működik, de a legnagyobb értéket a Windows rendszerrel együtt nyújtja. A Windows 2000-ben már meglévő, de azt továbbfejlesztő VPN szolgáltatás akár több telephely hálózatát képes ipari szabvány protokollokkal biztonságosan összekapcsolni az Interneten.
Az ISA Server csökkenti a hálózati ütközések számát és a sávszélességgel kapcsolatos költségeket, a kimenő internetes forgalom csökkentése érdekében pedig a tartalmat helyileg, a webes gyorsítótárból teszi elérhetővé.
Az ISA Server lehetővé teszi a hozzáférés szabályozását többek között felhasználó, csoport, alkalmazástípus, időpont, tartalomtípus és cél szerint. A központi menedzselési szolgáltatások egyszerűbbé teszik a nagyméretű, elosztott rendszerek, például a fiókirodai hálózatok adminisztrálását.
Az ISA Server grafikus feladatpultokat és telepítővarázslókat tartalmaz, amelyek egyszerűsítik a biztonság kezelését, a kiszolgálók közzétételét és a hozzáférés szabályozását; ennek köszönhetően a rendszergazdák a bonyolult működési eljárások helyett az üzleti szabályokra koncentrálhatnak.
A tűzfal és a gyorsítótár mellett az ISA Server naplózást, jelentéskészítést, figyelést, integrált sávszélesség-szabályozást és riasztást is lehetővé tesz.
Az ISA Server architektúrája bővíthető, a biztonsági funkciók más cégek által készített víruskereső, tartalomfigyelő, webhely-blokkoló és más szoftverekkel bővíthető.

2.6. Lotus – Netregister Iratkezelési rendszer

Az elektronikus iratkezelés a Lotus rendszerben történik, melynek felügyelete a rendszergazda feladata. A Lotus üzemeltetésének és felhasználói szabályait, jogosultsági tábláját, mentési szabályait az Iratkezelési Szabályzat tartalmazza.
A rendszer leírása digitális és nyomtatott formában megtalálható a rendszergazdánál, melyet a rendszergazda számára kiosztott teendővel lehet e-mailben megkérni.

IT katasztrófahelyzetek kezelése

A Hivatal működésében a következő IT katasztrófa helyzetek okozhatnak fennakadásokat:

a) *Hálózati hiba*

Hálózati hiba esetén az első teendő a hiba helyének meghatározása, majd a hibajelenség megszüntetése a legrövidebb időn belül. A hibabejelentés a rendszergazda feladata az IK illetékes munkatársa felé.

a. Fizikai kábelszakadás esetén a hiba elhárításának a hibás szakasz feltárása után 2 órával meg kell történni.

b. Aktív eszköz (switch) meghibásodása esetén a hibás eszközt javítás céljából el kell távolítani a hálózatból. A javítás idejére a kiesett aktív eszközt a hálózati elemek átszervezésével, vagy ha ez nem lehetséges, akkor ideiglenesen beépítet aktív eszközzel kell pótolni.
A kiesett hálózati szegmens hálózatba való újra bekapcsolását a hibajelenség észlelése utáni munkanap reggel 8 óráig el kell végezni.
A javítás után a hibás eszköz üzembe helyezése nem zavarhatja meg a napi munkavégzést, ezért ezt munkaidőn túl kell végrehajtani.

b) Szerver hiba

a. adatbázis és file szerverek:
Mivel a Hivatal nem napi 24 órás szolgáltatást nyújt, ezért nem indokolt a Hivatal szerver állományának ún. melegtartalékot kialakítani.
Szerver meghibásodás esetén az eszköz fizikai hibáinak kijavítása után azonnal meg kell kezdeni az operációs rendszer újratelepítését, az operációs rendszer alatt üzemeltetett célszoftver telepítését, majd az adatok visszaállítását.
Amennyiben a javítási idő meghaladja a 24 órát, akkor a napi működéshez szükséges adatokat egy működő szerverről kell biztosítani a mentés állományok segítségével.

b. Active Directory jogosultságot kezelő szerverek:
Mivel a felhasználók struktúrája egy helyen az Active Directory adatbázisban tárolódik, ezért 2 szerver van domain controllernek kijelölve. Mindkét szerveren megtalálható a mindenkori adatbázis állapot egy-egy teljes példánya. Amennyiben az egyik szerver meghibásodik, a másik zavartalanul tovább tud működni, majd a meghibásodott szerver a javítás után automatikusan frissül a működő szerverről. Mindkét szerver egyidejű meghibásodása esetén az Active Directory adatbázis mentéséből kell visszaállítani a korábbi állapotot.
Mindkét esetben a javítás ideje legfeljebb 24 órát vehet igénybe.

c) Külső hálózati kapcsolatok hibája

1) Internet kapcsolat megszakadása esetén a hibát az IK-nak jeleznie kell a Debreceni Egyetem Informatikai Csoportja felé, mivel a hiba elhárítását e szerv végzi.
2) Az Önkormányzati és Területfejlesztési Minisztérium (a továbbiakban: ÖTM) felé irányuló hálózati kapcsolat hibája esetén az IK értesíti az ÖTM Informatikai Osztályát. A hiba elhárításáról e szerv gondoskodik.

Záró rendelkezések

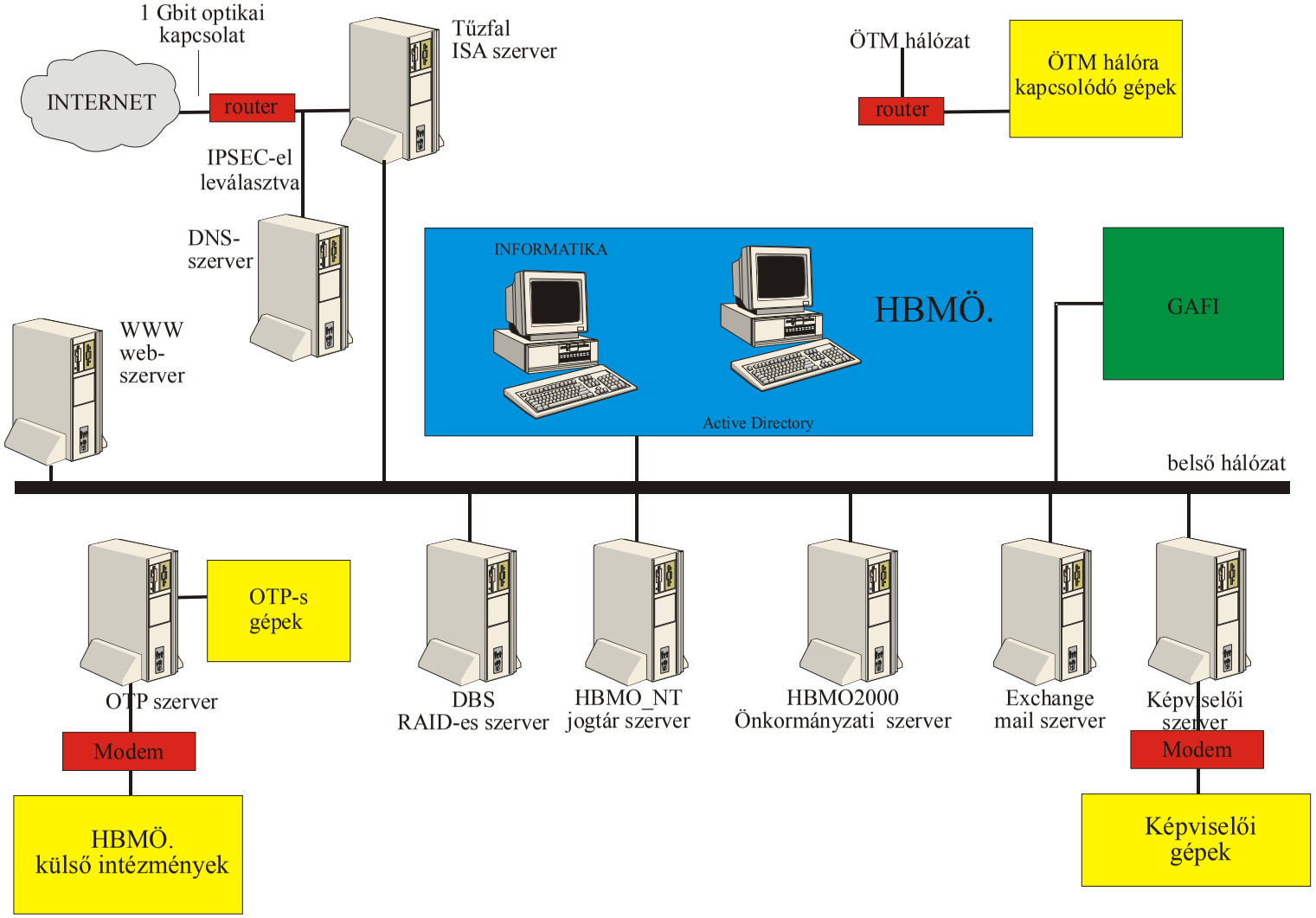
Jelen szabályzat 2008. július 1. napján lép hatályba.

Debrecen, 2008 július 1.

Vasas Lászlóné dr.
megyei főjegyző

1. számú **melléklet**

Az IT rendszer elvi vázlata:



Az IP címekhez tartozó hálózati mask: 255.255.254.0

HBMÖ – Rack szekrény

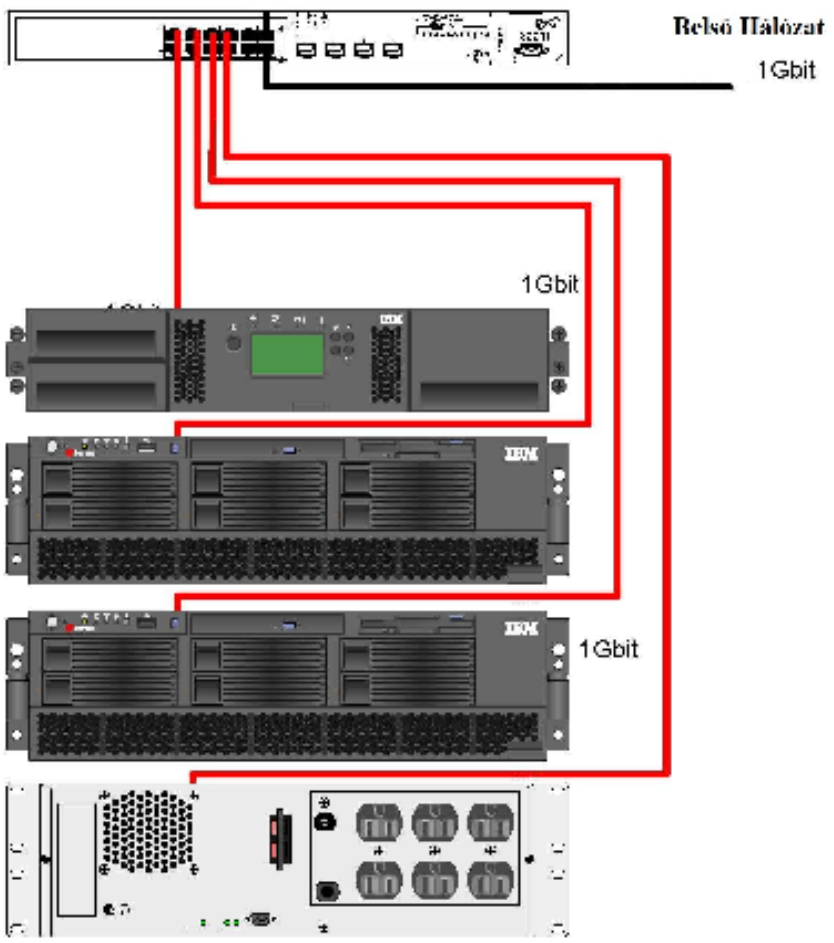
LAN SWITCH (3Com 4200G 12 port Switch)
IP address: 192.168.73.205
Default Gateway: 192.168.72.82

Tape Libary
IP address:
192.168.73.203

File Server IP address: 192.168.73.201
publikálva 193.6.186.65 külső címen
3389 és 1352 TCP portokon.

Domino Server IP address: 192.168.73.202
publikálva 193.6.186.66 külső címen
3389 és 1352 TCP portokon.

UPS szünetmentes tápegység
IP address: 192.168.73.204



2. számú melléklet

Kiegészítés
az Informatikai Biztonsági Szabályzathoz

1. TATIGAZD főkönyvi könyvelési rendszer

A program hálózati környezetben működik. A program és az adatállományok az önkormányzat adatszerverén helyezkednek el. A jogosultságok beállításával a Közgazdasági Főosztály 6 munkaállomása használhatja a programot.

A rendszer használói a következők

Modul	Felhasználó
Bank, pénztár vegyes rögzítés és könyvelések	Már Norbert Mészáros Krisztina
Előirányzat nyilvántartás	Szőkéné Dankó Ildikó
Kötelezettségvállalás	Jankóné Papp Mária
Kötelező és önként vállalt feladatok, egyéb pénzeszköz átadás	Szakál Ferencné
Tárgyi eszköz nyilvántartás, személyi juttatások	Gergely Margit

A munkaállomásokon illetéktelen használat elleni védelmet az egyéni jelszó biztosítja.

Adatvédelem: Az adatok és a program mentése havi rendszerességgel floppy lemezre történik. (Nagyobb mennyiségű adat rögzítése, könyvelése esetén gyakrabban is történhet). A mentés készítése Már Norbert (távollétében Mészáros Krisztina) feladata.
A program sérülése esetén a program újra installálásával kell elhárítani a hibát.
Az adatállomány sérülése esetén az utolsó mentett állomány visszatöltésével visszaállítható a mentett állapot. A mentés időpontja után rögzített tételeket újra rögzíteni és könyvelni kell.

2. SALDO Pénzügyi Integrált Információs rendszer

A program hálózati környezetben működik. A program és az adatállományok a megyei önkormányzat Közgazdasági Főosztályán található szerveren helyezkednek el. A jogosultságokat a programon belül a rendszergazda állítja be az egyes moduloknak megfelelően minden munkahelyre. A jogosultságok beállítása Mészáros Krisztina feladata a Főosztályvezetővel történő egyeztetés után. A munkaállomásokon illetéktelen használat elleni védelmet az egyéni jelszó biztosítja.

A program moduljai és a felhasználók

Modul	Felhasználó	Helyettesítő
Alapozó iktatás	Nagy Alida	Nádas Anita Mészáros Krisztína
Szállítói és vevői kötelezettség-vállalások nyilvántartás	Jankóné Papp Mária	Nádas Anita
Bérjellegű kötelezettségvállalások nyil-Vántartás	Vincze Ferencné	Szakál Ferencné
Közgyűlési határozatok kötelezettségvállalásának nyilvántartása	Máthé Gábor	
Szállítói számlák és szállítói egyéb iktatás	Nádas Anita	Hangrád Zoltánné
Vevői egyéb iktatás	Jankóné Papp Mária	Nádas Anita
Kötelező és önként vállalt feladatok és egyéb átadott pénzeszközökhöz kapcsolódó számlák, ill. lakáskölcsön iktatása	Szakál Ferencné	Nádas Anita
Eseti bérjellegű kifizetések, ill. egyéb jogviszony kifizetéseinek iktatása	Vincze Ferencné	Nádas Anita
Banki vegyes iktatás	Hangrád Zoltánné	Nádas Anita
Banki átutalás	Hangrád Zoltánné	Nádas Anita
Banknapló nyilvántartása	Hangrád Zoltánné	Nádas Anita
Pénztári kifizetések nyilvántartása	Vincze Ferencné	Nádas Anita
Valutapénztári elszámolások	Szakál Ferencné	Gergely Margit Nádas Anita
Számlázás	Jankóné Papp Mária	Nádas Anita
Előirányzat nyilvántartás	Szőkéné Dankó Ildikó	Már Norbert Mészáros Krisztina
Tárgyi eszköz nyilvántartás	Gergely Margit	Már Norbert Mészáros Krisztina
Személyi juttatás és munkaadókat terhelő járulékok könyvelése	Gergely Margit	Már Norbert Mészáros Krisztina
Főkönyvi könyvelés	Mészáros Krisztina	Már Norbert
Rendszergazdai jogosultságok	Mészáros Krisztina	
Lekérdezések	Nagy László Balogh Károlyné Mózsa Géza	

Adatvédelem: Az adatok és a program mentése havi rendszerességgel CD lemezre történik. (Nagyobb mennyiségű adat rögzítése, könyvelése esetén gyakrabban is történhet). A mentés készítése Mészáros Krisztina (távollétében Már Norbert) feladata.
A program sérülése esetén a program újra installálásával kell elhárítani a hibát.
Az adatállomány sérülése esetén az utolsó mentett állomány visszatöltésével visszaállítható a mentett állapot. A mentés időpontja után rögzített tételeket újra rögzíteni és könyvelni kell.

3. Tárgyi eszközök nyilvántartása

A program egyedi számítógépen működik. A program és az adatállományok Gergely Margit számítógépén helyezkednek el. A munkaállomáson illetéktelen használat elleni védelmet az egyéni jelszó biztosítja.

Adatvédelem: Az adatok és a program mentése havi rendszerességgel floppy lemezre történik. (Nagyobb mennyiségű adat rögzítése, könyvelése esetén gyakrabban is történhet). A mentés készítése Gergely Margit feladata.
A program sérülése esetén a program újra installálásával kell elhárítani a hibát.
Az adatállomány sérülése esetén az utolsó mentett állomány visszatöltésével visszaállítható a mentett állapot. A mentés időpontja után rögzített tételeket újra rögzíteni és könyvelni kell.

4. Intézményi Munkaügyi Információs rendszer

A program egyedi számítógépen működik. A program és az adatállományok Vincze Ferencné számítógépén helyezkednek el. A munkaállomáson illetéktelen használat elleni védelmet az egyéni jelszó biztosítja.

Adatvédelem: Az adatok és a program mentése havi rendszerességgel floppy lemezre történik. (Nagyobb mennyiségű adat rögzítése, könyvelése esetén gyakrabban is történhet). A mentés készítése Vincze Ferencné feladata.
A program sérülése esetén a program újra installálásával kell elhárítani a hibát.
Az adatállomány sérülése esetén az utolsó mentett állomány visszatöltésével visszaállítható a mentett állapot. A mentés időpontja után rögzített tételeket újra rögzíteni.

5. Számlázó rendszer

A program egyedi számítógépen működik. A program és az adatállományok 2005. évvel bezárólag Jankóné Papp Mária számítógépén helyezkednek el. 2006. évtől a SALDÓ rendszerben történik a szálázás. A munkaállomáson illetéktelen használat elleni védelmet az egyéni jelszó biztosítja.

Adatvédelem: Az adatok és a program mentése havi rendszerességgel floppy lemezre történik. (Nagyobb mennyiségű adat rögzítése, könyvelése esetén gyakrabban is történhet). A mentés készítése Jankóné Papp Mária feladata.

A program sérülése esetén a program újra installálásával kell elhárítani a hibát.

Az adatállomány sérülése esetén az utolsó mentett állomány visszatöltésével visszaállítható a mentett állapot. A mentés időpontja után rögzített tételeket újra rögzíteni.

6. MVOKS szavazatszámláló rendszer

A program a közgyűlés üléseinek lebonyolításában van segítségre. A rendszer különálló, csak az ülések ideje alatt használatos számítógépen működik. Kapcsolódó berendezések a képviselők által használt pultok, egy mindenki számára jól látható tábla, valamint a terem hangosítására szolgáló keverőpult.
A rendszer adatainak rendelkezésre állásával különböző statisztikák készítésére van lehetőség (pl. szavazásokon való jelenlét, hozzászólások száma ideje, stb.). A statisztikák készíthetők ülésenként, illetve adott időszakra vonatkozóan. Ezek alapjául szolgálnak a képviselők tiszteletdíjának számítása kapcsán.

A program a fő számítógépen kívül bármennyi gépre telepíthető, azonban azokon ülés indítására nincs lehetőség, csak a már meglévő adatok használatára (pl. írott, vagy hangos jegyzőkönyv megtekintése, statisztikák készítése, stb.).

A fő gépen működő program kezelésére jelenleg két munkatárs jogosult:
Luczi Péterné és
Tóthné Bobonka Magdolna.

Jelenleg ugyanezen két munkatárs által használt számítógépre van telepítve a rendszer lekérdezés végett.

Adatvédelem: A közgyűlés üléseinek befejezésével az adatállományokról mentés készül, ami az adatszerver ’Szavazó’ mappájában kerül tárolásra. A ’Szavazó’ mappához a kezelő munkatársaknak van hozzáférési joga.
Az adatok mentése fél évente CD lemezre írással történik, a mentésért felelős: Tóthné Bobonka Magdolna.
A rendszer működésével kapcsolatos bármilyen probléma esetén a készítő GLOBOMAX Kft. munkatársai szolgálnak segítséggel.

7. Wintiszt közszolgálati humánpolitikai rendszer

A program a hivatal munkatársainak személyi adatait tárolja, kezeli, alapvetően a Ktv. ill. az Mt. vonatkozó paragrafusainak előírásai alapján működik.

A program jelenleg 2 felhasználó hozzáférését teszi lehetővé, hálózatos módon működik. A program adatai az adatszerveren tárolódnak a ’Wintiszt’ nevű mappában.

Adatvédelem: A ’Wintiszt’ mappához teljes hozzáférési jogosultsággal (írás, olvasás, törlés, módosítás) a humánpolitikai munkatársak (Kovátsné Korn Anikó, Vincze Fruzsina) rendelkeznek.
A program adatainak mentése merevlemezre legalább hetente egyszer, de nagy mennyiségű módosítás vagy program módosítás esetén akár többször is történik.
A mentések CD-re írása havonta egyszer történik. A mentésért felelős Kovátsné Korn Anikó.

A rendszer hibáinak javítására, a működés közbeni problémák orvoslására a rendszert készítő Qualisoft Kft. munkatársai jogosultak.

8. Iktatóprogram

A hivatalba beérkező és kimenő levelek jogszabály szerinti iktatására szolgáló program.

A program hálózaton keresztül érhető el, az adatok a Domino szerveren találhatók.

Adatvédelem:
Az adatok mentése naponta kazettára és havonta DVD lemezre, melyek kezeléséről az iratkezelési szabály rendelkezik. A mentésért felelős a rendszergazda. A jogosultsági tábla az iratkezelési szabályzat részét képezi melynek beállításáért a rendszergazda felelős.

3. számú melléklet

ADATLAP
A Hajdú-Bihar Megyei Önkormányzat
Active Directory adatbázisába való felvételhez/módosításhoz

Munkavállaló neve	
Felhasználói neve	
Felhasználó e-mail címe	

Hozzáférési jogosultságok az adatszerver mappáihoz

Mappa neve	Hozzáférés *
Alelnöki	
Elnökség	
Eüszoc	
fejleszt_fooszt	
Iktat	
Intezm_fooszt	
Jegyzo	
Jogi	
jogi_fooszt	
KGT	
KornAniko	
Kozgazd	
Kozoktatas	
minosegiranyitasi rendszer	
Munkaugy	
otp	
Saldo	
Szavazo	
TTG	
Vagyon	
Wintiszt	
Egyéb hozzáférés, mégpedig _____	

*** : X** - új felhasználó hozzáférésének biztosítása
T - a felhasználó meglévő hozzáférésének törlése

Debrecen, 200……

_____ _____
szervezeti egység vezetője **megyei főjegyző**

***Megjegyzés*:** Az ’Átadás’, és a ’Közgyűlés’ mappákhoz minden felhasználó részére teljes hozzáférés biztosított, a ’Közérdek’ mappához csak olvasási jog van engedélyezve.