6/2011. SZ. GF ÜGYVITELI UTASÍTÁS A PTE SZERVER SZOBÁINAK ÉS TELEFONKÖZPONT HELYISÉGEINEK BELÉPTETŐ RENDSZERÉRŐL

I. ÁLTALÁNOS RENDELKEZÉSEK

AZ UTASÍTÁS CÉLJA

1.§.(1) Az utasítás célja a PTE-, elsősorban informatikai munkatársai részére biztosítani a géptermi belépésre is feljogosító RFID beléptető kártyák és PIN kódok ügyviteli - informatikai szabályozását.

AZ UTASÍTÁS HATÁLYA

2.§.(1) Az utasítás tárgyi hatálya kiterjed a PTE által üzemeltetett és fenntartott szerverszobákra, géptermekre.

(2) Az utasítás személyi hatálya kiterjed a PTE minden közalkalmazottjára, hallgatójára, oktatójára és külső partnereire, akik bármelyik PTE tulajdonú szerverterembe lépnek.

II. FOGALMAK, ÉRTELMEZÉSEK

3.§.(1) A PTE épületeiben a 2010-es évben RFID-kártyás munkaidő regisztrációs, és hozzáférés szabályozó rendszer került bevezetésre a Szántó Kovács János u. 1/b. és a Honvéd u. 5. telephelyeken a Gazdasági Főigazgatósághoz tartozó munkatársak részére.

(2) A munkaidő regisztrációhoz használatos RFID kártyák sokoldalúan felhasználhatóak. Ebből adódóan azok a (elsősorban informatikai tevékenységet végző) munkatársak, akiknek a munkaköre kapcsán szükséges a szerverszobákba, géptermekbe, telefonközponti helyiségekbe rendszeres időközönként belépni, a megfelelő jogosultságok kiosztása után egy azonosító kártyával (és a hozzá tartozó pin kóddal) megtehetik ezt az érintett helyiségekbe.

III. HOZZÁFÉRÉSI JOGOSULTSÁGOK KIOSZTÁSA

KÖZALKALMAZOTTI JOGVISZONYBAN LÉVŐK RÉSZÉRE

4.§.(1) A PTE-n a géptermi „beléptető kártya" és PIN kód kombinációjának a használata elsősorban az informatikai munkakörökben dolgozó munkavállalók és a portaszolgálat/épületfelügyelet munkatársai részére érhető el a Szántó K. J. u.-i, a Honvéd u.-i, a 400 ágyas klinika és az Akác u.-i klinikai tömb telephelyeken. A kártyák rendszerhez illesztése, visszavonása és a jogosultsági szintek szabályozása és karbantartása az Adatbiztonság Felelős feladata.

HOZZÁFÉRÉSI JOGOSULTSÁG IGÉNYLÉSÉNEK MENETE

5.§.(1) A géptermi belépésre jogosító hozzáférés igénylését a felhasználó a ServiceDesk Osztályánál (sd@pte.hu) kezdeményezheti az erre rendszeresített edocs (http://edocstest.pte.hu/kitolt/szerverszoba_belepo) formanyomtatványon. Amennyiben a jogosultságot az Informatikai Igazgató jóváhagyja, az Adatbiztonság Felelős elvégzi a dolgozó RFID kártyájának a rendszerhez való hozzáadását és a szükséges PIN kód beállítását. Ezen jogosultságokat min. évente felül kell vizsgálni auditálás céljából. A felülvizsgálat elvégzése vagy elvégeztetése az Adatbiztonság Felelős feladata.

KÜLSŐ PARTNEREK RÉSZÉRE

6.§.(1) Abban az esetben, amikor egy külső partner képviselője (Magyar Telekom, NIIF, villanyszerelő, stb.) az előre tervezhető feladatainak az ellátása miatt szeretne bejutni egy egyetemi tulajdonú gépterembe a következő eljárást kell alkalmazni.

a) A külső partner képviselője az igényét legalább két nappal előtte jelzi az SD-n (sd@pte.hu, 72/536-006), a pontos dátum megjelölésével és az adott napon belül megjelöl egy egy órás intervallumot.
b) Az SD továbbítja az igényt a hálózatos és a windows csoport felé.

c) A két csoport visszajelzésétől függően az SD értesítést küld a külső partner részére a kért időponttal kapcsolatban, elfogadva azt vagy új időpontot ajánl fel.
d) A külső partner a megjelölt időpontban köteles pontosan érkezni és az engedélyezett, rendelkezésre álló idő lejáratakor a munkaterületet elhagyni.

(2) Amennyiben előre láthatóan több mint egy órás munkát kell elvégezni, akkor legalább négy nappal előre kell a bejutási igényt jelezni annak érdekében, hogy az IIG tudjon szabad munkatársat biztosítani, adott esetben a túlórát megszervezni. Sürgős esetben, és meghibásodás esetén a bejutási szándékot ennek feltüntetésével kell az SD-n jelezni, aki ebben az esetben 1 órán belül köteles visszajelzést küldeni arról, hogy megoldható-e a bejutás. Munkaidőben az SD sürgős prioritással egyeztet az illetékes csoportok tagjaival, munkaidőn túl az ügyeletesekkel a bejutás megszervezése érdekében A külső partnerek figyelmét az SD köteles felhívni az előre egyeztetett időpontok betartására. A megjelölt időn túl, és a felügyelet nélkül a gépteremben külső partner megbízottja nem tartózkodhat.
(3) Vendégkártya vagy látogató kártyák kiadása: használata jelenleg nem támogatott.

A RIASZTÓ RENDSZER HASZNÁLATA A GÉPTERMEKBEN

7.§.(1) A riasztórendszer kezelőjét használva minden gépteremi belépésre jogosult személy a saját PIN-jét alkalmazva léphet be a géptermi helyiségekbe. Ezek alapján minden jogosultnak szükséges elsajátítani a riasztórendszer aktiválási és deaktiválási folyamatát.

ÁLTALÁNOS HASZNÁLAT (SZÁNTÓ K. J. 1. 2. EM.)

8.§.(1) Mivel a gépteremben folyamatos tartózkodás, munkavégzés nincs, és a gépterem a többi irodai helyiségtől elkülönülten lett kialakítva, ezért minden nappali munkavégzéskor az egyes gépteremből való távozáskor a rendszeradminisztrátor vagy operátor köteles aktiválni a rendszert.

(2) Az aktiválás után, természetesen előfordulhat esti munkavégzés, melynek befejeztével a munkát végző személy felelőssége a riasztórendszer aktiválása.

ÁLTALÁNOS HASZNÁLAT (400 ÁGYAS)

9.§.(1) Mivel folyamatos munkavégzés a 400 ágyas klinika gépteremben nem történik, így az ott munkát végző személy felelőssége a géptermi riasztórendszer aktiválása és deaktiválása.

ÁLTALÁNOS HASZNÁLAT (HONVÉD U. 1.)

10.§.(1) Mivel folyamatos munkavégzés a gépteremben nem történik, így az ott munkát végző személy felelőssége a géptermi riasztórendszer aktiválása és deaktiválása.

ÁLTALÁNOS HASZNÁLAT (AKÁC U.)

11.§.(1) Mivel folyamatos munkavégzés a gépteremben nem történik, így az ott munkát végző személy felelőssége a géptermi riasztórendszer aktiválása és deaktiválása.

TEENDŐ RIASZTÁS ÉS INCIDENS ESETÉN (SZÁNTÓ, HONVÉD U. 1. ÉS 400 ÁGYAS)

12.§.(1) Minden épületben a géptermi helyiségekbe a rendszer behatolás esetén riasztást végez, ebben az esetben a létesítmény felelős és a külsős felügyeleti partner [LDSZ Kft.] feladata a riasztás körülményeinek kivizsgálása. Első esetben azokban a helyiségekben amelyekben fel van szerelve kamera, a megfigyelő kamerákkal kell a helyiségeket ellenőrizni. Amennyiben a kamerákkal semmi szokatlan nem tapasztalható az informatika vagy az épületfelügyelet munkatársai a géptermi ajtó mellett elhelyezett konzolon a riasztást megszüntetik a saját kódjukkal.

MONITOROZÁS

13.§.(1) A rendszer minden eseményt naplóz, így mindig látszik, hogy ki aktiválta, illetve ki deaktiválta a riasztót. A riasztórendszer valamint a beléptető rendszer riportjai alapján, havi rendszerességgel ellenőrizzük, hogy a belépő személyek gondosan jártak-e el a riasztórendszer használatával kapcsolatban.

SZERVERSZOBÁK, GÉPTERMEK, TELEFONKÖZPONTI HELYISÉGEK BIZTONSÁGA

14.§.(1) A szerverszobák, géptermek, és telefonközponti helyiségek és az ott található informatikai eszközök biztonságának szavatolása érdekében a szerverszobák, géptermek teljes körű felügyeletét az informatikai munkatársak, az adatbiztonság felelős és az épületfelügyelet munkatársai látják el.

(2) A szerverszobába való belépést a beléptető rendszer automatikusan naplózza. A látogatói belépés csak és kizárólag belépési jogosultsággal rendelkező személy kíséretével lehetséges. A szerverszobában való tartózkodást kamera rögzíti. Ahol a kamerás védelem még nem megoldott ott legkésőbb a 2012. gazdálkodási évben a fejlesztést meg kell valósítani.

(3) A szerverszobák, géptermek igénybevételének jogosultsága az üzemeltetőkre, illetve a szerződéses viszonyban álló külső személyekre terjed ki. A jogosultságot az Informatikai Adatbiztonság Felelős határozza meg.

IV. A SZERVERSZOBÁKBAN TALÁLHATÓ KAMERÁKKAL KAPCSOLATOS ELŐÍRÁSOK

15.§.(1) Hogyan figyelheti kamerán keresztül a géptermet illetve a gépteremben dolgozókat a munkáltató?

A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény 3. § (1) bekezdése értelmében személyes adat akkor kezelhető, ha ahhoz az érintett személy hozzájárult, vagy ha azt törvény elrendelte.

A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvényt (a továbbiakban: Vtv.) 26. és 28. §-ai felhatalmazást adnak a törvény hatálya alá tartozó személy- és vagyonőr számára arra, hogy magánterületen – ideértve annak a közönség számára nyilvános részeit is – elektronikus megfigyelő rendszert alkalmazzon. A megfigyelés és rögzítés akkor jogszerű, ha ahhoz az érintett kifejezetten hozzájárult. A hozzájárulás megadható azzal is, ha az érintett a megfigyelt területre a megfelelően elhelyezett ismertetés ellenére bemegy, kivéve, ha a körülményekből egyértelműen más következik (Vtv. 30. § (1)-(3) bek.). Az ismertetés tartalmi elemeit a Vtv. 28. § (2) bekezdése állapítja meg. A rögzített felvételeket a törvény alapján három munkanapig lehet tárolni.

A kamerák felállításáról előzetesen tájékoztatni kell a dolgozókat, e tájékoztatásnak arra is ki kell terjednie, rögzítik-e és tárolják-e a kamerák által felvett képet, és ha igen, milyen célból. Kamerát használni csak meghatározott célból lehet, a céltól eltérő felhasználás jogellenes. Az érintetteknek joguk van megtekinteni a róluk készült felvételeket, és kérhetik azok törlését is.

E rendelkezésekkel kapcsolatban hangsúlyozandó, hogy nem teremtenek jogalapot arra, hogy a munkáltató a kamerák használatával ellenőrizze a munkavállalói munkahelyi magatartását, munkavégzését.

A rögzítés nélküli kamerás megfigyelés is adatkezelésnek minősül.

Cél a proaktív szemlélet megvalósulása révén a jogsértések és a biztonsági incidensek megelőzése, a vagyonvédelem megvalósítása.

A RÖGZÍTETT FELVÉTELEK MEGŐRZÉSE

16.§.(1) [Vagyonvédelmi Törvény: 2005.évi CXXXIII. törvény.]

A rögzített felvételeket a törvény alapján három munkanapig lehet tárolni.

A felvétel tárolásával nő annak is a veszélye, hogy a felvételt manipulálják, maga a felvétel illetve az abban szereplő személyes információk illetéktelenek tudomására jutnak. A felvételek indokolatlan tárolása ellentétes az adatkezelés célhoz kötöttségének alkotmányos elvével, hiszen egyfajta készletre tárolást jelent.

A kamera felvételeinek rögzítéséhez, tárolásához egy önálló berendezésre van szükség. A digitális tárolásra pedig kétféle lehetőségünk van.

Akár egy számítógép merevlemeze is alkalmas a célra, ám mindenképpen egy erős gépre, illetve egy digitalizáló kártyára van szükség. Bár a hatályos jogszabályok szerint maximum három napig őrizhetjük a felvételeket (lásd Vagyonvédelmi Törvény: 2005.évi CXXXIII. törvény), egy ötszáz gigabájtos merevlemezen több hétnyi anyagot tárolhatunk. A rögzítés folyamatos, ha a háttértároló megtelik, a program mindig a legrégebbi felvételeket törli.

A számítógépes tárolás mellett a másik lehetőség egy asztali rögzítő, az úgynevezett DVR, ami úgy néz ki, mint egy DVD-lejátszó, csak merevlemez van benne.

Természetesen nem szükséges a felvételek minden egyes kockáját megőrizni, elég, ha csak az eseményeket rögzíti számunkra a rendszer. Ez egy programmal oldható meg, ami a fény-tartalomváltozást figyeli, és csak azokat a felvételeket őrzi meg, melyeken mozgást „lát". Az érzékenységet, hogy milyen pixelelváltozásra reagáljon, be is lehet állítani.
Mozgásérzékelő felvétel esetén támaszkodhatunk a kamera beépített mozgásérzékelő mechanizmusára.

A riasztásra történő felvétel a külső érzékelővel is ellátható kamera által küldött riasztási jelre indul el. Amikor az IP kamera a digitális bemenetén megkapja a vezérlő jelet a külső szenzortól, jelet küld a DiskStation-nek is, hogy kezdje meg a felvételt.

NAPLÓ

17.§.(1) Kritikus események, mint például a kamera szétkapcsolása vagy a kamerabeállítások változtatása, naplókban kerülnek rögzítésre. A naplókat megtekinthetjük, és kézileg törölhetjük/menthetjük őket attól függően, hogy a jövőben is igényt tartunk-e rájuk. Amikor a naplóméret eléri a határát, a legrégebbi naplóbejegyzés helytakarékosság okán törlésre kerül.

A RÖGZÍTETT FELVÉTELEKHEZ TÖRTÉNŐ HOZZÁFÉRÉS SZABÁLYOZÁSA

18.§.(1) Jelszóval védve több szinten.

BIZTONSÁGI ADATMENTÉSEK

19.§.(1) Lokális biztonsági adatmentés.
Az adatbázis szerver napi és heti mentést készít, amelyet saját meghajtóin tárol. Sikertelen mentési kísérlet esetén, elektronikus úton azonnal értesítésre kerül a felelős service owner.
(2) Központi biztonsági adatmentés
A mentési központba történő mentések az adatforgalom csökkentése érdekében inkrementális vagy differenciális mentéssel kerülnek megvalósításra amennyiben ezt az adatbázis mérete indokolja. Sikertelen mentési kísérlet esetén a mentést meg kell ismételni vagy az új állománnyal együttesen kell menteni.

V. ZÁRÓ RENDELKEZÉSEK

HATÁLYBA LÉPÉS

20.§.(1) Az utasítás 2011. november 11. napján lép hatályba.
(2) Az utasítás szakmai tartalmáért (előkészítéséért, előterjesztéséért, aktualizálásáért, és évenkénti felülvizsgálatáért) az Informatikai Igazgatóság vezetője felelős.
(3) A végrehajtással kapcsolatban további tájékoztatást nyújt, illetve az utasítás előírásai betartásának ellenőrzéséért felelős az Informatikai Igazgatóság.

Dátum, 2011. november 09.

PÉCSI TUDOMÁNYEGYETEM GAZDASÁGI FŐIGAZGATÓ 6.

Krutki Józsefné dr.
gazdasági főigazgató