Üzemeltetési környezet leírása (KAPELLA menetvonal igénylés-kezelő rendszer, tesztrendszer és fejlesztői környezet, illetve hardverkörnyezet) 1. sz. melléklet

NetBIOS név	Megnevezés	Méret	Operációs rendszer	IP1	man. IP1	man. IP2	CPU	Memória	HDD
kmst020st	IBM Storage System DS3200 Dual Controller	2U	none	none	192.168.252.20	192.168.252.21	n.a.	n.a.	7db IBM 3.5" HDD SATA 1TB Dual Port HS 7200rpm
kasrv162fw	IBM x3500 m3 Torony (fw1)	5U	FreeBSD 8.0		none	none	1db Xeon Dual Core	512MB	2db 250 GB SAS
kasrv163fw	IBM x3500 m3 Torony (fw2)	5U	FreeBSD 8.0		none	none	1db Xeon Dual Core	512MB	2db 250 GB SAS
kasrv010esx	IBM szerver x3650 M2 QC Xeon E5504 2.00GHz, 2x 3GB SAS HBA Controller PCI Express x8, DVD-RW, BR10i, 2x675W Hot-Swap pws	2U	VMWare ESXi 4.0	192.168.250.10	192.168.252.10	none	2db QC Xeon E5504 2.00GHz	32GB	4x256GB 2.5" HotSwap SSD
kasrv011esx	IBM szerver x3650 M2 QC Xeon E5504 2.00GHz, 2x 3GB	2U	VMWare ESXi 4.0	192.168.250.11	192.168.252.11	none	1db QC Xeon E5504 2.00GHz	32GB	2x256GB 2.5" HotSwap SSD

	SAS HBA Controller PCI Express x8, DVD-RW, BR10i, 2x675W Hot-Swap pws								
kasrv012esx	IBM szerver x3650 M2 QC Xeon E5504 2.00GHz, 2x 3GB SAS HBA Controller PCI Express x8, DVD-RW, BR10i, 2x675W Hot-Swap pws	2U	VMWare ESXi 4.0	192.168.250.12	192.168.252.12	none	1db QC Xeon E5504 2.00GHz	16GB	2x256GB 2.5" HotSwap SSD
kmsw250sw	LINKSYS Switch 8X1000Mbps, Menedzselt	1U	none	none	192.168.252.250	none			
kmsw251sw	LINKSYS Switch 8X1000Mbps, Menedzselt		none	none	192.168.252.251	none			
kmsw252sw	SMC 16 port switch	1U	none	none	none	none			

2. sz. melléklet

Követelmények és feladatok

Műszaki specifikáció

Jelen üzemeltetési feladat magában foglalja:

a) a KAPELLA Menetvonal-igénylő Informatikai Rendszer (továbbiakban: KAPELLA) üzemeltetését (üzemi, teszt, dev környezet)
b) a KAPELLA rendszer működéséhez szükséges adatbázis (adatmentés, helyreállítás) üzemeltetését
c) a KAPELLA és a kapcsolódó informatikai rendszerek közötti adatátvitelt biztosító interfészek üzemeltetését, monitorozását
d) valamint a KAPELLA rendszer működését biztosító hardverek üzemeltetését, mely kiterjed a fizikai és virtuális szerverek hardver- és operációs rendszer szintű üzemeltetésére, a fizikai és virtuális hálózat üzemeltetésére, a biztonságos távoli elérési rendszer működtetésére, és a biztonsági szolgáltatásokra (pl: Tanúsítvány kezelés)

I. Az üzemeltetési körben meghatározott főbb célok és az ajánlatban elvárt követelmények, feladatok

1. KAPELLA és a hozzá kapcsolódó adatbázis rendszerüzemeltetése során elvégzendő feladatok:
   - az alkalmazás és interfészek üzemkészségének folyamatos, gépi úton történő, háttérben futó monitorozása, manuális ellenőrzése,
   - az alkalmazáshoz kapcsolódó interfészek működésének funkcionális ellenőrzése,
   - adatkonzisztencia ellenőrzés, szükség esetén manuális, illetve automatikus hibajavítás elvégzése,
   - hibák észlelése során intézkedés kezdeményezése a javítás érdekében, Megrendelő tájékoztatása,
   - adatfeldolgozás támogatása, adathibák kezelése
   - Megrendelő igénye szerint a program használatának biztosításához szükséges általános felhasználói segítségnyújtás,
   - tesztrendszer és adatbázisának frissítése az éles rendszer módosításával egy időben,
   - fejlesztői környezet és adatbázisának frissítése/módosítása az éles rendszer fejlesztésével összefüggésben,
   - a tesztrendszer éles adatbázisból történő frissítése megrendelői igény alapján,
   - az elvégzett tevékenység dokumentálása, Megrendelő folyamatos tájékoztatása (státusz készítés a havi feladatokról, hibákról, üzemeltetési eseményekről),
   - Üzemeltetési dokumentációk éves frissítése, aktualizálása.

2. Hardver környezet üzemeltetésével kapcsolatos feladatok ellátása, mely az alábbi tevékenységek elvégzésére terjed ki:
   - Redundáns hardver eszközök üzemeltetetése
   - Felmerülő hibajelenségek SLA-ban vállalt szintek alapján megoldani.
   - Havi riportok (SLA, üzemeltetési és IB események) és éves szolgáltatásértékelés

- Rendszerhez kapcsolódó hibajegyek és elhárítási idők központi kezelése
- Tanúsítvány alapú web szolgáltatások üzemeltetése
- Behatolás érzékelő rendszer (IDS), üzemeltetése és fejlesztése
- Integrált jogosultságkezelő rendszer üzemeltetése
- Mentési és archiválási rendszer üzemeltetése, rendszeres mentések készítése és rendszeres helyreállítási gyakorlatok elvégzése
- IT szolgáltatások, IT rendszer monitorozása, teljesítménymérése
- Információbiztonsági és üzemeltetési események nyilvántartása és kezelése
- Eseménynapló állományok központi gyűjtése és rendszeres elemzése
- Vészhelyzeti kézikönyv fenntartása és rendszeres gyakorlatok elvégzése
- Üzemeltetési dokumentációk és folyamatleírások éves frissítése, aktualizálása
- Disaster Recovery Site üzemeltetése

3. Általános üzemeltetési feladatok:

- *Fizikai és virtuális szerverek hardver- és operációs rendszer szintű üzemeltetése:*

Szerverek üzemeltetése:

- Szerver szoftverhez, hardverhez kapcsolódó hibajelenségek és igények SLA-ban vállalat megoldása
- Javító csomagok telepítése
- Tevékenység dokumentálása

- *Fizikai és virtuális hálózat üzemeltetése:*

- Hálózati eszközök fenntartása
- Hibajelensége és igények teljesítése

- *Monitorozó rendszer üzemeltetése:*

- Központi IT rendszer monitorozása teljesítmény mérése
- Figyelmeztető rendszer üzemeltetése
- Monitorozó rendszert érintő hibák elhárítása
- Igények teljesítése

- *Adatmentés és helyreállítás:*

- Fájlszintű adatmentés
- Virtuális kiszolgálók mentése
- Adatbázis mentések elvégzése
- Helyreállítási igények elvégzése

- *Biztonságos távoli elérési rendszer üzemeltetése (VPN):*

- Felhasználó-adminisztráció

- VPN környezet üzemeltetése
- Központi rendszereket érintő VPN hibák elhárítása

- *Központi tárhely (Storage) üzemeltetése:*
  - Az igényelt fájlrendszer kialakítása és beállítása
  - Központi tárhely üzemeltetése
- *Adatbázis üzemeltetése:*
  Központi adatbázisok:
  - Hibajelenségek elhárítása és igények tejesítése SLA-ban vállalt szinten
  - Adatbázis jogosultság kezelése
  - Adatbázis, ill. táblák helyreállításának elvégzése
- *Monitoring E-mail rendszer:*
  - A Monitoring E-mail rendszer üzemeltetése
- *Tűzfal üzemeltetése:*
  Tűzfal üzemeltetés:
  - Interface-ek üzemeltetése, felügyelete
  - Hardver- és szoftverüzemeltetés
  - A tűzfal konfiguráció módosítása
  - A tűzfal hibák, igények SLA-ban vállalt szintű megoldása
  - Biztonsági javítások elvégzése
  - Konfirguráció mentés készítése
- *WEB szerver:*
  WEB-szerver üzemeltetés:
  - WEB szolgáltatást érintő hibák és igények SLA-ban vállalat megoldása
  - Biztonsági javítások, beállítások elvégzése
- *Integrált jogosultsági rendszer:*
  Jogosultság kezelőrendszer üzemeltetése:
  - Felhasználók kezelése (létrehozás, módosítás, visszavonás)
  - Jogosultságok kezelése

4. Biztonsági szolgáltatások:

- *IDS rendszer:*
  IDS rendszer üzemeltetése:

- IDS rendszert érintő hibák és igények megoldása
- Biztonsági konfiguráció módosítása
- Javítások telepítése
- Jelentések, értesítések

- *Log elemzés:*
  - SYSLOG szerver üzemeltetése
  - Központi logok rendszeres elemzése
  - Rendszeres riportok, jelentések készítése
- *Kockázatkezelés:*
  Központi rendszerek érintő kockázatok kezelése:
  - Éves kockázat kezelés elkészítése
  - Kockázatok nyilvántartása
  - Kockázatokra tett lépések nyilvántartása
- *IT Biztonság:*
  Központi rendszereket érintő IT Biztonság kezelése:
  - Biztonsági szabályok meghozatala
  - Kontroll funkciók fejlesztése és fenntartása
  - Biztonsági események feltárása, nyilvántartása
  - Belső auditok lefojtatása
  - Behatolás vizsgálatok elvégzése
  - Riportok, jelentések készítése
  - Rendszerekhez tartozó ISMS fenntartása
  - Üzemeletetési dokumentációk ellenőrzése
- *Tanúsítványkezelés:*
  - Publikus WEB szerver tanúsítványainak kezelése
  - Belső CA üzemeltetés
  - Belső tanúsítványok kezelése (kiadás, , visszavonása, stb.)
- *DRP szolgáltatások:*
  - Vészhelyzet gyakorlatok irányítása
  - Vészhelyzeti kézikönyv fenntartása

5. Service Delivery:

- *Hibajegy-kezelés:*
  - Hibajegyek, események nyilvántartása:
  - Riportok
- *SLA:*
  Szolgáltatási szinthez kapcsolódó feladatok:
  - SLA és teljesítménymáréshez kapcsolódó rendszerek fenntartása
  - Havi riportok elkészítése
- *IT folyamatok:*
  Központi rendszereket érintő:
  - Folyamat fenntartása
  - Igények alapján folyamatok módosítása
- *SDM:*
  - Ügyfél igények összefogása
  - Üzemeltetés állapotáról tájékoztatás

II. Funkcionális követelmények

A rendszerrel szemben támasztott funkcionális követelmények fenntartása, hibamegoldások
Rendelkezésre állás:

- 7x24 és 99,9%

Rendszereket érintő hibák elhárítása:

Hibaosztály	Válaszidő (óra)	Megoldási idő (óra)
Kritikus hiba	2	8
Súlyos hiba	12	16
Közepes hiba	24	36
Enyhe hiba	48	72

III. A KAPELLA működését biztosító adatbázis és a kiszolgáló hardverek jellemzői:

A teljes környezet egy VMware VSphere 4.0 (VS40) rendszerre épül. A VMware által kifejlesztett virtuális infrastruktúra, mely nagy megbízhatóságot, és a rendelkezésre álló erőforrások optimális kihasználtságát biztosítja.

A VPE Kft-nek jelenleg a KAPELLA adatbázisban és a Monitoring adatbázisban két adatbázis szerveren vannak tárolva az adatai, melyek PostgreSQL alapúak. A két adatbázis szerveren megtalálhatók az adott adatbázis üzemi, teszt, valamint a KAPELLA esetében a fejlesztési (dev) adatbázisai.

A KAPELLA rendszer felhasználói kézikönyve elérhető a VPE Kft. honlapján, az alábbi címen: http://www2.vpe.hu/hu/kapella

1. A KAPELLA adatbázis fizikailag a következő objektumokat tartalmazza:
    - 226 adatbázis tábla
    - 589 adatbázis függvény
    - 158 szekvencia
    - 51 trigger

Az adatbázis logikailag a következő fő adatcsoportokat kezeli:

- Teljes vasúti infrastruktúra leírás menetrendi időszakokra lebontva
    - Szolgálati helyek
    - Vasútvonalak
    - Infrastruktúrakezelő társaságok
- Generált útvonalak
- Menetvonal megrendelések
- Kiszerkesztett menetrendek
- Szolgáltatások
- Partnerek
- Járművek
- Menetrendi időszakok
- Pályahasználati díjak
- Vágányzárak, vágányzári menetrendek
- Felhasználói műveletek (pl. státuszváltás) naplózása
- Felhasználók, Jogosultságok

2. A Monitoring adatbázis fizikailag a következő objektumokat tartalmazza:

    14 adatbázis tábla
    60 adatbázis függvény
    13 szekvencia

1 trigger

3. Az adatbázis logikailag a következő fő adatcsoportokat kezeli:

- Kiutalt menetvonalak
  - Iktatószám
  - Megrendelési időpont
  - Vonatnem kategória
  - Közlekedés napja és indulási ideje
  - Megrendelő szervezet
  - Lemondási díj
  - Késői megrendelés többletköltsége
  - Megrendelési idősáv azonosítója
  - Vonatnem
- Menetvonal közlekedéséhez kapcsolódó terv-tény adatok útvonalpontonként
  - Szolgálatai hely UIC statisztikai száma
  - Terv-tény időadatok
  - Közlekedtetési díj adott szakaszra
  - Naplózott adat típusa (áthaladás, indulás, érkezés) terv-tény
  - Vonatszám
- Menetrendtől való eltérések
  - Eltérés mértéke (idő)
  - Eltérés oka
- Partnerek
- Felhasználók, Jogosultságok

4. A VPE Kft. jelenlegi hardvereinek műszaki jellemzői

NetBIOS név	Megnevezés	Méret	Operációs rendszer	IP1	man. IP1	man. IP2	CPU	Memória	HDD
kmst020st	IBM Storage System DS3200 Dual Controller	2U	none	none	192.168.252.20	192.168.252.21	n.a.	n.a.	7db IBM 3.5" HDD SATA 1TB Dual Port HS 7200rpm
kasrv162fw	IBM x3500 m3 Torony (fw1)	5U	FreeBSD 8.0		none	none	1db Xeon Dual Core	512MB	2db 250 GB SAS
kasrv163fw	IBM x3500 m3 Torony (fw2)	5U	FreeBSD 8.0		none	none	1db Xeon Dual Core	512MB	2db 250 GB SAS
kasrv010esx	IBM szerver x3650 M2 QC Xeon E5504 2.00GHz, 2x 3GB SAS HBA Controller PCI Express x8, DVD-RW, BR10i, 2x675W Hot-Swap pws	2U	VMWare ESXi 4.0	192.168.250.10	192.168.252.10	none	2db QC Xeon E5504 2.00GHz	32GB	4x256GB 2.5" HotSwap SSD
kasrv011esx	IBM szerver x3650 M2 QC Xeon E5504 2.00GHz, 2x 3GB SAS HBA Controller PCI Express x8, DVD-RW, BR10i, 2x675W Hot-	2U	VMWare ESXi 4.0	192.168.250.11	192.168.252.11	none	1db QC Xeon E5504 2.00GHz	32GB	2x256GB 2.5" HotSwap SSD

	Swap pws								
kasrv012esx	IBM szerver x3650 M2 QC Xeon E5504 2.00GHz, 2x 3GB SAS HBA Controller PCI Express x8, DVD-RW, BR10i, 2x675W Hot-Swap pws	2U	VMWare ESXi 4.0	192.168.250.12	192.168.252.12	none	1db QC Xeon E5504 2.00GHz	16GB	2x256GB 2.5" HotSwap SSD
kmsw250sw	LINKSYS Switch 8X1000Mbps, Menedzselt	1U	none	none	192.168.252.250	none			
kmsw251sw	LINKSYS Switch 8X1000Mbps, Menedzselt		none	none	192.168.252.251	none			
kmsw252sw	SMC 16 port switch	1U	none	none	none	none			

IV. Interfészkapcsolatok:

Az alábbi ismert interfészkapcsolatok üzemelnek jelenleg a VPE szervere és idegen szerverek között.

Interfészkapcsolatok és adatkapcsolati lehetőségek							
Megnevezés	**Partner**	**Csatorna**	**Közvetlenül érintett interfész**	**További érintett interfészek**	**Adattartalom**	**Adatküldés iránya**	**Adatküldés gyakorisága**
CARGO interfész	CARGO	Webservice	KAPELLA, MEMO, ZUGDB, VEDB	VONTAT2	Menetvonal igénylés, Státuszváltás, Menetrend	VPE felől, VPE felé	folyamatos, 1 percenként
CARGO menetrend interfész	CARGO	SFTP	KAPELLA, MEMO	VONTAT2, Mb.rail	Menetrend	VPE felől	folyamatos, 5 percenként
CER interfész	CER	Webservice	KAPELLA, CER		Menetvonaligénylés, státuszváltás	VPE felől, VPE felé	folyamatos, 1 percenként
GYSEV 1.1-es							
GYSEV menetrend interfész	GYSEV	SFTP	KAPELLA, VIHAR	VONTAT2, Mb.rail	Menetrend	VPE felől	folyamatos, 5 percenként
GYSEV Tényadat	GYSEV	Webservice	TOR, KAPELLA, VIHAR				folyamatos, 1 percenként
IÜR interfész	MÁV PÜ	Webservice	KAPELLA, IÜR	FOR, PASS2	Menetvonaligény, PÜ véleény, Menetrend	VPE felől, VPE felé	folyamatos, 1 percenként
Kiutaló e-mail	Megrendelő	e-mail	KAPELLA		A link a kiutalások tartalmához	VPE felől	kiutaláskor
Külső adatbázisfelhasználók		Közvetlen adatbáziskapcsolat Interneten keresztül	Azonosító és jelszó ismeretében közvetlen SQL kapcsolaton keresztül a teljes adatbázis elérhető				
Külső TAKT felhasználók		Közvetlen adatbáziskapcsolat Interneten keresztül	A TAKT programban és annak kiegészítő alkalmazásaiban implementált lekérdezéseken keresztül a teljes adatbázis elérhető. Adatszűrés a távoli alkalmazásokon belül van megoldva.				
MÁV Tényadat	MÁV PÜ	Webservice	TOR, KAPELLA, FOR				folyamatos, 1 percenként
Minisztériumi tájékoztatás	Minisztérium	e-mail	KAPELLA		A kiutalt menetvonalakról értesítés a minisztérium számára	VPE felől	kiutaláskor
MMV interfész	MMV	Webservice	KAPELLA, MMV		Menetvonaligénylés, státuszváltás	VPE felől, VPE felé	folyamatos, 1 percenként
PDF interfész PÜ-nek	MÁV PÜ	Webservice	KAPELLA, IÜR		Menetrend	VPE felől	lekérdezéskor
PÜ tájékoztatás	MÁV PÜ	e-mail	KAPELLA		A kiutalt menetvonalakról értesítés a PÜ számára	VPE felől	kiutaláskor
Rakodóterület foglaltság lekérdezés	MÁV PÜ	Webservice	KAPELLA, IÜR		A rakodóterület foglaltság adatai	VPE felől	lekérdezéskor
START interfész	START	Webservice	KAPELLA, METERV	VONTAT2	Menetvonal igénylés, Státuszváltás, Menetrend	VPE felől, VPE felé	folyamatos, 1 percenként
START menetrend interfész	START	SFTP	KAPELLA	VONTAT2, Mb.rail	Menetrend	VPE felől	folyamatos, 5 percenként
TRAKCIÓ interfész	TRAKCIÓ	Webservice	KAPELLA, VONTAT2		Menetvonal igénylés, Státuszváltás, Menetrend	VPE felől, VPE felé	folyamatos, 1 percenként
TRAKCIÓ menetrend interfész	TRAKCIÓ	SFTP	KAPELLA, VONTAT2	MB.rail	Menetrend	VPE felől	folyamatos, 5 percenként
Vágányzári interfész	MÁV PÜ	Webservice	KAPELLA, IÜR		Vágányzári igénylés, Státuszváltás	VPE felől	folyamatos, 1 percenként
Veszélyhelyzeti interfész	MÁV PÜ	Webservice	KAPELLA, FOR, IÜR		Veszélyhelyzeti visszavonások	VPE felé	Veszélyhelyzeti visszavonás esetén
Vonatszám lekérdezés	MÁV PÜ	Webservice	KAPELLA, IÜR		Vonatszámozási állapot	VPE felől	lekérdezéskor
Vonatszám megadás	MÁV PÜ	Webservice	KAPELLA, IÜR		Vonatszám	VPE felé	folyamatos, 1 percenként
VPE-n belüli TAKT felhasználók	VPE munkatársai	Közvetlen adatbáziskapcsolat bérelt vonalon keresztül	Belső rendszer				

V. **Az üzemeltetési időszak alatt a VPE Kft. az alábbi fejlesztéseket tervezi a KAPELLA rendszeren:**

Feladat	Fejlesztés üzemi használatának kezdete	Fejlesztés leírása	Nagysága az üzemelő rendszerhez képest
HÜSZ,TÖR évközi lekövetése	Folyamatos	A 2013/2014-es HÜSZ, TÖR év közbeni változásainak lekövetése a KAPELLA rendszerben és interfészeken.	2%
KAPELLA igazítása a VPE Kft. mikro-szintű adatbázisához	2013. szeptember	A KAPELLA jelenleg a TAKT adatbázis 161 táblájában tárolt makro-szintű infrastruktúra adatokat használja. Az adatbázis elkülönített 64 db tk_topo táblájában mikro-szinten vannak tárolva az adatok, ami többlet funkcionalitást eredményezne a KAPELLA működését illetően.	5%
Vágányzári modul módosítása	2013. július	A KAPELLA-ban kialakításra kerülne az összehangolási eljárás és a vágányzári egyeztetés lebonyolítását támogató felület.	2%
Vágányzári megrendelő interfész fejlesztése	2013. július	A KAPELLA-ban jelenleg üzemelő VPE felől irányú interfész VPE felé ágának fejlesztése, mely segítségével interfészen keresztül is lehetne vágányzárat megrendelni.	1%
Szolgáltatásvéleményező interfész kifejlesztése a PCS-hez	2013. november	Kétirányú interfészkapcsolat építése a C-OSS által alkalmazott egy ablakos megrendelő rendszerhez (PCS)	2%
Félautomata katalógus felajánlás továbbfejlesztése	2013. október	Félautomata katalógus felajánló algoritmus továbbfejlesztésének KAPELLA-t érintő módosításainak követése	0,5%

HÜSZ mellékletek, e-HÜSZ igazítás	2013. október	Az adatbázis karbantartó felület továbbfejlesztésével a VPE Kft. és a PHM-ek erre kijelölt felhasználói képesek a HÜSZ-t érintő módosításokat közvetlenül elektronikusan átvezetni, állapotvezérelten. Jelen fejlesztés eredményeként lehetőség nyílna a VPE Kft. előtt, hogy a HÜSZ táblázatos formátumú mellékleteit automatikusan állítsa elő, valamint a honlapjáról elérhető elektronikus HÜSZ, ún. e-HÜSZ a továbbfejlesztett adatbázisból jelenítse meg az információkat.	0,5%
TÖR módosított koncepció szerinti ösztönző elemek kialakítása	2013. november	TÖR évközi változásain kívüli koncepcionális változások átvezetése a KAPELLA rendszeren	0,5%

VÉGLEGES MŰSZAKI-SZAKMAI AJÁNLAT

A PEGACONSULT Tanácsadó Kft. (1087 Budapest, Könyves Kálmán körút 54-60.), mint ajánlattevő az alábbi - az ajánlattételi felhívásban és dokumentációban megfogalmazottakkal egyező – tartalmú műszaki-szakmai ajánlatot teszi.

Az üzemeltetési feladat magában foglalja

a) a KAPELLA Menetvonal-igénylő Informatikai Rendszer (továbbiakban: KAPELLA) üzemeltetését (üzemi, teszt, dev környezet)
b) a KAPELLA rendszer működéséhez szükséges adatbázis (adatmentés, helyreállítás) üzemeltetését
c) a KAPELLA és a kapcsolódó informatikai rendszerek közötti adatátvitelt biztosító interfészek üzemeltetését, monitorozását
d) valamint a KAPELLA rendszer működését biztosító hardverek üzemeltetését, mely kiterjed a fizikai és virtuális szerverek hardver- és operációs rendszer szintű üzemeltetésére, a fizikai és virtuális hálózat üzemeltetésére, a biztonságos távoli elérési rendszer működtetésére, és a biztonsági szolgáltatásokra (pl.: tanúsítvány kezelés)

Az üzemeltetési körben meghatározott főbb célok és az elvárt követelmények, feladatok

1. KAPELLA és a hozzá kapcsolódó adatbázis rendszerüzemeltetése során elvégzendő feladatok:
   - az alkalmazás és interfészek üzemkészségének folyamatos, gépi úton történő, háttérben futó monitorozása, manuális ellenőrzése,
   - az alkalmazáshoz kapcsolódó interfészek működésének funkcionális ellenőrzése,
   - adatkonzisztencia ellenőrzés, szükség esetén manuális, illetve automatikus hibajavítás elvégzése,
   - hibák észlelése során intézkedés kezdeményezése a javítás érdekében, Megrendelő tájékoztatása,
   - adatfeldolgozás támogatása, adathibák kezelése
   - Megrendelő igénye szerint a program használatának biztosításához szükséges általános felhasználói segítségnyújtás,
   - tesztrendszer és adatbázisának frissítése az éles rendszer módosításával egy időben,
   - fejlesztői környezet és adatbázisának frissítése/módosítása az éles rendszer fejlesztésével összefüggésben,

- a tesztrendszer éles adatbázisból történő frissítése megrendelői igény alapján,
- az elvégzett tevékenység dokumentálása, Megrendelő folyamatos tájékoztatása (státusz készítés a havi feladatokról, hibákról, üzemeltetési eseményekről),
- Üzemeltetési dokumentációk éves frissítése, aktualizálása.

Hardver környezet üzemeltetésével kapcsolatos feladatok ellátása, mely az alábbi tevékenységek elvégzésére terjed ki:

- Redundáns hardver eszközök üzemeltetetése
- Felmerülő hibajelenségek SLA-ban vállalt szintek alapján megoldani.
- Havi riportok (SLA, üzemeltetési és IB események) és éves szolgáltatásértékelés
- Rendszerhez kapcsolódó hiba bejelentések és elhárítási idők központi kezelése
- Tanúsítvány alapú web szolgáltatások üzemeltetése
- Behatolás érzékelő rendszer (IDS), üzemeltetése és fejlesztése
- Integrált jogosultságkezelő rendszer üzemeltetése
- Mentési és archiválási rendszer üzemeltetése, rendszeres mentések készítése és rendszeres helyreállítási gyakorlatok elvégzése
- IT szolgáltatások, IT rendszer monitorozása, teljesítménymérése
- Információbiztonsági és üzemeltetési események nyilvántartása és kezelése
- Eseménynapló állományok központi gyűjtése és rendszeres elemzése
- Vészhelyzeti kézikönyv fenntartása és rendszeres gyakorlatok elvégzése
- Üzemeltetési dokumentációk és folyamatleírások éves frissítése, aktualizálása
- Disaster Recovery Site üzemeltetése

Általános üzemeltetési feladatok:

- *Fizikai és virtuális szerverek hardver- és operációs rendszer szintű üzemeltetése:*

  Szerverek üzemeltetése:

  - Szerver szoftverhez, hardverhez kapcsolódó hibajelenségek és igények SLA-ban vállalat megoldása
  - Javító csomagok telepítése
  - Tevékenység dokumentálása
- *Fizikai és virtuális hálózat üzemeltetése:*

  - Hálózati eszközök fenntartása
  - Hibajelensége és igények teljesítése

- *Monitorozó rendszer üzemeltetése:*
  - Központi IT rendszer monitorozása teljesítmény mérése
  - Figyelmeztető rendszer üzemeltetése
  - Monitorozó rendszert érintő hibák elhárítása
  - Igények teljesítése
- *Adatmentés és helyreállítás:*
  - Fájlszintű adatmentés
  - Virtuális kiszolgálók mentése
  - Adatbázis mentések elvégzése
  - Helyreállítási igények elvégzése
- *Biztonságos távoli elérési rendszer üzemeltetése (VPN):*
  - Felhasználó-adminisztráció
  - VPN környezet üzemeltetése
  - Központi rendszereket érintő VPN hibák elhárítása
- *Központi tárhely (Storage) üzemeltetése:*
  - Az igényelt fájlrendszer kialakítása és beállítása
  - Központi tárhely üzemeltetése
- *Adatbázis üzemeltetése:*
  Központi adatbázisok:
  - Hibajelenségek elhárítása és igények tejesítése SLA-ban vállalt szinten
  - Adatbázis jogosultság kezelése
  - Adatbázis, ill. táblák helyreállításának elvégzése
- *Monitoring E-mail rendszer:*
  - A Monitoring E-mail rendszer üzemeltetése
- *Tűzfal üzemeltetése:*
  Tűzfal üzemeltetés:
  - Interface-ek üzemeltetése, felügyelete
  - Hardver- és szoftverüzemeltetés
  - A tűzfal konfiguráció módosítása
  - A tűzfal hibák, igények SLA-ban vállalt szintű megoldása
  - Biztonsági javítások elvégzése
  - Konfirguráció mentés készítése
- *WEB szerver:*
  WEB-szerver üzemeltetés:

- WEB szolgáltatást érintő hibák és igények SLA-ban vállalat megoldása
- Biztonsági javítások, beállítások elvégzése

- *Integrált jogosultsági rendszer:*
  Jogosultság kezelőrendszer üzemeltetése:
  - Felhasználók kezelése (létrehozás, módosítás, visszavonás)
  - Jogosultságok kezelése

2. Biztonsági szolgáltatások:

- *IDS rendszer:*
  IDS rendszer üzemeltetése:
  - IDS rendszert érintő hibák és igények megoldása
  - Biztonsági konfiguráció módosítása
  - Javítások telepítése
  - Jelentések, értesítések
- *Log elemzés:*
  - SYSLOG szerver üzemeltetése
  - Központi logok rendszeres elemzése
  - Rendszeres riportok, jelentések készítése
- *Kockázatkezelés:*
  Központi rendszerek érintő kockázatok kezelése:
  - Éves kockázat kezelés elkészítése
  - Kockázatok nyilvántartása
  - Kockázatokra tett lépések nyilvántartása
- *IT Biztonság:*
  Központi rendszereket érintő IT Biztonság kezelése:
  - Biztonsági szabályok meghozatala
  - Kontroll funkciók fejlesztése és fenntartása
  - Biztonsági események feltárása, nyilvántartása
  - Belső auditok lefojtatása
  - Behatolás vizsgálatok elvégzése
  - Riportok, jelentések készítése
  - Rendszerekhez tartozó ISMS fenntartása
  - Üzemeletetési dokumentációk ellenőrzése
- *Tanúsítványkezelés:*

- Publikus WEB szerver tanúsítványainak kezelése
- Belső CA üzemeltetés
- Belső tanúsítványok kezelése (kiadás, , visszavonása, stb.)

- *DRP szolgáltatások:*
  - Vészhelyzet gyakorlatok irányítása
  - Vészhelyzeti kézikönyv fenntartása

3. Service Delivery:
   - Riportok

- *SLA:*
  Szolgáltatási szinthez kapcsolódó feladatok:
  - SLA és teljesítménymméréshez kapcsolódó rendszerek fenntartása
  - Havi riportok elkészítése
- *IT folyamatok:*
  Központi rendszereket érintő:
  - Folyamat fenntartása
  - Igények alapján folyamatok módosítása
- *SDM:*
  - Ügyfél igények összefogása
  - Üzemeltetés állapotáról tájékoztatás

Funkcionális követelmények

A rendszerrel szemben támasztott funkcionális követelmények fenntartása, hibamegoldások
Rendelkezésre állás:

- 7x24 és 99,9%

Rendszereket érintő hibák elhárítása:

Hibaosztály	Válaszidő (óra)*	Megoldási idő (óra)*
Kritikus hiba	2	8
Súlyos hiba	12	16
Közepes hiba	24	36
Enyhe hiba	48	72

Az ajánlott, alkalmazott munkamódszer, szoftverelemek bemutatása, valamint az üzemeltetési tevékenység hátterének és környezetének áttekintése

Data Center és a szerverek fizikai védelme

A **www.kapella.hu** tartomány szerverei jelenleg az Invitel adatközpontban (1108 Budapest, Kozma u. 2.) találhatóak.

IT rendszer és összetevői

A fizikai szerverek 2 csoportba oszthatók szerepkörök szerint:

- Tűzfal-
- Virtuális kiszolgálók

Az egyes szerepköröket 2 db tűzfal és 3 db virtuális kiszolgáló látja el a redundancia biztosításának érdekében. A fizikai szerverek egységes operációs rendszer környezetben Debian GNU/Linux stabil v5.0 verziót futtatnak.
Virtuális kiszolgálókon az egyes feladatok elvégzésére Debian GNU/Linux stable v5.0 és Microsoft Windows Server 2003 Standard verzió van telepítve.

Logikai védelem

Az FW1 és FW2 szerverek egyenként 100Mbps-os Internet és 80Mbps béreltvonali kapcsolattal rendelkeznek. Nyilvános IP címek portjain lehetséges a belső szerverek szolgáltatásait elérni. A kialakított környezet belső hálózati kapcsolattal nem rendelkezik, így kívülről elérhetőek az adatbázisok, web kiszolgálók, adminisztratív bejelentkezések.

Az Internet felől megkülönböztethetőek:

- a hozzáférési jogosultsággal rendelkező felhasználók, ügyfelek, adminisztrátorok, fejlesztők kapcsolódását a rendszerekhez.
- a hozzáférési jogosultsággal nem rendelkező illetéktelen, támadó személyek és sebezhetőséget kereső rendszerek kapcsolódási kísérleteit.

A rendszerre ható veszélyek kiváltó okát teljesen megszüntetni nem lehetséges, azonban szükséges a rendszerre gyakorolt hatásuk csökkentése. Ez utóbbi veszélyek kiszűrése, a megfelelő védelmi intézkedések érvényesítése, ellenőrzési pontok és felelős személyek megjelölése az alapfeladat. A rendszer egyes komponensein meghozott védelmi intézkedések ennek a célnak igyekeznek megfelelni.

Operációs rendszerek védelme

A telepített **Debian GNU/Linux** esetében a szerverek telepítése és biztonsági beállításainak alapjául a Securing Debian Manual[1]-ban szereplő irányelveket és ellenőrző listát[2] hajtja végre a telepítést végző adminisztrátor.

A főbb beállítások áttekintése:
A *partíciók* kialakításakor a több felhasználós környezetből és a szenzitív adatok védelme érdekében az egyes feladatok és szerepek alapján kerülnek felosztásra.
A *fájlrendszer* kiválasztásában a terhelhetőség, gyorsaság, naplózási szolgáltatások, a megbízhatóság és a könnyű adminisztráció játszik szerepet. A telepítés védett környezetben készült, internet kapcsolatba a biztonsági frissítések telepítése után és a biztonsági irányelvek betartását követően kerül.
Az *adminisztrátor (root) jelszó* az ajánlatkérőnélüzemelő jelszó-szabályok alapján került kialakításra, mely 8 karakternél nem rövidebb, kis- és nagybetűket és speciális karaktereket tartalmazó karaktersor. A root jelszó borítékban lezárva páncélszekrényében szükséges őrizni.

A jelszó-házirend elvei a következők 3:

- Jelszó-hosszúság: 8-16 karakter hosszúságú karaktersor
- Összetett karakterek
- md5 titkosítási algoritmus használata

A **Microsoft Windows Server 2003** telepítése a Windows Server 2003 Security Guide[4] irányelveinek megfelelően történik. A Windows kiszolgálókra vonatkozó alap biztonsági irányelvek és politikák kiegészülnek a fájlszerverekre vonatkozó irányelvekkel.

---

[1] SD http://www.debian.org/doc/manuals/securing-debian-howto/
[2] SD 211-217.oldal
[3] /etc/pam.d/common-password
[4] http://www.microsoft.com/downloads/details.aspx?familyid=8a2643c1-0685-4d89-b655-521ea6c7b4db&displaylang=en

Mentések

A mentések két területe a fájl- (WEB, PHP) és az adatbázis-mentések. A fájlok mentése heti teljes és napi különbségi mentéssel történnek. Az alkalmazás és a PostgreSQL adatbázis teljes mentése óránként történik, adatbázis dump-ok segítségével. Az adatbázismentések példányai naponta egyszer átkerülnek a **VPE belső szerverére (mail.vpe.hu),** utána napi pontossággal lehet visszaállni a korábbi adatbázis állapotra

Patch kezelés

A Windows és LINUX esetében kritikus, biztonsági hibákat javító frissítések a teszt és az éles környezet esetében kézzel kerülnek telepítésre. Jelentősebb verzióváltással járó frissítéseket változáskezelési folyamatban vezetik be. A javítások telepítése és kezelése szorosan összefügg a mentések kezelésével.

Vírusvédelem

Az előforduló vírusok a Linux operációs rendszerre nincsenek hatással, nem veszélyeztetik annak működését. Azonban a Linux kiszolgálók ügyfelei jelentős hányadban Windows munkaállomások, ezért kiemelt fontosságú, hogy e kapcsolódási területeken (http, sftp, ftp, samba, stb.) tárolt könyvtárakban legyen rendszeres víruskeresés. Ezen megoldások meggátolják a kártékony programok továbbterjedését.

Sebezhetőségi vizsgálatok, auditok

Havi rendszerességgel behatolási vizsgálatokat végeznek a **PEGAConsult Kft.** munkatársai, feltárva és megvizsgálva a rendszer sebezhetőségét. Ennek eredményéről, a feltárt hibákról és a meghozott ellenintézkedésekről jegyzőkönyv készíthető.

Hálózati biztonság, tűzfalak

Egyes fizikai szervereket tűzfal beállítások védik. Ezek szabályozzák a publikált szolgáltatások elérését és tiltják a nem kívánt szolgáltatás-eléréseket. 6 db publikus címen érhetők el az egyes szolgáltatások.

Felhasználói fiókok és jogosultág kezelés

Jelenleg az egyes rendszerekben lokálisan tárolt felhasználók és felhasználói csoportok kerültek alkalmazásra. Jelenlegi megvalósítás az Információ Biztonsági elemezésben került bővebb feltárásra.

EFR – Emeltszintű felügyeleti rendszer (Monitorozás)

A **PEGACONSULT Kft.** saját szervereiről végez monitorozási funkciókat. Követi a szerverek hibaüzeneteit, terhelését, rendelkezésre állását. Az értékek kritikus szint alá csökkenése esetén azonnal SMS riasztást küld az adminisztrátoroknak, akik 24 órás felügyeletet látnak el. Működése saját fejlesztésű modulok segítségével

eseménynaplók, szolgáltatás ellenőrzések és szkriptek futtatásából áll. A fenti vizsgálatokat az **EFR felügyeleti rendszer** percenkénti ciklusban hajtja végre. Ez a gyakorlatban azt jelenti, hogy meghibásodás esetén gyakorlatilag 1 percen belül SMS üzeneten keresztül értesülnek a PEGAConsult Kft. munkatársai a meghibásodásról, és el tudják kezdeni a hibaelhárítást.

Az üzemeltetési feladatok végrehajtásának ajánlott ütemezése, periodicitása
Folyamatos üzemeltetési tevékenységek

- A KAPELLA menetvonal igénylés-kezelő rendszer, az ahhoz kapcsolódó interfészek, a VPE adatbázisa (DBA feladatok), a rendszereket futtató hardverkörnyezet, operációs rendszerek, tűzfalak, hálózati elemek, storage rendszer és virtualizációs környezet folyamatos használatának biztosítása, üzemeltetése.
- Redundáns hardver eszközök üzemeltetetése
- Felmerülő hibajelenségek SLA-ban vállalt szintek alapján megoldani.
- Rendszerhez kapcsolódó hiba bejelentések és elhárítási idők központi kezelése
- Tanúsítvány alapú web szolgáltatások üzemeltetése
- Behatolás érzékelő rendszer (IDS), üzemeltetése és fejlesztése
- Integrált jogosultságkezelő rendszer üzemeltetése
- Mentési és archiválási rendszer üzemeltetése, rendszeres mentések készítése és rendszeres helyreállítási gyakorlatok elvégzése
- IT szolgáltatások, IT rendszer monitorozása, teljesítménymérése
- Információbiztonsági és üzemeltetési események nyilvántartása és kezelése
- Eseménynapló állományok központi gyűjtése és rendszeres elemzése
- Disaster Recovery Site üzemeltetése

Negyedéves üzemeltetési tevékenységek:

- Negyedéves riportok (SLA, üzemeltetési és IB események) és éves szolgáltatásértékelés

Éves üzemeltetési tevékenységek

- Vészhelyzeti kézikönyv fenntartása és rendszeres gyakorlatok elvégzése
- Üzemeltetési dokumentációk és folyamatleírások éves frissítése, aktualizálása

A szolgáltatási szint teljesítéséhez, üzemeltetési feladatok ellátásához ajánlott humánerőforrások szükségessége és időbeni rendelkezésre állásuk

A PEGAconsult Kft. az üzemeltetési feladatok ellátásához 7x24 órában HelpDesk-et biztosít az alábbi elérhetőségekkel:

Telefon	+36 20 402-4020
Email	support@pega.hu

A HelpDesk alábbi csoportokat és személyi összetevőket foglalja magában:

- Elsőszintű támogatók (7x24 órás) 5 fő
- Második szintű támogatók
  - Rendszerüzemeltetési szakértők 3 fő
  - Alkalmazásüzemeltetési szakértők 3 fő
- Harmad szintű támogatók
  - Apache+PHP specialista 2 fő
  - IBM HW specialista 2 fő
  - Postgres DBA specialista 2 fő
  - Linux és VMWare specialista 2 fő

3. sz. melléklet

Informatikai biztonsági szabályzat

VPE Kft.
Informatikai Biztonsági Szabályzat
Hatályos 2013. október 1-tól

Verzió: 1.0

VPE/102-85/1/2013

Vasúti Pályakapacitás-elosztó
Korlátolt Felelősségű Társaság

	Kelt	Név	Beosztás	Aláírás
Készítette:	2013.09.17	Bak Máté	IT előadó	
Ellenőrizte:	09.27	Tálasné Balla Klára	Osztályvezető	
Jóváhagyta:		Németh Réka	Ügyvezető	

Verziókövetés

Változtatások átvezetése

Verzió	Dátum	Változtatás tárgya	Változtatás indoka	Változtatást átvezette Aláírás	Változtatást ellenőrizte Aláírás
1.0	2013.10.01.	Hatálybalépés	-		

Változtatások hatályba lépésének engedélyezése

Verzió	Dátum	Név	Aláírás
1.0	2013.10.01.	Németh Réka	

Tartalom

1. Általános rendelkezések

1.1 Az Informatikai Biztonsági Szabályzat (továbbiakban: IBSZ) célja

Az IBSZ kiadásának célja:

- A Vasúti Pályakapacitás-elosztó Kft. (továbbiakban: VPE) területén a termékeket és szolgáltatásokat, valamint a társaság működését támogató informatikai rendszerek által kezelt adatok bizalmasságát, sértetlenségét és folyamatos rendelkezésre állását fenyegető veszélyek megelőzésére, elhárítására alkalmazott védelmi intézkedések végrehajtásának szabályozása,

- A VPE informatikai rendszereinek fejlesztésében, üzemeltetésében résztvevő társaságok és azok munkavállalóinak feladatának, és felelősségének meghatározása,

- hogy a védelmi intézkedések maradéktalan implementálásának alapját képezve hozzájáruljon a társaság egyenszilárdságú és meg nem kerülhető biztonsági alrendszerének kialakításához.

Az IBSZ kiadásának szükségessége:
Az IBSZ a VPE informatikai rendszereinek, információbiztonsági dokumentációjának egyik fontos dokumentuma. Rögzíti az informatikai eszközök, és rendszerek használata, valamint üzemeltetése során betartandó szabályokat, valamint a felhasználók (VPE munkavállalók, üzemeltető és fejlesztő szervezetek) felelősségi körét a rendszer által kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése érdekében.

1.2 Hatálya

Az IBSZ-t a VPE ügyvezető igazgatója hagyhatja jóvá és helyezheti hatályba. Az IBSZ a jóváhagyás napján lép hatályba és a következő verzió kibocsátásáig vagy visszavonásig érvényes.

1.2.1 Személyi hatály

Az IBSZ személyi hatálya kiterjed a VPE valamennyi, az informatikai elemeivel bárminemű kapcsolatba kerülő vagy az informatikával a jövőben kapcsolatot létesítő munkavállalójára, tisztségviselőjére, nevezetesen:

- Informatikáért felelős munkatárs,
- Az üzemeltetésért felelős természetes és jogi személyekre,
- A fejlesztésért felelős természetes és jogi személyekre,
- Üzleti területek szakmai felelőseire,
- Az informatika folyamataiban érintett szervezeti egységek kijelölt szakmai felelőseire,
- A VPE egyéb munkavállalóira.

Illetve az informatikával szerződéses vagy más módon kapcsolatba kerülő egyéb természetes és jogi személyekre a velük kötött szerződés vagy titoktartási nyilatkozat alapján.

1.2.2 Tárgyi hatály

Az IBSZ tárgyi hatálya kiterjed a következő VPE által használt informatikai rendszereire, azok hardverelemére és fizikai környezetére:

Informatikai rendszer	Üzemeltető
KAPELLA	PEGAconsult Kft.
TAKT	TRAN-SYS Rendszertechnika Kft.
KAPELLA adatbázis	PEGAconsult Kft.
Iktató	PEGAconsult Kft.
Díjképző	PEGAconsult Kft.
InfoTéka	Négypólus Számítástechnika Kft.
VPE belső hálózat	Négypólus Számítástechnika Kft.
Munkaállomások	Négypólus Számítástechnika Kft.

1. táblázat
VPE informatikai rendszerek

Az IBSZ tárgyi hatálya kiterjed továbbá,

- minden, az informatikai rendszerekhez tartozó szoftver elemre,
- VPE-nél keletkezett, tárolt, fogadott, küldött adat felhasználására vonatkozó utasításokra,
- minden, informatikai rendszerekben keletkezett, a rendszerek által kezelt, azok által továbbított információkra, illetve a rendszerekhez kapcsolódó papíralapon vagy elektronikus formában tárolt dokumentumokra

1.3 Az IBSZ és más szabályzatok kapcsolata

Az IBSZ szorosan kapcsolódik a VPE Kft. alább felsorolt szabályzataihoz:

- Munkavédelmi Szabályzat,
- A VPE Vasúti Pályakapacitás-elosztó Kft. Selejtezési és leltározási szabályzata,
- KAPELLA és KAPELLA DB Kiviteli és migrációs terv,
- KAPELLA és KAPELLA DB Üzemeltetési kézikönyv,
- KAPELLA és KAPELLA DB Vészhelyzeti kézikönyv.

1.4 Felülvizsgálat

Az IBSZ aktualizálása az informatikai biztonságért felelős munkavállaló (IT előadó) feladata. Új védelmi intézkedés bevezetése, védelmi intézkedés módosítása, fejlesztése esetén át kell vezetni a Szabályzatban a változásokat.

Aktualizálás szükséges a hatályos jogszabályok, belső szabályzatok változásának megfelelően is, valamint az IBSZ tartalmát befolyásoló szoftver/hardver fejlesztés esetében, illetve éves rendszerességgel.

Az elkészült új verziójú, módosított Szabályzatot helyben szokásos módon kell közzétenni a VPE-n belül, és egyidejűleg gondoskodni kell arról, hogy megküldésre kerüljön a VPE által kijelölt külső partnerei felé, melyért az IT előadó felelős.

2. Fogalomtár

KAPELLA: on-line Menetvonal-igénylő és kezelő rendszer a kapacitás-elosztási folyamat támogatására. A rendszer 100%-os vagyoni értékű jogával a VPE rendelkezik.

Iktató rendszer: on-line iktató rendszer, amelyen keresztül végzi a VPE a céget érintő, ott keletkező, bejövő és kimenő dokumentumok regisztrálását, delegálását, feladatok osztását a végfelhasználókra, valamint azok teljesítésének naplózását. A rendszerhez minden VPE munkavállaló rendelkezik hozzáféréssel. A rendszer 100%-os vagyoni értékű jogával a VPE rendelkezik.

TAKT: menetrendszerkesztésre, valamint az adatbázis (makro- és mikro-szintű, 100%-os VPE tulajdonban) karbantartására lehetőséget adó program, melyben a VPE több mint 10%-os vagyoni értékű joggal rendelkezik.

HÜSZ: Hálózati Üzletszabályzat, amely tartalmazza a kapacitás-elosztás jogszabályi hátterét, a nyílt hozzáférésű vasúti pályahálózat igénybevételének feltételeit, a vasúti infrastruktúra adatokat, a kapacitás-elosztás eljárásait, a vasúti infrastruktúrához hozzáférésre jogosultak számára nyújtandó szolgáltatásokat, díjakat.

TÖR: Teljesítményösztönző Rendszer, amely tartalmazza, a TÖR jogszabályi hátterét, alapelveit, elemeit, a reklamációkezelés folyamatát, jogvitás ügyek kezelésének eljárását, elszámolási szabályokat, adatigények meghatározását.

IT munkatárs: a VPE informatikai területéért felelős alkalmazottja.

SLA: Service Level Agreement - szolgáltatási szint megállapodás

Rendszerüzemeltető: az IT munkatárs koordinálásával rendszerfelügyeletet ellátó, külső, szerződésben meghatározott, rendszergazdai szerepkörben tevékenykedő cég.

Felhasználó: az infrastruktúrát használó személy. Általában munkavállaló, de minden olyan személy, aki a cég által rendelkezésre bocsátott informatikai infrastruktúrát használja.

Mobil eszköz: hordozható számítógép, internetkapcsolat létesítésére alkalmas mobiltelefon vagy adathordozó.

Tűzfal: célja, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás. Külső tűzfal, ami a teljes hálózatot részben elválasztja az Internettől. Belső tűzfal a helyi hálózatnak egy különösen védendő részét zárja el annak többi részétől és az Internettől is.

3. Feladat-, felelősség- és hatáskör elhatárolása

3.1 Ügyvezető igazgató

A VPE mindenkori ügyvezető igazgatója, aki felelős a VPE által kezelt adatvagyon bizalmasság, sértetlensége és rendelkezésre állása megőrzésért.
Feladata és felelőssége a VPE egészére kiterjedően:

- mindazon anyagi, humán és erkölcsi feltétel biztosítása, amely szükséges a VPE informatikai rendszereinek védelmi rendszerterve megvalósításához,
- IBSZ kiadása, érvényesítése
- informatikai szolgáltatóra vonatkozó követelmények betartásának ellenőrzése, együttműködve az IT munkatárssal,
- engedélyezi a VPE munkavállalók felhasználói jogosultságát,
- kijelöli a felhasználók jogosultságainak beállítását, jóváhagyását, ellenőrzését végző felelős személyt,
- intézkedések foganatosítása az ellenőrzések során feltárt hiányosságok megszüntetésére,
- vizsgálat kezdeményezése és lefolytatása a tudomására jutott biztonságsértő eseményekkel kapcsolatosan

3.2 IT munkatárs

A VPE IT munkatársa feladatai:

- A VPE Kft. informatikai eszközeinek felügyelete, kapcsolattartás a rendszergazdákkal, programfejlesztőkkel.
- Javaslattétel az informatikai rendszer működésének javítására, a szükséges fejlesztések előkészítése
- Naprakész nyilvántartás készítése a szoftver és információ-technikai eszközállományról
- Jelentések készítése a menetvonal-igénylő informatikai rendszerének adatbázisa alapján
- Informatikai szabályzatok elkészítése, folyamatos aktualizálása
- A rendszergazdák által elvégzett munkák felügyelete, ellenőrzése, nyilvántartása
- A VPE honlapjának felügyelete, adatok feltöltése
- Adatszolgáltatás a „Közadat-program"-ban
- Közreműködés a VPE Kft. informatikai stratégiájának elkészítésében
- Közreműködés a VPE Kft. informatikai témájú közbeszerzési-, és versenyeztetési eljárásoknban
- Közreműködés a VPE Kft. folyamataihoz illeszkedő IT fejlesztési igények összegyűjtésében, rendszerezésében, tervezésében
- Közreműködés a VPE Kft. folyamataihoz illeszkedő IT megoldások kidolgozásában, a fejlesztésekhez kapcsolódó dokumentációk összeállításában
- Közreműködés a VPE Kft. IT rendszereihez kapcsolódó egyéb rendszerekkel összefüggő egyeztetések lebonyolításában, a kapcsolattartásban
- A VPE Kft-nél lebonyolított informatikai fejlesztések VPE oldali projektvezetői feladatainak ellátása kijelölés szerint

3.3 Kiemelt felhasználók

Valamennyi VPE informatikai rendszert felhasználó köteles:

- elolvasni és megismerni az adott rendszer felhasználói kézikönyvét,
- az adott rendszer használata során a jelszó használati és a jogosultsági szabályokat betartani,
- az adott rendszer használata során az észlelt biztonsági eseményeket a közvetlenül fölérendelt vezetőnek vagy a rendszer felhasználói adminisztrátorának haladéktalanul jelezni.

A VPE informatikai rendszereinek kiemelt felhasználó típusait a 2. táblázat tartalmazza.

Szerepkör	*Feladat*	*Fizikai terület*	*Logikai terület*	*Objektum*	*Jogosultság*
Üzemeltető (KAPELLA)	Üzemeltetési tevékenységek	Általa kezelt eszközök helyiségei, illetve Invitel Datacenter	KAPELLA és interfészek	KAPELLA rendszer és adatbázis (éles, teszt és dev) Monitoring adatbázis	Írás, olvasás, törlés, futtatás, frissítés, telepítés
Üzemeltető (TAKT)	Üzemeltetési tevékenységek	Általa kezelt eszközök helyiségei	TAKT	TAKT és adatbázis (éles, teszt, dev)	Írás, olvasás, törlés, futtatás, frissítés, telepítés
Üzemeltető (VPE)	Üzemeltetési tevékenységek	Általa kezelt eszközök helyiségei, VPE szerverszoba	Levelezés, belső hálózat	MS Exchange, Windows Server, Asztali alkalmazások	Írás, olvasás, törlés, futtatás, frissítés, telepítés
Felhasználói adminisztrátor (KAPELLA)	Felhasználói fiókok karbantartása	VPE iroda	KAPELLA	KAPELLA rendszer és adatbázis (éles, teszt és dev)	Írás, olvasás, törlés,
Felhasználói adminisztrátor (TAKT)	Felhasználói fiókok karbantartása	VPE iroda	TAKT	TAKT és adatbázis (éles, teszt, dev)	Írás, olvasás, törlés,
Felhasználói adminisztrátor (VPE)	Felhasználói fiókok karbantartása	VPE iroda	Munkaállomások Levelezés, belső hálózat	MS Exchange, Windows Server	Írás, olvasás, törlés,
Adatbázis szerkesztő	Infrastruktúra karbantartás, HÜSZ követés	Általa kezelt eszközök helyiségei	TAKT-KAPELLA adatbázis	TAKT adatbázis szerkesztő	Írás, olvasás, törlés
Adatbázis lekérdező	Jelentések, lekérdezések készítése, elemzése	Általa kezelt eszközök helyiségei	TAKT-KAPELLA, Monitoring és Díjképző adatbázis	TAKT adatbázis szerkesztő, pgAdmin	Olvasás
Honlap szerkesztő	Honlap naprakészen tartása	Általa kezelt eszközök helyiségei	Honlap	Honlapszerkesztő	Írás, olvasás

2. táblázat
Kiemelt felhasználótípusok

3.4 Felhasználók

Valamennyi felhasználó:

- köteles e szabályzat megismerésére,
- jogosult a munkavégzéséhez szükséges informatikai infrastruktúrához való hozzáférésre,
- köteles az alkalmazás használata során a jelszó használati és jogosultsági szabályokat betartani,
- jogosult a magáncélú felhasználás során keletkezett anyagainak elkülönítésére,
- köteles együttműködni a rendszerüzemeltetésért felelős személyekkel,
- a munkaállomás hibás működése vagy zavar esetén köteles haladéktalanul értesíteni az IT munkatársat

3.5 Üzemeltető szervezetek

Az üzemeltető szervezet, mint a VPE rendszerének üzemeltetője informatikai biztonsági feladatait és felelősségét szervezeti szinten a VPE IBSZ-ben általános jelleggel meghatározott feladatok és a saját biztonsági szabályzatai határozzák meg.

3.5.1 PEGAconsult Kft.

1087 Budapest, Könyves Kálmán krt. 54-60. I. emelet. A PEGAconsult Kft. felelős a következőkben felsorolt informatikai rendszerek üzemeltetéséért.

3.5.1.1 KAPELLA

KAPELLA üzemeltetése, valamint a hardver környezet üzemeltetésével kapcsolatos feladatok ellátása. Az üzemeltetés során elvégzendő feladatokat részletesen a hatályos üzemeltetési szerződés tartalmazza.

3.5.1.2 Iktató

Iktató rendszer üzemeltetése, valamint a hardver környezet üzemeltetésével kapcsolatos feladatok ellátása. Az üzemeltetés során elvégzendő feladatokat részletesen a hatályos üzemeltetési szerződés tartalmazza.

3.5.1.3 Díjképző

Díjképző rendszer üzemeltetése, valamint a hardver környezet üzemeltetésével kapcsolatos feladatok ellátása. Az üzemeltetés során elvégzendő feladatokat részletesen a hatályos üzemeltetési szerződés tartalmazza.

3.5.2 TRAN-SYS Rendszertechnika Kft.

1036 Budapest, Lajos u. 48-66. B lépcsőház V. emelet. A TRAN-SYS Rendszertechnika Kft. felelős a következőkben felsorolt informatikai rendszerek üzemeltetéséért.

3.5.2.1 TAKT

TAKT rendszer üzemeltetése. Az üzemeltetés során elvégzendő feladatokat részletesen a hatályos támogatási szerződés tartalmazza.

3.5.3 Négypólus Számítástechnika Kft.

VPE munkaállomások, belső hálózat, levelező szerver üzemeltetése Az üzemeltetés során elvégzendő feladatokat részletesen a hatályos üzemeltetési szerződés tartalmazza.

4. Informatikai biztonsággal szemben támasztott követelmények

A rendszer informatikai biztonságát a bizalmasság, sértetlenség és rendelkezésre állás követelményei szerint, mindhárom területet figyelembe véve kell megvalósítani.

- Bizalmasság: a VPE által az informatikai rendszerekben, illetve azokon kívül feldolgozott adatok csak a munkakörük által indokoltan jogosult szereplők számára hozzáférhetőek. További szereplők számára a rendszerben tárolt és onnan kinyert adatok nem lesznek hozzáférhetők.
- Sértetlenség: a VPE-nél történő adatrögzítés és adatmódosítás úgy került kialakításra, hogy a felhasználóknak ne legyen lehetőségük jogosultságaikkal illetéktelen módosításra, adatok meghamisítására.
- Rendelkezésre állás: a VPE rendelkezik olyan informatikai rendszerrel (KAPELLA), amelynek teljes vagy részleges működésképtelensége esetén a kapacitás-elosztással és az országos vonatközlekedéssel kapcsolatos információk áramlása részben vagy teljesen megakadna. Ennek érdekében a VPE elvárása a rendszerrel számban a 99,9%-os rendelkezésre állás biztosítása.

Ennek megfelelően a VPE-nél keletkező, vagy beérkező adatok/dokumentumok a következők szerint csoportosíthatók:

- Publikus: szabad hozzáférés mindenki (VPE-n kívül is) számára
- Alap: szabad hozzáférés minden VPE munkavállaló számára
- Fokozott: hozzáférést információ, dokumentum vagy mappa létrehozója, vagy az ügyvezető igazgató engedélyezheti
- Kiemelt: hozzáférést kizárólag az ügyvezető igazgató engedélyezheti

4.1 Adatok besorolása

Adat keletkezése	Adat megnevezése	Besorolás szerkesztés szerint	Besorolás megtekintés szerint
Üzemmenettel kapcsolatos adatok	Menetvonal adatok	Kiemelt	Fokozott
	Pályakapacitás adatok	Kiemelt	Fokozott
	Infrastruktúra adatok	Kiemelt	Publikus
	Hálózat-hozzáférési díj adatok	Kiemelt	Publikus
	PHM adatszolgáltatás	Kiemelt	Fokozott
	VPE által karbantartott dokumentumok: HÜSZ, DM, DD, TÖR	Fokozott	Publikus
VPE támogató tevékenység	Pénzügyi adatok	Kiemelt	Kiemelt
	IT feladatok	Fokozott	Fokozott
	Osztály (MESZKO, KAPELO) feladatok	Fokozott	Fokozott
Szabályozó tevékenység	Szabályozó dokumentumok	Fokozott	Alap

3. táblázat
VPE-nél keletkező adatok biztonsági besorolása

4.2 Fájlok védelme, mentések

A kiemelt biztonságú adatokat a VPE informatikai rendszerekben kezeli, ennek megfelelően azok bizalmasságának védelme érdekében a következő védelmi intézkedések kerülnek alkalmazásra:

- a felhasználók adatokhoz való hozzáférése jogosultságokon keresztül szabályozható,
- fokozott jelszó biztonsági politika

Az adatok sértetlenségének védelme a felhasználók által munkájuk során létrehozott eredménytermékek esetén az azt létrehozó munkatársak feladata. A Felhasználók által létrehozott vagy rendelkezésre álló adatállományokat csoportokra utaló könyvtárba, illetve a profillal járó hálózati meghajtóra szükséges elhelyezni a fájlszerveren.
A saját gépen tárolt fájlok archiválásáról mindenkinek magának kell gondoskodni, szükség esetén az IT munkatárs segítségének igénybevételével. Saját fájlokat (képek, zene stb.) mindenki a saját gépén tárolja.
A fájlszerveren tárolt saját fájlokat az IT előadó a merevlemez kapacitásának növelése érdekében előzetes értesítés nélkül törölheti.
Az elsődleges szerverről teljes mentés készül minden héten vasárnap, amely a másodlagos szerverre átkerül. Naponta csak a változások kerülnek mentésre. Minden héten hétfőn reggel, automatikusan, külső HDD-re kerül a teljes mentés. A mentésért az IT munkatárs, illetve a Rendszergazda a felelős. Szerverhiba esetén a HDD-ről kerülnek visszaállításra az adatok, amely a Négypólus Kft. feladata. A mentési stratégia a következő:

- Fájlszerver könyvtárai,
- Active Directory (Felhasználók csoport tagságai, kapcsolódó egyéb tulajdonságok felhasználó specifikus beállításai)
- User Roaming Profile-ok
- Exchange szerveren tárolt postafiókok mentésével, biztosítva az azonnali visszatöltési lehetőséget
- Alkalmazások beállításai, alkalmazások adatbázisai

A rendszer beállításáról és a biztonságos üzemeltetéséről a Rendszergazda gondoskodik.

A nem helyi szervereknél a mentések két területe a fájl (-WEB, PHP) és az adatbázismentések. A TÖR adatbázis esetében a teljes mentések heti rendszerességgel történnek, a napi különbségek mentése, pedig naponta. A KAPELLA adatbázisról napi rendszerességgel készül teljes mentés. A mentéseket a PEGACONSULT Kft. végzi. Az átadás-átvételt követően az IT munkatárs a külső adattárolót, valamint az átadásról készült jegyzőkönyvet köteles elzárni a páncélszekrénybe.

5. Informatikai biztonsági rendszer kialakítása

5.1 Adminisztratív védelem

5.1.1 Azonosítások, hitelesítési mechanizmusok

A munkaállomásokhoz, valamint az informatikai rendszerekhez való hozzáférés felhasználói név és jelszó birtokában történik.
A munka kezdésekor a felhasználói felületen (operációs vagy egyéb informatikai rendszer) a felhasználónak meg kell adni a saját felhasználói nevét és a hozzá tartozó titkos jelszót. Ezekkel az adatokkal minden felhasználó egyedileg azonosítja magát.
A következő rendszerek esetében kerül sor jelszavas beléptetés:

- munkaállomás/operációs rendszer
- KAPELLA
- TAKT
- Iktató
- Díjképző
- InfoTéka
- adatbázisok

5.2 Fizikai védelem

5.2.1 Belépés a VPE irodájába

VPE alkalmazottak kivételével a székhelyre, illetve az irodába történő belépés az épület portáján történő regisztrációval lehetséges.

5.2.2 Belépés a szerverterembe

A KAPELLA szerverkörnyezete az Invitel Datacenterben található, és az Invitel szabályzata alapján történik a belépés, és a mozgáskövetés a teljes ott tartózkodás alatt.
Az Exchange szerverkörnyezet a VPE irodájában található szerverszobában kap helyet. Belépésre kizárólag az IT munkatárs, a Pályahálózat kapacitás-elosztási osztály vezetője jogosult, valamint a Rendszergazda a korábban felsoroltak valamelyikének felügyelete alatt. Munkaidőn kívüli rendkívüli esetben az IT munkatárs, illetve a Pályahálózat kapacitás-elosztási osztály vezetőjének tájékoztatása mellett az ügyeletes OSS menedzser is jogosult belépni.
A belépésekről a belépést jóváhagyó, valamint felügyelő köteles naplót vezetni.
Az ügyvezető igazgatónak lehetősége van eseti belépési engedély kiadására.

5.2.3 Adathordozók, hordozható eszközök

A külső adathordozók zárható szekrényben vannak elhelyezve a VPE telephelyén. Kulccsal csak az IT munkatárs rendelkezik. A szekrényben lévő informatikai eszközökhöz csak az IT munkatárs férhet hozzá, és a kivett/betett eszközökről nyilvántartást vezet.
A VPE eszközei közötti nyilvántartásokban szereplő hordozható informatikai eszközöket (számítógép, projektor stb.) a munkavállalók munkájuk elvégzéséhez igénybe vehetik.
Amennyiben a munkavállaló a hordozható eszközöket a VPE székhelyétől eltérő helyen kívánja használni, úgy azt szükséges kikölcsönözni. Az eszközöket az Informatikai előadó

tartja nyílván, felé kell jelezni annak igénybevételét. Az IT munkatárs köteles nyilvántartást vezetni a hordozható berendezések kölcsönzéséről. (1. számú melléklet)
A VPE tulajdonát képező közös használatban lévő hordozható műszaki- és számítástechnikai eszközöket (pl.: laptop, projektor, digitális fényképezőgép, diktafon stb.) kizárólagosan magán célú használatra igénybe venni csak a VPE ügyvezetőjének írásos engedélyével, valamint az IT munkatárs jóváhagyásával lehet. (2. számú melléklet)

5.2.4 Dokumentumok kezelésének szabályai a felhasználói munkahelyeken

Fokozott és kiemelt biztonsági osztályba tartozó dokumentum, információ nem maradhat egyetlen VPE munkavállaló íróasztalán a munkaidő letelte után. Azt követően a munkavállalónak kötelessége elzárni az ilyen jellegű anyagokat. Az IT munkatárs legalább negyedévente köteles az előírás betartásának vizsgálatára, előzetes bejelentés nélkül. A vizsgálat eredményeiről írásban köteles értesíteni az ügyvezető igazgatót.
Ehhez hasonlóan, amennyiben a felhasználók elhagyják munkaállomásukat kötelesek annak zárolására. Az esetleges mulasztás esetére az IT munkatárs felelős beállítani minden számítógépen, hogy 5 perc után automatikusan, jelszóval védve aktiválódjon a képernyőzárolás. A beállítást a felhasználók nem módosíthatják. Ennek betartását az IT munkatárs időszakonként (legalább negyedévente), előzetes bejelentés nélkül ellenőrzi.

5.2.5 Szoftvernyilvántartás és védelem

A VPE informatikai berendezéseire jogtiszta alapszoftverek kerülnek telepítésre. A telepítéseket az IT munkatárs vagy az ő koordinálásával és felügyeletével a szerződésben álló rendszergazda végzi.
Az alapszoftvereken túli, egyéb szoftvereknek a gépre telepítését, meglévők törlését, cseréjét az Ügyvezető engedélyezése mellett csak az IT munkatárs vagy annak felügyelete mellett a rendszergazda végezheti. A VPE jóváhagyja nyílt forráskódú szoftverek alkalmazását, azok használatáról és telepítésének engedélyezését az IT munkatárs döntés előkészítője elfogadásával az ügyvezető igazgató teheti.
Bármilyen legális vagy illegális program gépre telepítéséből eredő kárért (akár gépben keletkező kár, akár a szerzői jogok megsértéséből eredő kár) a felelősség a gépet használó munkavállalót terheli. Ennek érdekében az IT munkatárs, illetve a rendszergazda köteles félévente átvizsgálni minden munkaállomást.
A Felhasználó nem jogosult a cég szoftvereit magáncélra lemásolni, sem más gépre telepíteni.
A szoftverlicence-k és -forráskódok (fizikai) tárolása az IT előadó páncélszekrényében történik. A forráskódot tartalmazó adattároló átvételekor az átvevőnek és a szállítónak minden esetben meg kell győződni a forráskód meglétéről, majd együttesen kell lezárt borítékban elhelyezni.

5.3 Logikai védelem

5.3.1 Azonosítás, jogosultságkezelés

5.3.1.1 Felhasználói azonosítók

A munkaállomások esetében a bejelentkezés a felhasználó vezetéknevéből és keresztnevéből képzett loginnévvel történik a következőképpen: *gipsz.jakab*

A VPE informatikai rendszereibe történő belépés a legtöbb esetben a felhasználó vezetéknevéből és a keresztnév első betűjéből képzett loginnévvel történik a következőképpen: *gipszj*

5.3.1.2 Jelszókezelés

Minden felhasználó köteles a jelszavát titokban tartani, annak illetéktelen személynek történő továbbadása a VPE üzleti titok kezelésére vonatkozó szabályok megsértését jelenti.
A különböző hozzáférési jelszavakat tilos nyilvános helyen tartani.

5.3.1.3 Jelszóképzés szabályai

A jelszavak kiválasztásánál a következő alapvető szabályokat kell betartani:
A jelszó nem lehet rövidebb 8 karakternél, és nem egyezhet meg az utolsó alkalommal használt jelszóval. Minden esetben tartalmaznia kell numerikus karaktert (számjegyet), illetve kis- és nagybetűket is (í, y és z kivételével).

Az informatikai rendszerek ellenőrzik, hogy az alábbi lehetőségek ne fordulhassanak elő:

- Könnyen ki található jelszavak,
- A loginnevet, mint jelszók,
- Vezetéknév, keresztnév, mint jelszó,
- Azonos számokból vagy betűkből álló jelszó.

A jelszavakat mindenki köteles lezárt borítékban átadni az IT munkatársnak, a borítékon a nevének feltüntetésével. A borítékok felbontása indokolt esetben két tanú jelenlétében történik.
Minden esetben jegyzőkönyvet kell készíteni, majd az a jegyzőkönyv másolatával a borítékot le kell zárni.
A munkaállomások biztonságának növelése érdekében az IT munkatárs vagy a rendszergazda jogosult bármikor jelszócserét kérni.

5.3.2 Operációs rendszer, alkalmazás, adatbázis sajátosságai, védelmi funkciói

5.3.2.1 Munkaállomások

Átlagos asztali PC munkaállomás (16 db):

- Windows XP Professional
- Microsoft Office 2007

Átlagos notebook munkaállomás (11 db):

- Windows XP Professional
- Microsoft Office 2007

Frissített asztali PC munkaállomás (1 db):

- Windows 8 Professional
- Microsoft Office 2013

Frissített notebook munkaállomás (1 db):

- Windows 7 Professional
- Microsoft Office 2007

5.3.2.2 Szerver számítógépek, helyi szerverek

A VPE telephelyén jelenleg 3 szerver üzemel. Egy elsődleges és egy másodlagos szerver (arra az esetre, ha az elsődleges szerver meghibásodna), és egy tűzfal szerepet ellátó szerver.

Elsődleges szerver:

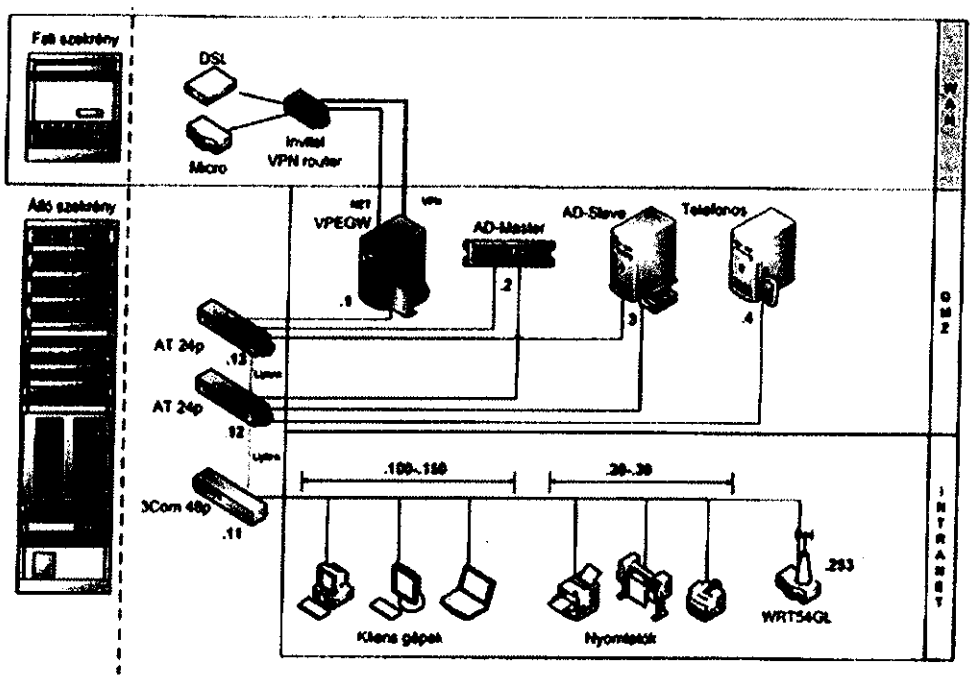
- MS Windows Server 2003 Active Directory szolgáltatása
- MS Exchange 2007 levelezőszerver szolgáltatása
- Nyomtatószerver szolgáltatása
- Fájlszerver szolgáltatása
- Helyi dolgozók autentikálása
- Mentés készítése a következőkről: „AD User Profile", levelezés adatok, valamint ezek replikálása a másodlagos szerverre.

Másodlagos szerver:

- MS Windows Server 2012 Active Directory szolgáltatása (elsődleges szerver hibája esetén)
- MS Exchange 2007 levelezőszerver szolgáltatása (elsődleges szerver hibája esetén)
- Összes adat replikálása az elsődleges szerverről
- Az elsődleges szerverről az adatok naponta egyszer kerülnek mentésre, a másodlagos szerverre.
- Külső adattárolóra a mentések erről a szerverről történnek.

Tűzfal:

A tűzfalszabályok folyamatosan változnak, mivel a naplófájlok alapján dolgozik egy programcsoport, amely bizonyos eseményekre tiltásokat kezdeményez. Ilyen esemény például a nagyobb mértékű spamtevékenység egy adott IP-címről vagy -tartományról.
Havonta egyszer kerül a rendszer teljes körű ellenőrzésre a Rendszergazda által, amely az adott hónap első hetében esedékes, hiba esetén a szükséges intézkedésekről az IT munkatárs köteles értesíteni az ügyvezető igazgatót.



1. sz. ábra - A VPE jelenlegi irodai informatikai rendszerének kialakítása

Felhasználói típusok:

- Domain Administrator,
- Domain User,
- Local Administrator.

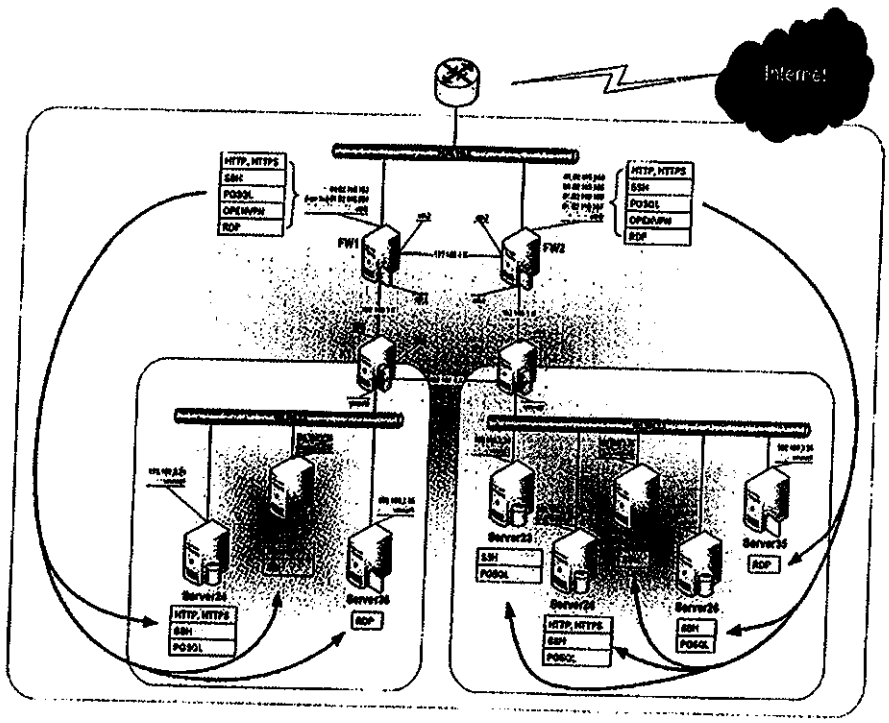
5.3.2.3 Szerver számítógépek, nem helyi szerver

A www.vpe.hu tartomány szerverei az Invitel Datacenterében kerültek elhelyezésre. A fizikai szerverek 2 csoportba oszthatók szerepkörök szerint:

- Tűzfal-
- Virtuális kiszolgálók

Az egyes szerepköröket 2-2 kiszolgáló látja el a redundancia biztosításának érdekében. A fizikai szerverek egységes operációs rendszerkörnyezetben Debian GNU/Linux stabil v4.0 verziót futtatnak.

Virtuális kiszolgálókon az egyes feladatok elvégzésére Debian GNU/Linux stable v4.0 és Microsoft Server 2003 Standard verzió került telepítésre.



2. sz. ábra - A VPE KAPELLA és TAKT rendszereket kiszolgáló szerverparkja

Tűzfal:
Évente egyszer, október első hetében a kialakított tűzfalszabályok rendszerének felülvizsgálata.

Monitorozás:
A PEGACONSULT Kft. végez monitorozási funkciókat. Követi a szerverek hibaüzeneteit, terhelését, rendelkezésre állását. Az értékek kritikus szint alá csökkenése esetén azonnal SMS riasztást küld az adminisztrátornak, akik 24 órás felügyeletet látnak el.

Negyedévente kerül sor egy KAPELLA környezetek biztonsága tárgyú értekezletre a PEGAconsult Kft. munkatársaival, ahol a résztvevők elemzik az elmúlt időszak eseményeit, valamint a stratégia fontosságú lépéseket is megtervezik a környezet biztonsága és rendelkezésre állása érdekében.

5.3.2.4 Hálózati szolgáltatások elérése

Azon VPE felhasználók számára, akik megfelelő jogosultsággal rendelkeznek az informatikai rendszerek hozzáféréséhez, a különböző rendszereket és környezeteket a következők szerint érhetik el.

Informatikai rendszer név	Környezet	Elérés
KAPELLA	Éles	www.kapella.hu
	Teszt	www.teszt.kapella.hu
	Dev	www.dev.kapella.hu
Iktató	Éles	www.iktato.vpe.hu
	Teszt	www.iktato-teszt.vpe.hu
Díjképző	Éles	www.dij.vpe.hu
	Teszt	www.dij-teszt.vpe.hu
	Dev	www.dij-dev.vpe.hu

4. táblázat
Informatikai rendszerek elérhetősége

Az adatbázis (éles, teszt, dev) elérés a KAPELLA web alkalmazás és az ügyfélgépekre telepített TAKT menetrendszerkesztő alkalmazás segítségével történik.
A TAKT menetrendszerkesztő alkalmazás adatelérése a PostgreSQL felhasználó és csoportjaik segítségével lehet.

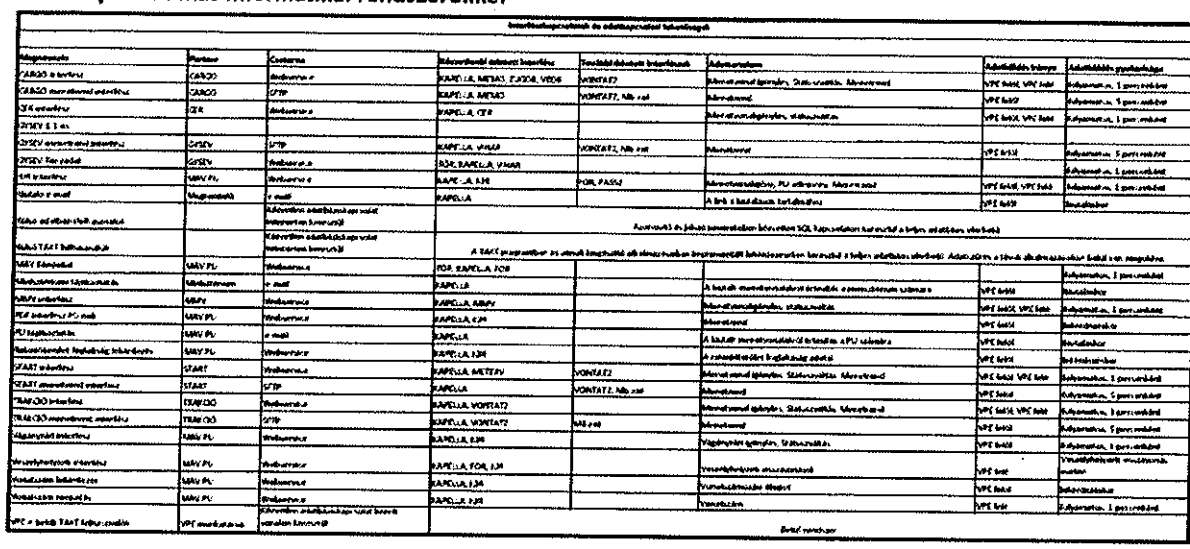
Jelenleg a VPE Kft-nél a kapacitás-elosztó tevékenységét folytató, illetve az adatbázis szerkesztő/lekérdező jogosultsággal rendelkező munkatársaknak van jogosultsága az alkalmazást használni. Új felhasználó felvételét, felhasználó inaktívvá váltását, illetve a jogosultságok módosítását kizárólag a „adminisztrátor" jogosultsággal rendelkező munkavállalók végezhetik.

Külső partner fejlesztő munkatársa kizárólag a VPE ügyvezető igazgatójának engedélyével érheti el a VPE-n kívülről az informatikai rendszereket, adatbázisokat. Az engedélynek a következőket kell tartalmaznia:

- engedélyre vonatkozó kérelem dátuma
- engedély oka
- engedélyezés dátuma
- engedélyezés hatálya
- engedélyezett fejlesztő nevének és a fejlesztő társaság megnevezése
- fejlesztő részére biztosított jogosultságok a 2. sz. táblázat alapján
- fejlesztés megnevezése, melynek keretében a fejlesztő felhasználhatja a kapott jogosultságokat

Az engedélyezés előtt a külső partner fejlesztője köteles aláírni egy felelősségvállaló nyilatkozatot (3. melléklet).

5.3.3 Kapcsolat más informatikai rendszerekkel



5.3.4 Bejelentkezés külső hálózatról

Kiutazások során szükséges lehet biztosítani a kiutazó munkavállalóknak, hogy elérjék a belső levelezés hálózatát. Ennek érdekében az ügyvezető igazgató engedélyezheti, hogy belső munkatársak nem bizalmas hálózatból hozzáférjenek a levelező rendszerhez.
A távoli elérés https titkosítással került kialakításra a következő elérési úttal:
https://mail.vpe.hu/owa

A bejelentkezés a munkaállomások esetében beállított felhasználó névvel és jelszóval lehetséges.
Az ügyvezető igazgató engedélyének a következőket kell tartalmaznia:

- felhasználó neve
- engedélyre vonatkozó kérelem dátuma
- engedély oka
- engedélyezés dátuma
- engedélyezés hatálya

5.3.5 Kártékony kódok és behatolás elleni védelem

A VPE telephelyén lévő elsődleges és másodlagos szerveren a vírusoktól való védelem érdekében Eset Nod32 víruskereső alkalmazás fut. A vírusdefiníciós adatbázis frissítése a munkaállomásokon automatikusan történik.
Az Invitel Datacenterében elhelyezett szervereken futó Linux operációs rendszerre nincsenek hatással a vírusok, nem veszélyeztetik annak működését. Ezeken a szervereken nincs víruskereső alkalmazás, mert a Linux elég biztonságot nyújt.
Az alap-vírusvédelemről, mindegyik, az informatikai rendszerben működő számítógépre feltelepített vírusmentesítő program gondoskodik. A VPE elektronikus levelezési rendszerét, így a bejövő kimenő e-mailek vírusellenőrzését, szűrését külön vírusmentesítő program biztosítja (levelezőszerver).

5.3.6 Biztonsági ellenőrzések

5.3.6.1 Biztonsági események

A szabályok megsértése jellemzően a következő eseményekben merül ki:

- bizalmas (fokozott vagy kiemelt biztonságú) adatok, információ verbális megosztása illetéktelenekkel vagy azok nyilvánosságra hozatala,
- bizalmas adatok (fokozott vagy kiemelt biztonságú), információ dokumentumon, adathordozón vagy IT rendszeren, pl. levelezéssel történő illegális továbbítása,
- vétlen közreműködés illetéktelen számítógépes hozzáférésben, pl. az iroda helyiség bezárásának, a számítógépes rendszerből való kilépés elmulasztásával a helyiség elhagyása esetén,
- tudatos közreműködés illetéktelen számítógépes hozzáférésben, pl. a jelszó elárulásával, annak érdekében, hogy a közreműködő ez által anyagi vagy más előnyhöz jusson,
- jelszóval történő visszaélés,

A vétségek szankcionálása annak súlyának függően munkajogi vagy büntetőjogi szinten történhet.
Biztonsági események észlelése esetén a jelen szabályzat személyi hatálya alá tartozó valamennyi személy köteles haladéktalanul tájékoztatni vezetőjét.

5.3.6.2 Biztonsági ellenőrzések

Az IT munkatárs köteles szúrópróba szerű ellenőrzést tartani a VPE irodájában, és meg vizsgálni az IBSZ-ben rögzített szabályok érvényesülését.
Vizsgálat személyi hatálya kiterjedhet:

- vezetők
- felhasználók
- rendszergazdák
- üzemeltetők

A vizsgálat gyakorisága:

- negyedévente

Az ellenőrzés formái a következők lehetnek:

- Beszámoltatás,
- Helyszíni ellenőrzés.

A vizsgálat során meg kell állapítani:

- milyen események történtek,
- az események milyen és mekkora kárt okoztak, okozhattak,
- milyen intézkedések szükségesek a keletkezett kár elhárításához, illetve annak mérsékléséhez
- események kiváltó okai, eseményei
- a bekövetkezett eseményekért közvetlenül és közvetve felelős személyek, a felelősség mértékével.

A vizsgálat eredményét az IT munkatárs köteles kiértékelni, és intézkedési tervet készíteni, javaslatot tenni, amennyiben szükséges. A vizsgálat eredményét az ügyvezető igazgatónak elő kell terjeszteni.

6. Üzemzavar, működési hiba esetén teendők, intézkedések, feladatok

Meghibásodás észlelésekor a hardver- vagy operációs rendszer hibát a rendszergazda felé, az alkalmazás hibát az alkalmazás üzemeltetők felé jelenteni kell.
Az észlelt hibát a Felhasználó köteles jelenteni elsődlegesen az IT előadó felé, aki amennyiben szükséges, azonnal értesíti a megfelelő személyt. Abban az esetben, ha az IT előadó nem érhető el, akkor az éppen szolgálatot teljesítő OSS-manager feladata a hiba bejelentése. A hatályos értesítési rend minden szobában kifüggesztésre kerül (4. melléklet). Az IBSZ hatályba lépését követően az IT munkatárs felelőssége az értesítési rendek ellenőrzése, illetve cseréje, amennyiben változás történt benne.

KAPELLA:
A PEGACONSULT Kft. 24 órás ügyeletet tart. Az Invitel Datacenterében elhelyezett szerverek hibája esetén értesítést kapnak a rendszertől, és azonnal intézkednek a hiba kijavításáról.

Hiba esetén értesíteni kell:

- elsődlegesen: Bősze Domonkos (06-20/280-74-94)
- másodlagosan: Marossy Szabolcs (06-30/218-72-05)
- harmadlagosan: Vingler Csaba (06-20/274-97-96)

TAKT:
Hiba esetén értesíteni kell:

- Vincze Béla (06-20/448-54-91)

VPE munkaállomások, levelezés:
A Négypólus Kft. a szolgáltatásokat az alábbi időszakban nyújtja:

- szolgáltatási időszak: munkanapokon 9:00 - 17:00
- készenléti időszak: szolgáltatási időszakon kívül eső, munka- és munkaszüneti napokon egyaránt.

Készenléti időszakban csak kritikus vagy súlyos hiba esetén vehető igénybe a Négypólus Kft. segítsége.

Hiba esetén értesíteni kell:

- elsődlegesen: Köves Krisztián (06-30/982-96-06)
- másodlagosan: Mészely Attila (06-70/369-18-71)
- harmadlagosan: Tóth-Szabó Nóra/ügyfélszolgálat (06-70/369-18-73)

Kritikus hibák:

- Internetkapcsolat megszakad, vagy lassan, bizonytalanul működik,
- Munkaállomás (notebook vagy asztali PC) nem kapcsolható be, gyakran lefagy, lassan, bizonytalanul működik,
- Perifériák meghibásodása

Súlyos hibák:

- Felhasználói profil nem töltődik be, a munkavégzés lehetetlen,
- Levelezés nem elérhetőm vagy nem lehet levelet küldeni és fogadni sem,
- Nyomtatás nem lehetséges, hálózati hiba.

2. sz. melléklet

Hordozható műszaki- és informatikai eszközök igénylése - kizárólagos magán célú használatra.

Alulírott, Németh Réka, a VPE ügyvezető igazgatója engedélyezem a Társaság tulajdonát képező műszaki- és/vagy számítástechnikai eszköz magán célú használatát az alábbi dolgozónak:

Igénylő neve:

Igényelt eszköz:

Igénylés időtartama:

20..... év ..... hó ..... napjától- .....hó .....napjáig.

.....

Németh Réka
Ügyvezető igazgató

3. sz. melléklet

FELELŐSSÉGVÁLLALÓ NYILATKOZAT

Alulírott

Név: .....
Anyja neve: .....
Születési hely, idő: .....
Lakcím: .....
Személyi igazolvány szám: .....
Adószám: .....

mint a VPE Kft-vel mint Megbízóval - továbbiakban Megbízó - szerződéses kapcsolatban álló Megbízott - továbbiakban: Megbízott - és/vagy Megbízott szerződéses alkalmazottja és/vagy megbízottja és/vagy lehetséges megbízott kijelentem, hogy a Megbízott és a Megbízó közötti szerződések alapján végzendő tevékenységek során a tudomásomra jutott üzleti titkot időbeli korlátozás nélkül a legteljesebb mértékben megtartom, azt harmadik személy számára át nem adom, harmadik személy számára hozzáférhetővé nem teszem. Jelen nyilatkozatban foglalt kötelezettségek függetlenül attól terhelnek, hogy a feladat ellátásra a megbízás létre jött-e vagy sem.

Kijelentem továbbá, hogy a megszerzett üzleti titkot haszonszerzés végett vagy más célból fel nem használom, nyilvánosságra nem hozom, továbbá megteszek minden intézkedést annak érdekében, hogy az üzleti titok harmadik személyek részéről se sérüljön meg.

Tudomásul veszem, hogy jelen nyilatkozat alkalmazása szempontjából különösképpen üzleti titoknak minősül a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás, irat vagy adat, melynek titokban maradásához a Megbízónak, Megbízottnak, vagy a Megbízó szerződő partnereinek méltányolható érdeke fűződik.

Tudomásul veszem, hogy az üzleti titok általam, vagy az általam felkért harmadik személyek által történt megsértése esetén Megbízó felé kötbérfizetési kötelezettségem áll fenn, melynek mértéke.....,- Ft, azaz tízmillió forint összeg.

Jelen nyilatkozatomat elolvasást és értelmezést követően, mint akaratommal mindenben megegyezőt az alulírott tanúk előtt írtam alá.

Budapest, 20..... ..... hó ..... nap

.....
felelősségvállaló

Előttünk, mint tanúk előtt:
++

1. Név: .....
Lakcím: .....
Szem.igsz.: .....

2. Név: .....
Lakcím: .....
Szem.igsz.:.....

4. sz. melléklet

Értesítési rend

Bak Máté (+36 1 301 99 29) vagy (+36 30 356 95 00) ha nem elérhető

OSS manager (+36 1 301 99 25)

PEGACONSULT Kft.

1. Bősze Domonkos
(06 20 280 74 94)
domonkos.bosze@pega.hu
KAPELLA interfész

2. Marossy Szabolcs
(06 30 218 72 05)
szabolcs.marossy@pega.hu
KAPELLA szerver

3. Vingler Csaba
(06 20 274 97 96)
vingler@pega.hu
KAPELLA

4. Vincze Béla
(06 20 448 54 91)
vincze.bela@vbnet.hu
KAPELLA

5. Szeibert Richard
(06 20 463 73 85)
richard.szeibert@pega.hu
KAPELLA interfész

Négypólus Kft.

1. Köves Krisztián
(06 30 982 96 06)
krisztian@negypolus.hu
IT, levelezés

2. Mészely Attila
(06 70 369 18 71)
attila.meszely@negypolus.hu
IT, levelezés

3. Tóth-Szabó Nóra
(06 70 369 18 73)
nora.toth-szabo@negypolus.hu
Ügyfélszolgálat

4. Károlyi József
(06 70 501 21 90)
jozsef.karolyi@negypolus.hu

HIBABEJELENTÉS-SZERVER
Munkaidőben (8:30-17:00):
+36 1 350 61 57
Munkaidőn kívül (17:00-8:30): +36 70 36 35 230
Ha a telefonállomás nem érhető el: +36 70 501 21 90

TRAN-SYS Kft.

1. Vincze Béla
(06 20 448 54 91)
takt@vbnet.hu
TAKT

Internet hiba esetén rendszergazdával történt egyeztetés után
Invitel hibabejelentő
06 80 880 088

Telefon hiba esetén
T-Home
hibabejelentő:
1400

Belső telefon hiba
Papp Gábor
06 30 668 67 00

4. sz. melléklet

Vállalkozó 7x24 órás rendszerfelügyeleti tevékenységet ellátó munkatársainak elérhetősége

A rendszerrel szemben támasztott funkcionális követelmények fenntartása, hibamegoldások

Rendelkezésre állás:

- 7x24 és 99,9%

Rendszereket érintő hibák elhárítása:

Hibaosztály	Válaszidő (óra)	Megoldási idő (óra)
Kritikus hiba	2	8
Súlyos hiba	12	16
Közepes hiba	24	36
Enyhe hiba	48	72

A szolgáltatási szint teljesítéséhez, üzemeltetési feladatok ellátásához ajánlott humánerőforrások szükségessége és időbeni rendelkezésre állásuk:

A PEGAconsult Kft. az üzemeltetési feladatok ellátásához 7x24 órában HelpDesk-et biztosít az alábbi elérhetőségekkel:

- Telefon: +36 20 402-4020
- E-mail: support@pega.hu

A HelpDesk alábbi csoportokat és személyi összetevőket foglalja magában:

- Elsőszintű támogatók (7x24 órás) 5 fő
- Második szintű támogatók
  - Rendszerüzemeltetési szakértők 3 fő
  - Alkalmazásüzemeltetési szakértők 3 fő
- Harmad szintű támogatók
  - Apache+PHP specialista 2 fő
  - IBM HW specialista 2 fő
  - Postgres DBA specialista 2 fő
  - Linux és VMWare specialista 2 fő