2/2010. sz. Gazdasági Főigazgatói Utasítás a PTE belső hálózatának eléréséről

1. Dokumentum adatlap

Azonosítás	
Dokumentum címe	2/2010. sz. Gazdasági Főigazgatói Utasítás a PTE belső hálózatának eléréséről
Állomány neve	Belso_halozat_utasitas.docx
Dokumentum verzió	1.0
Kiadás időpontja	2010.03.31.
Hatályba lépés időpontja	2010.03.31.
Készítette	Ripli Péter
Ellenőrizte	Vukovics Mihály, Hetesi Zoltán, Uherkovich Péter, Vránics Tamás
Jóváhagyta (IIG)	Sári Csaba

2. Tartalomjegyzék

3. Célkitűzés

A Pécsi Tudományegyetem Gazdasági Főigazgatóságához és Klinikai Központjához tartozó szervezeti egységekkel (továbbiakban GF, KK) szerződéses viszonyban álló külsős partner cégek munkatársai és az egyetemi közalkalmazottak (akik munkavégzéséhez elengedhetetlen a távoli hozzáférés megléte) részére a távoli munkavégzés lehetőségének megteremtése a lehető legmagasabb biztonsági szint megtartása mellett, a legkedvezőbb költségtényezőkkel.

A távoli hozzáférés komoly informatikai biztonsági kockázatot jelent, melyet minden rendelkezésre álló eszköz felhasználásával minimalizálni kell.

Az utasítás tartalmazza a VPN végpontok

- engedélyezési, létesítési, nyilvántartási és ellenőrzési eljárásainak,
- valamint a használatra és a működtetésre vonatkozó előírásoknak a részletes szabályozását.

Az alapelvek és szabályok figyelmen kívül hagyása miatt bekövetkező szándékos (és) vagy nem szándékos károkozás miatt a munkatárs munkajogi a külsős partner szerződésszegési felelősséggel tartozik.

4. Az utasítás hatálya

4.1. Szervezeti hatály

A jelen utasítás szervezeti hatálya kiterjed a PTE GF és KK szervezeti egységeire.

4.2. Személyi hatály

Jelen utasítás hatálya kiterjed a PTE Gazdasági Főigazgatóság Informatikai Igazgatósága (IIG) által üzemeltetett VPN rendszerek felhasználóira. Az utasításban foglaltakat minden esetben be kell tartani VPN rendszer bármely funkciójának használatakor. Az utasításban foglalt elveket érvényesíteni kell a PTE-vel szerződéses kapcsolatban álló cégek és személyek körére is.

Az utasítás nem vonatkozik a karok, intézmények által önállóan üzemeltetett VPN rendszerekre.

5. Fogalmak, meghatározások

5.1. A távmunka meghatározása

Távmunkának nevezünk minden olyan tevékenységet, mellyel a GF és a KK munkatársai vagy külső szerződéses partnerek, egy külső hálózatról elérik a belső informatikai rendszert, és az eléréshez nem az egyetem által üzemeltetett adatátviteli médiát használják. A továbbiakban a távmunkát VPN elérésnek, VPN rendszernek is nevezzük.

A VPN valójában egy magánhálózati csatorna a publikus hálózati infrastruktúrán, azaz az Interneten. Az Internethez történő kapcsolat fizikailag tetszőleges lehet (jellemzően ADSL, KábelNet, GPRS stb.).

5.2. Az informatikai biztonság alapfogalmai

- Adatbiztonság: Adatbiztonságon az adatok és megfelelő megjelenítésüket végző alkalmazások sértetlenségének, bizalmasságának és rendelkezésre állásának megfelelő színvonalú biztosítását értjük.
- Informatikai biztonsági kockázat: Az informatikai biztonsági kockázat arányos az informatikai rendszer elemeit képező értékek (adatok, eszközök) sérülésének mértékével és a sérülés valószínűségével.
- Bizalmasság: Azon követelmény, amely meghatározza azt a kört, akik számára az adott információ megismerhető. Az információt védeni kell a jogosulatlan hozzáféréstől vagy közzétételtől.
- Sértetlenség: Az információ pontosságára, teljességére, valamint érvényességére vonatkozik az üzleti értékeknek és várakozásoknak megfelelően. Az információs sértetlenségének nem teljesülését jogosulatlan hozzáférésből eredő szándékos módosítás vagy az információ véletlen sérülése okozhatja.
- Elszámoltathatóság: Minden tevékenységet egyértelműen hozzá kell rendelni az adott tevékenység végrehajtójához, így a végrehajtó személy felelős azaz elszámoltatható az elvégzett tevékenységért.
- Letagadhatatlanság: Követelmény, hogy a felhasználók egy későbbi időpontban ne tudják, valamilyen okból önkényesen megtagadni az előzőekben általuk végrehajtott tranzakciót.

5.3. Felelősségi körök

A tevékenység központi irányítását az Adatbiztonság Felelős látja el.

Az Informatika Igazgatóság Infrastruktúra Üzemeltetési Osztály (IÜO) osztályvezetője felelős:

- A VPN rendszer folyamatos rendelkezésre állásáért.
- A VPN rendszer üzemeltetés és használat rendszeres független felülvizsgálatának biztosításáért.

Az Adatbiztonság Felelős feladatai:

- A biztonsági események kivizsgálása és az esemény kapcsán felmerült problémák elhárítása az IÜO közreműködésével;
- A VPN rendszer biztonsági szolgáltatásai és a PTE informatikai biztonsági követelményeinek összehangolása.

A ServiceDesk (SD) Osztály osztályvezetője felelős:

- A VPN igénylések és megszüntetések szabályszerű lebonyolításáért,
- A VPN jogosultságok beállításával kapcsolatos teendők adminisztrálásáért.

A VPN felhasználó felelős:

- A biztonsági szabályok mindenkori betartásáért.
- A biztonsági incidensek jelentéséért.

A munkautasítás betartatása az érintett szervezeti egység vezetőjének a feladata. A munkautasítás minden VPN felhasználóra kötelező érvényű.

Minden, jelen dokumentum hatálya alá tartozó tiltott tevékenység kivizsgálásra kerül, és annak mértékétől függően fegyelmi eljárást von maga után.

6. Az utasítás tartalma

6.1. VPN kapcsolat létesítése és megszüntetése

A felhasználók kötelezettsége minden körülmények között a kapcsolat igénylési megszüntetési és a használati biztonsági szabályok betartása.

6.1.1. **Létesítés**

VPN kapcsolat létesítésére csak az a személy jogosult, akinek igényét az Informatikai Igazgató (vagy az Adatbiztonság Felelős) jóváhagyta, és a távmunkával kapcsolatos felhasználói utasítást tudomásul vette, elfogadta, és azt aláírásával igazolta. A VPN kapcsolat létesítésére vonatkozó igényt a http://www.iig.pte.hu oldalon a „VPN hozzáférés igénylés" webes formanyomtatványon kell bejelenteni. Segítség a ServiceDesk Osztályon kérhető (sd@pte.hu Tel.: 6006)

Az igénylés teljesítése kizárólag abban az esetben történhet meg amennyiben az egyetemi alkalmazott szervezeti egységének a vezetője vagy a külső partner cég alkalmazottjának az erre jogosult felettese az igénylési formanyomtatványt aláírta.

A jóváhagyást követően, az IÜO elvégzi a kliens oldali és konfigurációs beállításokat (melyeken ezt követően változtatni szigorúan tilos).

6.1.2. **Megszüntetés**

A VPN kapcsolat megszűntetésére vonatkozó igényt a ServiceDesk Osztályon keresztül kell bejelenteni.

- Kilépés esetén
  A felhasználó munkaviszonyának megszűnése esetén minden VPN rendszerrel kapcsolatos jogosultsága megszűnik a PTE informatikai jogosultságainak megszüntetésével egy időben.
- Áthelyezés esetén
  Amennyiben a felhasználót más munkakörbe helyezik, minden esetben meg kell vizsgálni azt, hogy szükséges-e a VPN használat lehetőségét továbbra is fenntartani. Amennyiben ez kétséges, azt az adott osztályvezető, szervezeti egység vezető és az IIG ServiceDesk osztály tudomására kell hozni.
- Biztonsági incidens esetén
- Amennyiben a felhasználó hibájából következik be a PTE IT rendszereit súlyosan fenyegető biztonsági incidens, a VPN kapcsolat megszüntetésre kerül.

6.2. A VPN használata, használatának körülményei

- A PTE által biztosított VPN rendszert csak munkavégzés céljából, a felhasználó feladatkörében foglalt tevékenységek elvégzése során lehet felhasználni. Az ettől eltérő felhasználás szigorúan tilos!
- A PTE által biztosított VPN kliens munkaállomást a felhasználó más személynek semmilyen formában nem engedheti át!
- Naplózás: A felhasználók minden tevékenysége naplózva lesz és szükség esetén visszakereshető. Jelen utasítás be nem tartásából eredő károkért a PTE a felhasználót teszi felelőssé. Ilyen esetben az eseményt tartalmazó naplóállomány bizonyító erejű. A VPN rendszer használatával kapcsolatos kérdésekben a VPN szolgáltatás gazdája nyújt segítséget.
- A felhasználók rendelkezésére bocsátott VPN felhasználói utasítást minden felhasználónak meg kell ismernie.
- A VPN kliensprogram beállításait a felhasználó semmilyen módon és semmilyen esetben nem változtathatja meg! A program beállításait csak a VPN service owner módosíthatja, illetve írásbeli felhatalmazásuk birtokában az erre kijelölt személyek.
- Minden esetben zárolni kell a munkaállomást, ha a felhasználó – akár rövid időre is – elhagyja a munkaállomást, mert ellenkező esetben illetéktelenek bizalmas adatokhoz férhetnek hozzá a PTE informatikai rendszerében.

6.2.1. Felhasználó hozzáférés, azonosítás működése

6.2.1.1. Kapcsolódás a rendszerhez

A felhasználók azonosítása két lépésben történik, melyből az első önműködően történik:

- Először a felhasználónak a szolgáltató Internet hálózatához kell kapcsolódnia.
- Amennyiben az Internet kapcsolat sikeresen felépült, megkezdődhet a PTE rendszeréhez történő kapcsolódás. A felhasználói név és jelszó megegyezik a PTE belső hálózatában használt - ún. Active Directory címtárban érvényesen tárolt – névvel, jelszóval (ETR kód).

6.2.1.2. Jelszókezelés

- A VPN rendszer alkalmazásához szükséges jelszót a felhasználónak szigorúan bizalmasan kell kezelnie.
  - A jelszót tilos másokkal közölni!
  - A jelszót tilos bárhova leírni!
- A bejelentkezésnél nem javasolt a "Jelszómentés" funkciót használni!
- A felhasználói jelszó elfelejtése biztonsági incidensnek minősül, amelyről értesíteni kell a ServiceDesk osztályt. sd@pte.hu Tel.:6006
- Ha a felhasználói jelszó illetéktelen személy tudomására jut, az súlyos biztonsági incidensnek minősül. Haladéktalanul értesíteni kell a ServiceDesk osztályt, amely intézkedik a VPN kapcsolat letiltásáról, majd új felhasználói hozzáférés létrehozásáról. A VPN rendszer tulajdonosa ilyen esetben kivizsgálja, hogy milyen módon jutott a jelszó illetéktelenekhez.
- Abban az esetben, ha a felhasználó jelszava lejár (azaz eléri az érvényességi idő végét) nem lehet távolról bejelentkezni a VPN rendszerbe. A felhasználónak gondoskodnia kell arról, hogy a jelszó lejárta előtt, az egyetem belső hálózatában, a rendszerbe belépve a jelszót megváltoztassa, vagy fel kell vennie a kapcsolatot a ServiceDesk szolgálattal, amely intézkedik az új jelszó generálásáról. sd@pte.hu Tel.:6006
- Új jelszó csak a jelszókezelési eljárásnak megfelelően adható.

6.2.1.3. Sértetlenség, Elszámoltathatóság

Az Internet felöli támadások ellen a VPN kliensbe épített személyes tűzfal ad védelmet. A személyes tűzfal használatát a VPN rendszer kikényszeríti VPN kapcsolat felépítése során, annak érdekében, hogy ez a funkció véletlen vagy szándékos módosítását a felhasználó ne tudja megtenni.

Az elszámoltathatóság biztonsági feltétele érdekében a következő tevékenységek naplózása történik meg:

- VPN felhasználó ki/bejelentkezése
- VPN felhasználó által forgalmazott adatmennyiség
- VPN adminisztrátor ki/bejelentkezés
- VPN konfigurációs módosítás
- Szűrési feltétel megsértése

6.2.2. Vírusvédelem

Valamennyi kliens vírusvédelmi rendszerrel rendelkezik, melyet kikapcsolni tilos. Ennek beállításáról az IÜO köteles gondoskodni.

6.3. VPN felhasználók csoportosítása, hozzáférési alternatívák

A VPN kapcsolaton keresztül megvalósuló hálózati hozzáférés lehetséges szintjeit a biztonsági szempontok figyelembevételével az Adatbiztonság felelős és az IÜO Osztályvezető határozza meg és rögzíti. Az illetékes jóváhagyó – a szolgáltatás megrendelésekor - ezen csoportokba sorolhatja dolgozóit.

A csoportok ismérvei

- Várható felhasználási idő

- Elérhető belső informatikai szolgáltatások köre (pl. SAP; e-Medsol ; MS file service)

A felhasználó kötelességei a használni kívánt rendszereket illetően azonosak az egyedi rendszer leírásoknál található felhasználói utasításokkal.

6.3.1. **Besorolás biztonság alapján**

Távmunkában működő PTE tulajdonú gépen kizárólag olyan operációs rendszer futatható, amelynek minden paramétere megegyezik az irodai környezetben megszokottal, környezeti beállítások, szolgáltatások. Biztonsági incidensek esetén egyes szolgáltatások és elérések időlegesen, de indokolt esetben véglegesen tiltásra kerülnek.

Nem PTE tulajdonú gépen a felhasználó dönthet, arról, hogy engedi-e az egyetem Windows Platform policy beállításait érvényesíteni a gépén vagy sem. Ha igen, akkor az elérhető szolgáltatási kör megegyezik a PTE tulajdonú gépekével, ha nem, akkor kizárólag az egyetemi e-mail levelezés szolgáltatás elérését tudjuk számára biztosítani.

6.4. Rendelkezésre állás, elérhetőség

A VPN rendszer rendelkezésre állását, elérhetőségét a rendszer központi elemei és az elérési hálózat rendelkezésre állása határozza meg. Elérési hálózat alatt a szolgáltató Internet kapcsolatát értjük, melynek rendelkezésre állását szerződés garantálja a felhasználó részére.

A rendszer egyéb, IIG-IÜO által üzemeltetett része 7*24-ben üzemeltetői-ServiceDesk, munkanapokon 08-17-ig pedig service owner felügyelet mellett érhető el.

6.5. Internet használat

A megfelelő jogosultsággal rendelkező felhasználók távoli VPN kliens munkaállomásukról is elérhetik a nyilvános Internet hálózatot az egyetemi tűzfalon keresztül.

6.6. Biztonsági incidensek

Biztonsági incidensek azok az események, amelyek során sérülnek a biztonsági követelmények (bizalmasság, sértetlenség, rendelkezésre állás).

Abban az esetben, ha a felhasználó tudomására jut, hogy:

- Kitudódott a jelszava,
- Elfelejtette a jelszavát,
- Rajta kívül más, illetéktelen személy használta a VPN kapcsolatot az ő nevében,
- Vírusfertőzés történt a kliens gépen,
- Hacker támadás érte,
- Számítógépét, vagy annak valamely komponensét eltulajdonították,
- Rendellenes működést tapasztal a VPN használata során
- Bármely más esemény történt, amely sérti a biztonsági követelményeket, a következőket kell tennie:
- Azonnal le kell állítani a VPN kapcsolatot, és ki kell kapcsolni a gépet, hogy az adatok rendelkezésre álljanak az incidens kivizsgálás esetén
- Értesíteni kell a ServiceDesk szolgálatot a bekövetkezett eseményről. Súlyos biztonsági incidens esetén ők értesítik a VPN service ownert.
- Követni kell a ServiceDesk szolgálat utasításait.

Biztonsági incidens után csak abban az esetben vehető használatba újra a VPN kliens, ha a VPN service owner azt engedélyezte.

6.7. Következmények

Minden, jelen dokumentumban részletezett és tiltott tevékenység kivizsgálásra kerül, és annak mértékétől függően fegyelmi eljárást von maga után.

7. Nyilatkozat

Az utasításban leírtakat elolvastam, megértettem és kötelező érvényűnek tekintem. Tudomásul veszem, hogy a fentiek be nem tartása fegyelmi eljárást (vagy szerződésszegést – külső partner esetén) vonhat maga után.

Pécs, ...

.....

Aláírás

Felhasználó neve:.....

Lakcíme:.....