Biztonsági kézikönyv

a TITÁN Térségi Információs Technológiai és Általános Nyilvántartórendszer

SZISZI Iratkezelő moduljához

Utolsó módosítás dátuma:

2012. december 01.

Tartalomjegyzék

Kapcsolódó dokumentumok

Adminisztrációs kézikönyv.

Telepítési kézikönyv.

Rendszeradminisztrátori kézikönyv.

Dokumentum célja

A kézikönyv célja, hogy a SZISZI iratkezelő rendszer – továbbiakban rendszer – biztonságos használatához, ajánlásokat tegyen, és ismertesse azokat a biztonsági megoldásokat melyekkel a rendszer rendelkezik.

A dokumentum hatóköre

Jelen dokumentum nem helyettesíti a szervezetnél alkalmazandó átfogó informatikai biztonsági koncepciót, szabályzatot. Hatóköre a rendszerre, a rendszert futtató szerver infrastruktúrára és a rendszerhez kapcsolódó kliensekre terjed ki.

A rendszer felépítése

A közigazgatás területén kiemelkedően fontos szempont, hogy olyan rendszert használjuk, amelynek segítségével pontosan nyomon követhetjük az egyes hivatalok munkafolyamatainak minden állomását, ezekről megfelelő jelentéseket kapjunk, s mindeközben rendszerünk integráltan tudja kezelni feltételrendszereinket. A TITÁN egy olyan komplex szolgáltatás, amely egyesíti egy folyamatvezérlő rendszer és a hagyományos rendszerek minden előnyét. Mindemellett saját fejlesztésű, nyílt forráskódú alapokra épülő fejlesztési környezet. A segítségével készült alkalmazások platform-függetlenül, kliens-szerver architektúrán alapulva webes felületen keresztül használhatóak. A TITÁN segítségével költséghatékonyan oldhatjuk

meg a digitális folyamatvezérlésre épülő papírmentes irodát és használhatjuk a TITÁN modulokként megvalósított szakági alrendszereit.

A rendszer futtatásához szükséges szerver oldali szoftverkörnyezet nyílt forráskódú rendszereken alapul, ami azt jelenti, hogy a rendszer működéséhez nem szükséges más harmadik gyártónak a licenc díjas terméke. Így a rendszer bevezetése és üzemeltetése gazdaságos, nem kötődik a felhasználói licence számához, így hosszú távon is megfelelő alternatívát nyújthat, jól tervezhető üzemeltetési költséget biztosítva a szervezet számára.

A szerver oldali architektúra bevált és általunk preferált alapja a Linux (Debian) operációs rendszer, erre építve Apache webkiszolgáló szerverrel, PHP és JAVA alapú alkalmazások futtatására alkalmas környezettel és PostgreSQL 8.2 vagy annál újabb adatbázis kezelő szerverrel biztosítjuk a rendszer stabilitását és gyorsaságát.

A szerver komponensek mindegyike több op. rendszer alatt is futhat (windows, unix-ok), ezért igény esetén más platformra is átültethető. Bár a linux eddigi tapasztalataink alapján robosztus és gyors, megbízható platformot biztosít rendszereinknek.

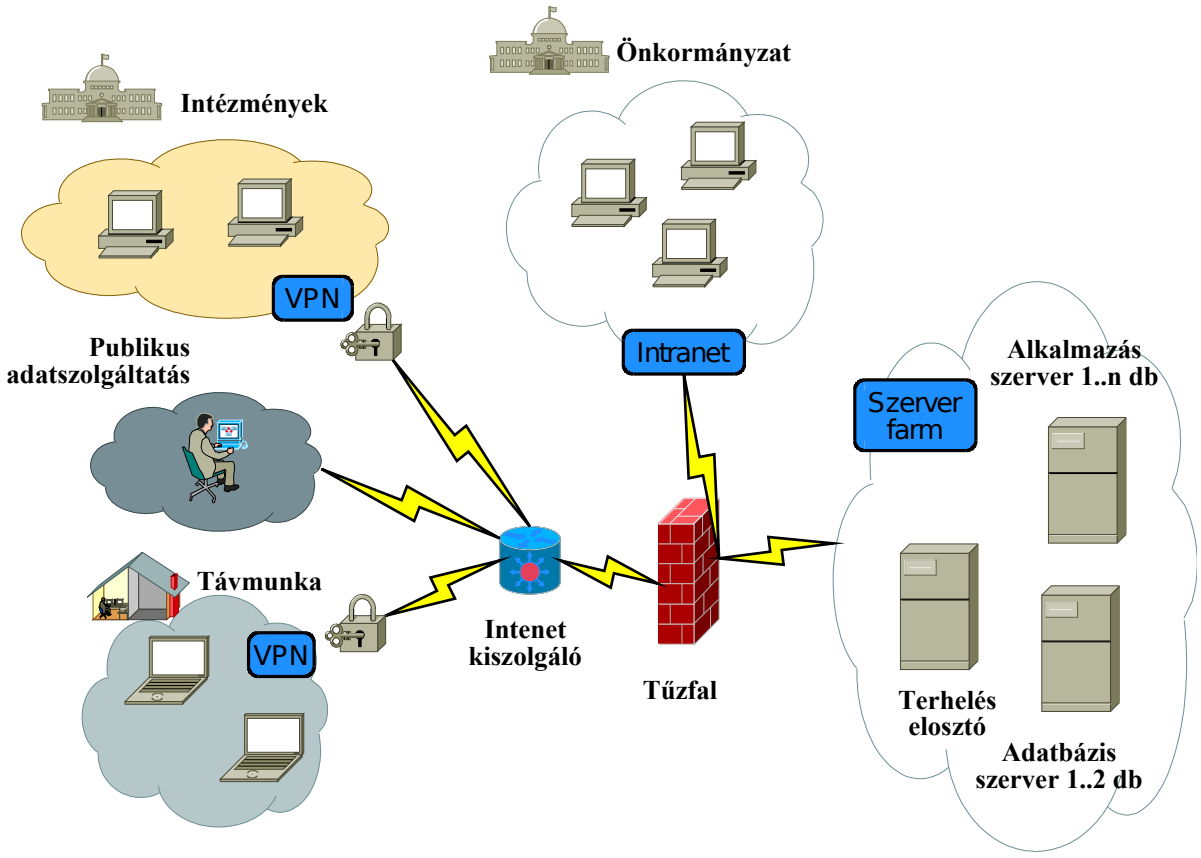
Az adatok tárolása központi adatbázisban történik, az adatbázis teljesen konzisztens, és a folyamat lépések kezelésének köszönhetően a rendszer használata csak egyszeres adatrögzítést igényel.

Kliens oldalon a rendszer használatához a következő szoftver elemek szükségesek:

- Böngészőprogram (IE, Firefox)
- A JAVA-s megoldások futtatásához szükséges JAVA runtime
- A nyomtatásokhoz pdf olvasóra (Acrobat Reader)
- A sablonok szerkesztéséhez és a táblázatok exportálásához Openoffice vagy MS Office

Az alábbi topológiai rajz egy olyan lehetséges megoldást ábrázol, amelyen a szervezet, és az esetlegesen hozzá kapcsolódó intézményei is használni tudják a rendszert. A szerver park elhelyezése természetesen bárhol megtörténhet, helyileg akár a szervezeten belül is, akár távoli szolgáltatónál is.

Az ábrán látható, hogy a rendszer minden eleme skálázható, tetszőleges módon bővíthető, így a megfelelő terhelés elosztás is biztosítható. A rendszert akár otthonról, távoli internetpontról is lehet használni, üzemeltetni, melyhez megbízható VPN kialakítását javasoljuk. A VPN kialakítását meg lehet oldani különleges hardver ill. extra licence díj alkalmazása nélkül is.



1. ábra Hardver infrastruktúra bemutatása Intézményi kiterjesztés esetén

A rendszer kezdetben összevonható egy szerverre is, és a későbbi felhasználószám növekedéssel összhangban újabb szerverek vonhatóak be a gyorsabb kiszolgálás érdekében.

Biztonsági szintek

A rendszer felépítéséből adódóan (nem a kliens gépen futó egyedül álló szoftver) a biztonságos használat és üzemeltetés érdekében több szinten kell a biztonságot tárgyalni:

- a szerver oldalon
  - operációs rendszer,
  - a rajta futó, a működéshez szükséges szerver oldali komponensek,
  - a TITÁN CORE, és a futtatott modulok
- a szerverhez kapcsolódó munkaállomások, és a használathoz szükséges kliens oldali alkalmazások,
- a komponensek közti kapcsolatok:
  - szerverek közti,
  - szerveren belüli,
  - szerver adminisztrációját biztosító,
  - munkaállomás – szerver

A rendszerben használt biztonsági megoldások

A szerver telepítésekor kiemelten fontos, hogy a telepítési kézikönyvben leírtak pontosan betartásra kerüljenek. Az így telepített szerver rendelkezni fog a jelen dokumentumban

később tárgyalt szerver oldali biztonsági tulajdonságokkal. A rendszer alapbeállításainak elvégzése és a napi adminisztrációs feladatok végrehajtása során a megbízható és biztonságos üzemeltetéshez elengedhetetlen az adminisztrációs kézikönyv ismerete és az abban foglaltak betartása.

Jogosultság- és hozzáférés-kezelés

Szerver

A szervert adminisztrálás céljából csak biztonságos hozzáférést lehetővé tevő un. Ssh kapcsolaton keresztül lehet elérni a telepítéskor megadott felhasználónév és jelszó ismeretében. A belépéshez szükséges jelszavak csak titkosítva kerülnek tárolásra.

A TITÁN működéséhez szükséges szerver komponensek (nyomtatás, folyamat vezérlő) a hálózat többi részéről nem érhetőek el.

A telepített szerveren csak a következő portok, funkciók érhetőek el távolról:

- 443 HTTPS A webes felület eléréséhez
- 25 SMTP Levelek fogadásához
- 22 SSH Biztonságos adminisztrációhoz

TITÁN CORE

Egy rendszer biztonságának sarkalatos pontja a használatához szükséges jelszavak minősége, ezért a felhasználói jelszavak bizonyos ideig (alap esetben 1 hónap) érvényesek csak, azokat a lejárati idő után kötelezően meg kell változtatni, illetve a biztonság érdekében azok minimális hossza is korlátozva van (alap esetben 5 karakterre, ami nem lehet hasonló az előző jelszóhoz vagy a bejelentkezési névhez).

Iratkezelő (TITÁN CORE modul) webes felhasználói felület

A rendszer több szintű jogosultságkezelési funkcióval van ellátva. Az első szintet a TITÁN rendszer szervezet szervere biztosítja, ahol strukturálisan rögzíthetőek az intézmények, egyéb szervezeti egységek (továbbiakban intézmények) adatai, azok egymáshoz viszonyított állapota (önálló, és részben önálló intézmények). Az intézményekbe lehet felhasználókat rögzíteni, akik jogosultak lehetnek az adott modul használatára, a bejelentkezési azonosító, és jelszó is itt van tárolva. A második szint az adott modul funkcióinak használatának szabályozása (a modulon belül mely funkciók érhetőek el). A harmadik szint az összefüggő adatok szintje, ahol a konfiguráláskor meghatározható, szabályok jelentik korlátozó tényezőt. A negyedik szint pedig egyed vagy rekordszintű jogosítás szintje, ahol adott adatcsoporthoz definiálhatunk a megszokottól eltérő jogosultságokat az egyes felhasználók számára.

Az iratkezelő rendszerre vonatkozó jogosultság beállítások

Az iratkezelés beállításait mindig az iratkezelési szabályzatnak megfelelően kell elvégezni!

Az iratkezelés jogosultság beállításaihoz ki kell alakítani az irattári tervben meghatározott iktatókörnyezetet (iktatóhelyek, iktatókönyvek felvétele, irattári jel, iktatószám formátum stb.).

Jogosultság beállítási szintek

1. szint (Szervezetszerver modul)

A rendszert használó szervezet belső felépítésének leírása illetve dolgozóinak összerendelése az egyes szervezeti egységekkel. A dolgozók helyes és átgondolt besorolása kulcs fontosságú, hiszen hiába bír egy adott felhasználó tetszőleges jogosultsággal hiszen ha hozzárendelt egyik szervezeti egység sem végez a jogosultsághoz feladatot akkor a felhasználó sem fogja tudni használni azt. Például: Hiába kap valaki iktatási jogosultságot, ha szervezeti egységeinek egyikéhez sem tartozik iktatókönyv. Bővebben lásd Adminisztrátori kézikönyv

2.szint (Bejelentkezéskezelő modul)

Lehetőség van a felhasználók csoportba sorolására és a csoportokon keresztüli jogosultságokkal való felruházásra. A rendszerben minden felhasználó ezen jogosultságai alapján illetve szervezeti egységei alapján végezheti tevékenységét, ha csak egy később szint felül nem bírálja esetleg ki nem egészíti valamely jogosultsággal. Bővebben lásd Adminisztrátori kézikönyv.

3. szint (Iktatókönyvek karbantartása menüpont)

Iktatókönyvek és azon szervezeti egységek összekapcsolása, ahova a kiválasztott iktatóhelyről (szervezeti egységről) iktatni lehet. Itt állítható be továbbá az is, hogy az adott iktatókönyvre, mely szervezeti egységek (első szintű szignálás) iratai iktathatóak, azok milyen irattári tételekre kerülhetnek, és végül milyen automatizálási feladatokat (automatikus szignálás) lehet végeztetni a rendszerrel. Bővebben lásd Adminisztrátori kézikönyv.

Visszakövethetőség, naplózás

Szerver

A szerver eseményekhez (be- , kilépés, szolgáltatás hibák, figyelmeztetések) részletes naplófileok készülnek. Ezen naplók a szerverre ssh-n titanadmin felhasználóval belépve az adminisztrációs menü segítségével megtekinthetőek.

TITÁN CORE

Az alap rendszer és a rajta futtatott modulok az op. rendszertől függetlenül központosítva naplóznak minden fontos, a modul működésével kapcsolatos információt (ki-, belépés, hibák, figyelmeztetések). A naplófilok a megfelelő jogosultsággal a webes felületen bejelentkezve a „rendszernapló megjelenítő” menüpont alatt lekérdezhetőek, kereshetőek.

Az adatok változását a rendszer elemi adat mező szinten naplózza, melynek két jelentősége is van: először is az adatok, adat változások időben visszakövethetőek, és szükség esetén vissza is állítható, másodszor pedig folyamatos monitorozást tesz lehetővé, ugyanis a rendszer minden esetben a változtatás időpontját, az eredeti és a változtatott adatot, valamint a felhasználót is rögzíti, így az esetleges felelősségek mindig egyértelműen meghatározhatóak.

Rendszernaplók rendszere, megtekinthetősége

A rendszernaplók áttekintésének segítségével a felhasználók műveleteit, mozgását követhetjük nyomon a rendszerben, és ezek felhasználásával tudunk a mindennapi problémáikra megoldást találni ill. egyéb probléma esetén a készítőket értesíteni a körülményekről. A rendszernaplók megfelelő jogosultság esetén a TITÁN webes felületéről is megtekinthetőek kereshető, rendezhető formában, viszont fontos tudni, hogy a naplók minden nap archiválódnak, így az adott napi listában csak azon a napon történt bejegyzések láthatóak (az archivált naplók alap telepítésnél egy hétre visszamenőleg őrződnek meg, bár ez felülbírálható; ettől hosszabb időszakra visszamenőleg csak különleges esetben lehet szükség, általában nem kívánalom). Az egyes bejegyzések szükség esetén email-ben is kérhetőek, így a fontosabb dolgokról a naplók külön figyelése nélkül is értesülhetünk. A felhasználók által kapott hibaablakon lévő hibakód az előfordulás dátumát és időpontját tartalmazza (pontokkal elválasztva), segítségével egy későbbi hibajelentés esetén is könnyen megtalálhatjuk az adott bejegyzést.

Az egyes naplók tartalmuk szempontjából szeparáltak, felhasználási területük a következők szerint alakul:

- **alert.log**: Rendszerszintű hibák ill. figyelmeztetések, melyeket mindenképpen érdemes figyelemmel kísérni, valamint egyértelmű rendszerhiba esetén értesíteni a készítőket.

- **auth.log**: A felhasználók ki- és bejelentkezéseit tartalmazó, információs jellegű napló.
- **drs*.log**: A dokumentumgeneráló szerverkomponens részletes naplói, dokumentum generálási hiba esetén (igen ritka) itt találhatunk bővebb információt a hiba okáról.
- **error.log**: Felhasználói szintű hibák helye, rendeltetésszerű működés esetén a legtöbb bejegyzést itt találhatjuk, melyek rendszerint a felhasználók által vétett kisebb elírások, stb. eredményeképp kapott figyelmeztetések.
- **jengine*.log**: Folyamatvezérlő szerverösszetevő belső működését érintő naplóbejegyzések, melyekre általában csak folyamatvezérlő belső hiba esetén van szükség (a rendszer készítőinek értesítése mellett).
- **message.log**: Egyéb figyelmeztetések, melyek a rendszer működésére jellemző egyéb információkat tartalmaz, általában ritkán kerül ide bejegyzés, mely értelmezés után nagyrészt figyelmen kívül hagyható.
- **php4.log**: Hibás telepítés vagy beállítások ill. időközben megváltozott rendszerkörnyezet után fordulhatnak elő kisebb rendszerhibák a webszerver motorjának működése során, melyik itt kerülnek rögzítésre. Általában operációs rendszer szintű fájl elérésekkel vagy jogosultságokkal kapcsolatos bejegyzések jelenhetnek itt meg (ezek korrigálását pl. a titanadmin felület segítségével tehetjük meg).
- **servers.log**: Az esetleges automatikus szerverszolgáltatás újraindítások naplóbejegyzései (ha túl sok bejegyzés kerül ide, akkor érdemes a szervert jobban átvizsgálni, mert valamilyen oknál fogva egy adott szolgáltatás időről időre kiesik, és nem tudja megfelelően kiszolgálni a befutó kéréseket).
- **urlhistory.log**: A felhasználók minden egyes lépését, kattintását rögzítő napló, melyből egyértelműen rekonstruálható, hogy mikor merre járt és mit választott a felületen az adott felhasználó (hibakeresésnél van nagyobb szerepe, ha szeretnénk tudni, hogy az adott felhasználó milyen úton-módon jutott a hibát okozó pontra).

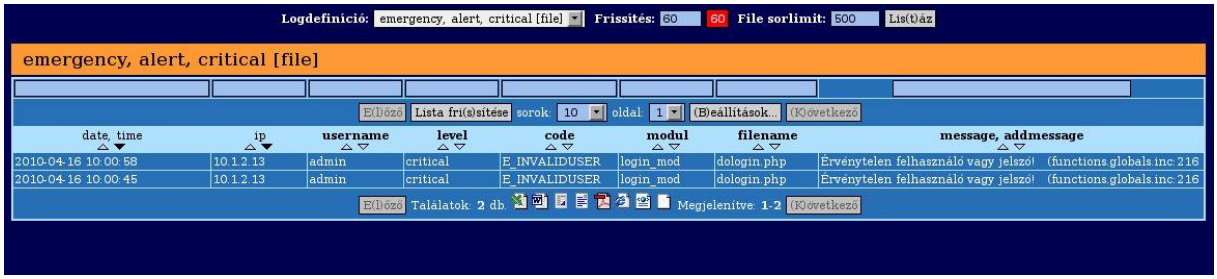
Rendszernaplók megtekintése, figyelése

Az adminisztrátorok számára a TITÁN rendszerbe belépve elérhető a rendszernapló megjelenítő funkció, amely lehetőséget biztosít a rendszernaplók rendszerezett és folyamatos megtekintésére, megfigyelésére.

A táblázat feletti Logdefiníció részben állítható, hogy milyen típusú, jellegű naplózásokat jelenítsünk illetve figyeljünk meg. A kiválasztható típusok megegyeznek a korábbiakban tartalmi szempontból leírt rendszerezéssel. Az egyestípusokon belül a táblázat szűrő sorának segítségével tetszőleges szűkítéseket eszközölhetünk a hatékonyabb munkavégzés érdekében.

Ezt követően állíthatjuk a frissítés időközét másodpercben. Ennek a funkciónak a segítségével folyamatosan értesülhetünk szinte a bekövetkezéssel egy időben az új naplóbejegyzésekről.

Állíthatjuk továbbá a napló állományok feldolgozandó maximális sorszámát is.



Iratkezelő (TITÁN CORE modul)

Az iratkezelőben végzett minden felhasználói művelet (pl. iktatás, irattározás) beleértve a lekérdezéseket is naplózásra kerül - a művelet idejével, a bejelentkezett felhasználó nevével, az esemény megnevezésével és a műveletben érintett adat azonosítójával, a művelethez kapcsolódó elemi adat változásokkal együtt (mi mire változott) - .

Ezen események az Esemény napló megtekintő felületen megtekinthetőek, vissza kereshetőek. Részletesen lsd. a rendszeradminisztrátori kézikönyv „Naplózások” fejezetében.

Adat védelem, adatbiztonság

Szerver

A rendszer megvalósításakor a nyílt forráskódú PostgreSQL tranzakciós adatbázis-kezelő rendszert alkalmazzuk, mely biztosítja, hogy az adatok mindig konzisztens módon kerülnek tárolásra. Az adatbázisokat a rendszer SSL titkosításon keresztül, jelszóval védve éri el.

A minősített adatok védelmére a kriptográfia által biztosított lehetőségeket használjuk (pl. MD5 és SHA1 message digest képző eljárások).

A beérkező levelek az iratkezelőben történő feldolgozás előtt SPAM és vírus ellenőrzésen esnek át. Az adatok vírusmentességét a clamav vírusvédelmi szoftverrel biztosítjuk. Az

ellenőrzésen fennakadt leveleket a rendszer automatikusan vissza utasítja, melynek tényéről a beküldőt értesíti.

TITÁN CORE

Felhasználói inaktivitás esetén a rendszer - egy központilag beállítható – idő leteltével a felhasználót automatikusan kilépteti a rendszerből. A saját vagy kapcsolódó rendszerből érkező rendszer szintű hibaüzeneteket a felhasználói felület elrejti a felhasználók elöl, és azokat a beállításoknak megfelelő helyre továbbítja (file, email, adatbázis).

A rendszerben tárolt adatokról a titánadmin felületen keresztül teljes értékű biztonsági mentés készíthető helyben, vagy távoli gépre hálózaton keresztül. Az esetleges adat sérülést követően (akár a rendszer teljes újra telepítése után) a felület segítségével az adatok vissza állíthatóak.

A mentés úgy javasoljuk beállítani, hogy az ssh – kapcsolaton keresztül napi rendszerességgel (munkaidőn kívül) egy a belső hálózaton elérhető biztonsági mentéseket végző archiváló szerverre készüljön. Az így keletkezett állományokat a szervezetnél kialakított adat mentési stratégiába be kell vonni (napi, heti, havi mentések).

A keretrendszer több technikával ellenőrzi a felhasználói felületről érkező adatok érvényességét és valódiságát:

- bemenő URL paraméterek kódolása,
- lapok védelme a kéretlen paraméterektől
- adatok fogadásakor a biztonságos HTTPS kapcsolat meglétének ellenőrzése

Iratkezelő (TITÁN CORE modul)

A rendszer képes csatolt dokumentumok, és a kimenő levelek digitális aláírására (időpecséttel), és a beérkező levelek MELASZ kompatibilis mellékleteinek vizsgálatára.

A digitális aláírással kapcsolatos funkciók rendszerben a Microsec Kft. E-SZIGNÓ megoldásának felhasználásával kerültek magvalósításra.

Rendszer biztonságos környezetének kialakítása

Kapcsolatok

Igaz, hogy a rendszer használata és adminisztrációja csak biztonságos (ssh, https) kapcsolaton keresztül történhet, a biztonság növelése érdekében javasoljuk VPN és valamilyen tűzfal megoldás használatát.

Kapcsolat honnan/hová	Védelem típusa
Helyi munkaállomás – szerver	Tűzfal :csak a HTTPS (443) port továbbítása legyen engedélyezve a szerver felé.
Kitüntetett adminisztrációs munkaállomás - szerver	Tűzfal :csak a SSH (22) és a HTTPS (443) port továbbítása legyen engedélyezve a szerver felé.
Külső munkaállomások – szerver	VPN:csak a HTTPS (443) port továbbítása legyen engedélyezve a szerver felé.
Központi mail szerver – szerver	Tűzfal :csak a SMTP (25) port továbbítása legyen engedélyezve a szerver felé.

Szerver elhelyezése, fizikai védelme

Kiemelten fontos szempontok a számítógépterem tervezésénél, kialakításánál és átalakításánál:

- a statikai követelmények (várható maximális födémterhelés, eszközök száma, azok várható súlya) figyelembe vétele
- a környezetből adódó rezgések, környezeti zavarok (pl. nagy-frekvenciás hálózat) figyelembe vétele
- a klimatizálás biztosítása
- a szünetmentes tápellátás biztosítása
- törekedni kell arra, hogy a géptermen belül automatikus betörés- és tűzjelző rendszert kell telepíteni, ami mozgás-, nyitás-, füst-, üvegtörés és vízérzékelőkkel rendelkezzen;
- törekedni kell a számítógépteremben az ablakok elfalazásáról, de ha ablakok mégis megmaradnak, akkor azokon legyen belülről átlátszó fólia
- a padlóburkolatok, berendezési tárgyak tűzálló és antisztatikus anyagból legyenek
- az épület villámvédelme elégítse ki a kommunális- és lakóépületekre vonatkozó előírásokat
- a nyílászárók (ajtók, ablakok) rendelkezzenek nyitottság és zártság ellenőrző eszközzel; ablakok esetében ez helyettesíthető biztonsági rácsokkal
- a számítógépterembe belépni szándékozók belépés előtti automatikus azonosításának lehetősége (pl. mágneskártya, proximity kártya) álljon rendelkezésre
- a számítógépterembe történő be- és kilépés rendje legyen szabályozva

Munkaállomások

A megfelelő adat biztonság elérésében a munkaállomások védelme is fontos szerepet játszik.

Javasoljuk az alábbi megoldások alkalmazását, szabályzások bevezetését:

- Minden munkaállomást úgy kell konfigurálni, hogy rendszerindítás csak a merevlemezről történhessen. A floppy-ról, CD-ről, USB pen-drive-ról, vagy hálózatról történő rendszerindítást megfelelő technikai megoldásokkal meg kell akadályozni.
- A nagy mennyiségű adat másolására alkalmas eszközök (CD író, USB pen-drive) használata csak az erre jogosult személy jóváhagyásával engedélyezett. Az ilyen eszközök használatát alapértelmezésben le kell tiltani a munkaállomásokon.
- A külső eszközök csatlakozását lehetővé tevő funkciók (IRDA, BlueTooth) használata csak az erre jogosult személy jóváhagyásával engedélyezett. Az ilyen eszközök használatát alapértelmezésben le kell tiltani a munkaállomásokon.
- A munkaállomások beállításának változtatását (BIOS) jelszóval kell védeni, a változtatást csak az erre jogosult személy végezhetik el.
- A munkaállomások beállítását, konfigurálását és üzemeltetését oly módon kell megoldani, hogy azon az üzemeltetőn kívül más személy ne telepíthessen semmilyen szoftvert.
- Minden munkaállomáson kötelező a képernyővédő telepítése. Amikor a Felhasználó 5 percen túl nem használja a számítógépét, a képernyővédőnek automatikusan el kell sötétítenie a képernyőt. Ajánlott, hogy a visszalépés csak a jelszó megadásával történhessen.

- A munkaállomásokon a szervezet számára fontos és bizalmas adatokat nem szabad tárolni.
- A szervezet biztosítsa az informatikai rendszerének egészére kiterjedő rendszeres és folyamatos vírusvédelmet, vírusellenőrző programnak mindig a legújabb verziója működjön. A frissítéseknek maximum 1 munkanapon belül meg kell történniük. Vírusellenőrzés történjen a helyi hálózaton, a levelező szerveren, valamint az összes munkaállomáson.
- A végleges, vagy kapott dokumentumokat, a rendszerekből exportált adatokat a központi szervereken kialakított mappákban kell tárolni.
- Az Internethez csak a szervezet hálózatán keresztül szabad csatlakozni – szigorúan tilos bármilyen egyedi modem használata.
- A felhasználók az Internetet csak a munkájukkal összefüggésben használhatják.
- Az Internetről tilos a munkához nem szükséges állományokat letölteni, vagy letöltött szoftverkomponenst (pl. plug-in-t), frissítést futtatni.
- A szervezeten belül tilos a lánc-levelek (un. spam-levelek) pilótajáték-szerű továbbküldése, terjesztése, csatolt ismeretlen állományok leindítása.