Rukon Kft. 1125 Budapest
Szarvas Gábor u. 29.

Informatikai adatvédelmi szabályzat

2018.05.01
Verzió 3.0

Készítette:

Becsei Sándor
Informatikai vezető

Tartalomjegyzék

Illetéktelen felhasználás elleni védelem

Az informatikai szervezet és a felhasználók kötelesek, minden rendelkezésre álló, eszközzel védeni az informatikai feldolgozás során írásos vagy elektronikus formában keletkezett adatokat a belső és idegen illetéktelen felhasználás ellen.

Önálló számítógépek és hálózatba kötött munkaállomások esetén egyaránt a hardver és a szoftver minden lehetőségét ki kell használni a védelemre (indítási hardver jelszó, bejelentkezési azonosító és jelszó, képernyővédő és annak jelszavas védelme stb.).

- Az indítási hardware jelszó szervezeti egységenként, egy telephelyen belül lehet egységes, de telephelyenként különböző kell legyen. Az indítási hardware jelszót csak különlegesen védendő információtartalmú felhasználói gépeken alkalmazzuk.
- Az informatika vállalati általános operációs rendszer szintű rendszergazdai jelszóval rendelkezik, melyet kéthavi sűrűséggel módosítani kell. Ezt csak az informatikai rendszer dolgozói ismerhetik, és csak a rendszergazdai feladatok ellátásához használhatják.
- Az operációs rendszer szintű felhasználói jelszavakat legkésőbb havonta módosíttatni kell a felhasználóval. Ezt az operációs rendszerből automatizálva oldjuk meg.
- Az egyes jelszóval védett alkalmazásokban a felhasználói jelszavak módosítása ugyancsak havonta szükséges. Ezt a lokális és hálózatos alkalmazásoknál egyaránt az alkalmazásban automatizálva állítjuk be.
- Jelszavas képernyővédőket kell alkalmazni minden NT operációs rendszert futtató számítógépen. A képernyővédő késleltetését annyi percre állítjuk be, hogy a felhasználót a tevékenységében különösebben ne zavarja, de már a kisebb távolmaradások alatt is a rendszer a felhasználó aktuális bejelentkezésére nézve zárt maradjon. A beállítandó késleltetés alkalmazásfüggő.
- A hozzáférés korlátozása az informatikai szervezetre is vonatkozik. Az informatikai szervezet rendszergazdái csak olyan jogosultságot kaphatnak, amivel a rendszergazdai feladatokat elláthatják. A jelszóval védett alkalmazásokon belül semmilyen operátori jogosultságot nem kaphatnak, hacsak a közvetlen mindennapi feladatok (hibák javításában történő közreműködés pld.) ezt meg nem követelik. Ilyenkor az adott felhasználói szervezet vezetője engedélyéhezi a jogosultság kiadását az informatikai vezető írásos javaslatára. A kiadott jogosultság személyre szóló, azonosítható, a rendszer által naplózható kulcsfelhasználói szintű jogosultság lehet.
- A felhasználók a szervereken futó alkalmazásokhoz, egyéb adatokhoz való jogosultságát, aktuális jogosultsági szintjeit az informatikai vezető a dolgozó munkahelyi vezetőjével konzultálva állapítja meg. A jogosultság kiadása csak írásos engedély alapján történhet, amely tartalmazza a kapott jogosultsági profilokat, a profil rövid leírását, időpontokat, megkötéseket. Az engedélyt a munkahelyi vezető és a jog kiosztása után az informatikai vezető aláírja. Minden jogosultságokban bekövetkezett változás a fenti eljárás szerint lehetséges. A jogosultságok kiadásához a fenti módon elkészített dokumentum a jogosultság adminisztrációs lap, melynek formai és tartalmi követelményeit az 1. számú melléklet tartalmazza.

  Az adatbázisok tartalmán kívül eső védendő adatokat lehetőség szerint a szervereken kell tárolni a megfelelő védelem és a mentések lehetőségei miatt. Ezeket az adatokat, valamint a szervereken tárolt felhasználói file-okat a szokásos rendszerességgel menteni kell. Ezért a mentésért az informatika felel.

A PC saját lemezein vagy hajlékony mágneslemezen tárolt adatok esetében a védelem a felhasználó (adattulajdonos) felelősségi körébe tartozik, amennyiben megfelelő védelmi és mentési eszközökkel rendelkezik. Erről a tényről, továbbá a feltételek meglétéről a felhasználót a használatbavételi jegyzőkönyvben értesíti az informatika. A tudomásulvételt a felhasználó aláírásával igazolja.

Minden külső hálózathoz való csatlakozás (pl. Internet) csak a következő esetben megengedett:

- nem hálózati munkaállomásról van szó
- (Alapértelmezésben, csak olyan munkaállomásról tesszük elérhetővé a külső hálózatokat, mely munkaállomás egyáltalában nem, még időlegesen sem csatlakoztatott a Rukon Kft. informatikai hálózatába.)

- hálózati munkaállomás vagy szerver esetében, csak egy szerződésben rögzített support tevékenység ellátása érdekében engedélyezhető a csatlakozás, mely csatlakozási pont az elérhető szoftver és hardver lehetőségekkel (pl. " tűzfal " PC, hatékony hozzáférési rendszer) az illetéktelen behatolás ellen védhető

- a fenti esetekben is csak az informatikai vezető írásos engedélyével

- az engedélyeket az informatikai vezető félévente felülvizsgálja

A jelszavakat az informatikai szervezet egy erre a célra rendszeresített tűzálló páncélkazettában tárolja, téma szerint felcímzett borítékban lezárva. A kazetta az informatikai vezető irodájában van. Kulcsa a kulcstartó páncéldobozban az informatika irodájában található. A páncéldobozhoz kulcsa az informatikai vezetőt éppen helyettesítő rendszergazdánál található. A jelszavas boríték felbontásáról dokumentumot kell készíteni, az azt felbontó aláírásával, részletesen leírva a felbontás okát.

Személyes adatok felhasználása

A Rukon Kft. által használt személyes adatok:

Tárolt adatok, adatfelhasználás célja: Kapcsolattartás a partnerekkel:

Felhasznált adatok

- Név
- Email cím (amennyiben vállalati email cím nem elérhető)
- Telefonszám (amennyiben nincs vállalati telefonszám)

Tárolás módja: Rukon Kft munkatársai egyénileg tárolják ezeket az adatokat, saját eszközeiken a mentésükről egyénileg gondoskodnak.

Ideiglenesen tárolt és kezelt személyes adatok:

A Rukon Kft. a tachográfkiértékelés során találkozik, és ideiglenesen kezel személyes adatokat. Ezek az adatok sofőrkártyán érkeznek, és kiértékelését a vállalat offline szoftver segítségével, egy speciális program segítségével végzi.

A speciális szoftver adatbázisa felhasználónévvel, jelszóval védett, így illetéktelenek az adatbázishoz nem férnek hozzá.

A program mely az adatokat tárolja, és feldolgozza, szintén jelszóval védett, a programhoz való hozzáférés csak a gépen helyi bejelentkezéssel, a géphez, és a programhoz, és az adatbázishoz beállított felhasználó/jelszó párossal nyitható meg.

A programhoz teljes hozzáférése csak a kiértékelést végző kolléga számára lehetséges. Az így kezelt adatokat, a Rukon Kft. elektronikus módon 1 év időtartamig tárolja. Célja az 561/2006 EU rendelet végrehajtása.

Online adattárolás

A Rukon Kft szerverein a bejelentkezés felhasználónévvel, és jelszóval történik, a program felhasználói nem a saját nevükkel jelentkeznek be a programba.

Az adatbázisban tárolt egyéb adatok ideiglenes tárolása történhet tachográf adat formájában. Az így tárolt adatok megnyitása csak egy speciális szoftverrel lehetséges.

Ez a jellegű adattárolás a GX Solutions szerverein történik.

Egyéb intézkedés:

A Rukon Kft. vezetése ügyvezetői utasításban rendelkezik az adatvédelmi felelős kinevezéséről.

Részletesebben az üzemelő rendszerek esetében

Kizárólag a Rukon Kft. alkalmazottai kaphatnak hozzáférési jogosultságokat.

- Külső tanácsadók, partnerek csak egyedi esetben, határozott időre és határozott feladat megoldásához láthatók eljogosultságokkal, amit dokumentálni kell.
- Minden operációs jogosultsággal rendelkező felhasználó egyedi azonosítót és jelszót kap, olyan csoportos jog, ahol a felhasználók egyedileg megkülönböztethetetlenül léphetnek be a rendszerbe, csak egyedi esetben engedélyezhető, és nem operációs jogosultsággal. A felhasználó köteles az azonosítóit titkosan kezelni, s a rendszert úgy kell beparaméterezni, hogy a felhasználók a jelszót havonta kötelesek legyenek módosítani.
- Az informatikai rendszerek naplót vezetnek az eseményekről, ahol a végrehajtó felhasználó azonosítója is szerepel, következésképp minden egyedi azonosítóval szereplő felhasználó ellenőrizhetően felelős az általa vagy az azonosítója felhasználásával más által végrehajtott eseményekért. Ezt a felhasználóban tudatosítani kell, ez magyarázza, miért kell szigorúan titkosan tartania jelszavát. Erről a hozzáférés megadásáról szóló dokumentum is értesíti a felhasználót. A felhasználó ennek tudomásulvételét a dokumentum aláírásával igazolja.
- Olyan rendszert nem üzemeltetünk belső adatok kezelésére, ahol erre az ellenőrzésre nincs lehetőség. Kivételt képez ez alól az irodai programok egy része, ahol a dokumentumok és a file-ok hozzáférésének eseti korlátozásáról a dokumentumot előállító felhasználó köteles gondoskodni, azok jelszavas védelmével.
- A rendszerek felhasználóit az informatikai szervezetnek folyamatosan figyelemmel kell kísérnie, és azon a felhasználók hozzáférési jogosultságát, akik az adott rendszerbe 3 hónapja vagy annál régebben nem jelentkeztek be, haladéktalanul fel kell függeszteni. A felhasználó jogosultságának fenntartásának tisztázása érdekében a rendszergazda tájékoztatása alapján, az informatikai vezető a felhasználói szervezet vezetőjével egyeztet.
- Munkaviszony megszűnése esetén a felhasználó hozzáférési jogosultságát azonnali hatállyal meg kell szüntetni. Amikor a rendszer erre lehetőséget ad, a felhasználót törölni kell a rendszerből.
- Az esetlegesen felszabadult felhasználói licencről az informatikai vezetőt a rendszergazda köteles tájékoztatni.
- Az informatikai szervezet szakemberei minden olyan adat-karbantartási, javítási feladatot, amely a rendszerben tárolt szakmai adatokat érinti, csak az adott szakterület vezetőjének tudtával és beleegyezésével végezhetnek el.
- A rendszerek által előállított naplókat az informatikai szervezet köteles követni, a naplózás mélységét a rendszer teljesítményét lényegesen nem befolyásoló alacsony szintre állítani. Az események és a rendszerek teljesítmények reprodukálhatósága miatt a naplókban fellelt minden nem üzemszerű eseményt dokumentálni kell.
- Bármely informatikai alkalmazásból nyert vagy nyerhető adatok felhasználása a Rukon Kft. adatvédelemmel foglalkozó belső szabályzatai vonatkozó utasításainak megfelelően engedélyezett.

- A rendszer operációs felhasználói számára a munkahelyi vezető állítson össze egy a rendszer moduljainak használatával kapcsolatos feladataik felsorolását tartalmazó leírást, melyet az informatikának egyértelműen meg kell feleltetni a rendszerben lévő standard, vagy egyedileg összeállított felhasználói profiloknak. A leírást csatolni kell a felhasználó jogosultsági lapjához.

Részletesebben a bevezetés alatt álló rendszerek esetében

A rendszer bevezetésének befejezéséig a tanácsadó cég munkatársai közül csak a bevezetés alatt álló modul konzulense lehet állandó felhasználó. A szerverek felügyeletét távdiagnosztika segítségével ellátó partner cég a szerződésben szereplő munkák ellátásához szükséges jogosultságokkal rendelkezhet.

Sérülés és megsemmisülés

Az adatok sérülés elleni védelme szorosan összefügg az üzemeltetés biztonságával, a hardver megbízhatóságával, és a mentési, archiválási stratégiával, ezért egyes kérdésekről az adott témakört tárgyaló fejezetekben lesz szó. A következő gondolatok néhány általános alapelvet tartalmaznak az adatok kezelésével kapcsolatban.

Az informatikai alkalmazásoknak az adott ország gazdasági szabályozóival és törvényeivel szoros összhangban kell működniük. Ennek része a szabályozás szerint az adatok rendelkezésre állásának, megtartásának rendszere (pl. a számviteli törvény a megelőző tíz év adatainak, bizonylatainak megtartását írja elő). A szabályozás hatálya alá eső adatokat az informatikai szervezet köteles a különböző törvényeknek megfelelő ideig reprodukálható állapotban megőrizni (archiválni).

Az üzemeltetés során minden adathordozó (merevlemez, mentés céljaira szolgáló hajlékony lemez, szalag, kazetta, CD, optikai lemez stb.) és egység meghibásodása potenciálisan adatsérüléshez vagy adatvesztéshez vezet. Ezért a fenti eszközök üzembiztonsága és az adathordozók hibamentessége határozza meg az adattárolás biztonságát. A szervereken a rendelkezésre álló diagnosztikai eszközök segítségével, heti rendszerességgel meg kell vizsgálni a merevlemezek állapotát, hiba esetén haladéktalanul a vonatkozó üzemeltetési szabályok szerint kell eljárni. Mentések során csak a mentőegység által megkövetelt típusú és minőségű hordozó használható.

Egy rendszer verzióváltásakor a korábbi verzió által előállított adatokat a mindenkori lehetőségek szerint az új verzió számára közvetlenül Backup vagy közvetve archiválva (TEXT, stb. állományban) elérhetővé kell tenni. Az eljárás pontos leírása az adott rendszer lehetőségeinek megismerése után lehetséges. Ezt a verzióváltás előtt írásban rögzíteni kell. A rendszer esetleges összeomlása során a helyreállítás csak a mentett adatok felhasználásával lehetséges. A rendszer és az adatbázis adatok hordozóit biztonságos helyen - a szervertől távol, elzárva, kizárólag más épületben tűz- nedvesség- és fizikai károsodás ellen védett helyen - kell elhelyezni az adatbiztonság és adatvédelem szabályainak figyelembevételével (pl. trezor). Az adathordozók azonosításának, a mentések, archiválások dokumentálásának áttekinthetőnek és egyértelműnek kell lennie.

Szerverszoba

A szerver szoba a T-systems Asztalos Sándor utcai telephelyén található. Kizárólag az informatikai vezető, valamint az ügyvezető jogosult a szerverekhez hozzáférni. Egyéb fizikai hozzáférés csak-e két személy jelenlétében lehetséges.

Szerver háttér adattároló egysége

A szervereken a felhasznált technika által biztosított adatbiztonságot szolgáló megoldások közül az aktuálisan elfogadott (jelenleg a RAID) szolgáltatást kell alkalmazni. A rendelkezésre álló diagnosztikai eszközökkel a működést, naplókat, az esetleges hibákat folyamatosan figyelemmel kell kísérni.

Áramellátás

A váratlanul bekövetkezett áramszünetek miatti rendellenes leállás problémákat okozhat, többek között adatvesztést. Ennek megelőzésére a szerverek és a hálózati aktív elemek mellett mindenképp szünetmentes áramforrást kell alkalmazni. A szerver melletti UPS áramszünet esetén normál leállítási procedúrát kell, hogy kezdeményezzen a szerveren. Az eszköz fizikai állapotáról és a leállítási procedúra működéséről havonta meg kell győződni, és dokumentálni. A szerverek áramellátásáról a szerződéses kereteknek megfelelően a T-systems gondoskodik.

Mentés és archiválás

A mentés egy rendszer elemeinek (adatok, konfigurációs beállítások, programok stb.) más adathordozóra való másolása olyan formában, hogy arról a mentés időpontjában tétező eredeti állapot visszaállítható.

Mentési stratégia és procedúra

A mentésért és dokumentálásukért közvetlenül a rendszergazdák felelősek. A központi mentések szabályos elkészítésért és dokumentálásáért a biztonságtechnikai rendszergazdák másodsorban felelősek, és minimum hetente kötelesek ellenőrizni a mentést, annak dokumentáltságát és szúrópróbaszerűen annak hitelességét. A vizsgálat elvégzését a rendszergazda aláírásával igazolja.

Egy működő rendszer minden eleméről aktuális mentéssel és a mentés aktualizált dokumentációjával kell rendelkeznie az informatikai szervezetnek.

A mentések dokumentációját meg kell őrizni. A mentési intervallumok megtervezésénél figyelembe kell venni a visszaállíthatóságot, valamint a rendszert érintő nagyobb változásokat.

A mentéshez használt adathordozóknak a mentési eszköz által megkövetelt minőségűnek és állapotúnak kell lenniük. Az adathordozót feliratozással egyértelműen azonosítani kell. Minden időpontban az adathordozó korábbi felhasználásának ismertnek kell lennie. Az adathordozó annyiszor használható, ahányszor a típus leírás engedélyezi. Ügyelni kell a fokozott igénybevételek számolására is, mint pl. a visszaolvasás.

Alapvető követelmény, hogy egy rendszer elemeit érintő minden komolyabb beavatkozás előtt mentést kell készíteni, azonosítani és dokumentálni továbbá meg kell meggyőződni annak teljes sikeréről. Ennek célja a beavatkozás sikertelensége esetén az eredeti állapot visszaállíthatóságának biztosítása. Ezt az adathordozót addig kell megőrizni, amíg a beavatkozás sikerességéről a rendszer üzemeltetése során teljesen meg nem győződtünk.

A rendszert érintő komolyabb beavatkozásnak minősíthető:

- Verzióváltás (operációs rendszer, adatbázis kezelő, rendszer release vagy verzió),
- Archiválás (funkció, a már nem szükséges korábbi időszak bizonylatainak, egyéb adatainak törlése és egy a rendszeren kívüli olvasható állapotba való elhelyezése),

- Hardver átkonfigurálás,
- Adatok reorganizációja,
- Mentési rendszer megváltozása.

A beavatkozás utáni állapotról is mentést kell készíteni - azonosítani és dokumentálni és a következő beavatkozásig, azt megőrizni. Célja az esetleges rendszerösszeomlások után a legutóbbi aktuális változat helyreállítása. A fenti szabályozás a rendszer minden elemét érintheti.

A rendszer üzemszerű használata során minden pillanatban módosulnak a tárolt adatok. A módosulások megtartásáról gondoskodni kell, erre szolgál az adatok mentésének ciklikus ismétlése. A ciklus legkisebb eleme a napi mentés, amely egy speciális szolgáltatás, amely vagy a teljes adathalmazt érint, vagy csak a változásokat helyezi el külső adathordozón automatikusan éjszaka lefutva. A napi mentéshez szükséges körülményeket műszak végén biztosítani kell. Műszak kezdetekor a mentés sikerességéről meg kell győződni, és az eredményt dokumentálni. A napi mentések csoportosításával lehet a biztonságos ciklikusságot előállítani.

A ciklikus mentési stratégia elemei:

- Napi mentés (egy hétig minden nap elkészül különböző adathordozókra).
- Heti mentés (a hét utolsó napjának mentése, amelyet egy hónapig kell megőrizni).
- Havi mentés (a hónap utolsó hetének mentése, amelyet negyedévig kell megőrizni).
- Negyedéves mentés (a negyedév utolsó hónapjának mentése, amelyet egy évig kell megőrizni).
- Éves mentés (az utolsó negyedév mentése, amely tartós tárolásra kerül).

A nagyobb biztonság miatt a heti mentéseket A és B hétre osztva külön-külön hordozó csomagra kell elkészíteni. Gazdasági szakmai megfontolások szerint egyes a ciklus felső szintjére emelt (heti, havi, negyedéves, éves) elemek lecserélhetők a gazdasági időszak lezárása után keletkezett mentésre, vagy ekkor külön mentés készülhet (üzemviteli mentés).

Kampányidőszakban az átlagos felhasználás nem indokolja a hét napos munkahétre való áttérést a mentések területén, egyedi esetben azonban alkalmazható.

Az egyéb alkalmazásokat kiszolgáló (kiegészítő) szerverek esetében meg kell határozni az azon tárolt mentendő adatok körét. Az adattárolás szerkezetét (pl. könyvtárszerkezet) és a hozzájuk kötött jogosultságokat úgy kell kialakítani, hogy a nem, vagy nehezen reprodukálható adatok kizárólag meghatározott helyekre kerülhessenek. Erről folyamatosan tájékoztatni kell a felhasználókat.

A kiegészítő szervereken tárolt adatok mentések módját (eszköz, szoftver) a rendszer kialakításának megfelelően kell kidolgozni az egységesítési elveknek megfelelően. Az adathordozók tárolási és archiválási rendjét egyedileg kell kidolgozni a szerveren tárolt adatok mérete és fontossága figyelembevételével.

A kiegészítő szerverekhez az informatikai vezető rendszergazdát köteles rendelni, aki felelős az adatok biztonságáért, ezt szúrópróbaszerűen ellenőrizni kell. A dokumentálás a korábban tárgyalt elvek szerint történik.

Az egyedi PC lokális háttértárain tárolt adatok, felhasználásáért és megőrzésért a számítógép felhasználói a felelősek. Az informatikai szervezet köteles segítséget nyújtani minden felhasználónak a mentésekhez használatos eszközök megismerésében és biztosításában és az adatvédelmi kérdések fontosságának tudatosításában.

Archiválási stratégia és procedúra

Az archiválás a mentett (és esetlegesen az elsődleges hordozóról törölt) adatok megőrzésének módja a visszakereshetőség és a reprodukálhatóság szem előtt tartásával.

Az archiválás fogalma a kiválasztott időszak és adatcsoport bizonylatainak és egyéb adatainak törlését jelenti egyidejűleg egy archív állományba helyezéssel. Az archív állomány az adott rendszer által olvasható formában tárolja az adatokat, és korlátozottan biztosítja a lekérdezhetőséget.

A rendszer esetleges release vagy verzió váltásánál (eddig ilyen jellegű tapasztalattal nem rendelkezünk) az archivált adatok további olvashatóságát mindenképp biztosítani kell.

A verzióváltások előtt ezt a kérdést pontosan meg kell vizsgálni, és csak a megnyugtató válaszok után szabad az áttérést megvalósítani.

Az archivált adatok mentésétre, tárolására és dokumentálására, az adatmentésekre vonatkozó utasítások érvényesek a következő kiegészítésekkel:

- Az archivált adatokat tartalmazó mentéseket legalább két példányban kell elkészíteni, és lehetőség szerint a szerveren is meg kell tartani.
- Az azonos adatokat tartalmazó archivált mentéseket mindig eltérő helyen kell tárolni.
- Az archív mentéseket soha nem szabad megsemmisíteni, vagy újrafelhasználni.
- Archivált mentés csak új és ellenőrzött adathordozóra készülhet.
- Az archivált adathordozók állapotát, reprodukálhatóságát évente legalább egyszer ellenőrizni kell, amiről jegyzőkönyvet kell készíteni.

Az archiválási intervallumokat a rendszer teherbírása alapján a vonatkozó jogszabályok figyelembevételével csoportszinten kell kialakítani.

A kiegészítő alkalmazások adatainak archiválása egyszerűen a külső adathordozóra másolt adatok megőrzését jelenti. Az mentés és adattárolás biztonsági szabályainak figyelembevételével egyedi, helyi szabályozás kidolgozása szükséges minden olyan esetben, amikor a tárolt adatok fontossága azt szükségessé teszi (többévi, nagy tömegű, jogszabályok által érintett adatok, stb.).

Az egyedi PC saját háttértárain tárolt adatok archiválásáért a PC felhasználója felel (PC a személyes felhasználású, kisebb jelentőségű vagy könnyen reprodukálható, származtatott adatokat lehet tárolni).

Üzembiztonság

Az üzembiztonság fenntartásáért elsősorban az informatikai vezető felel. Az üzembiztonsági paraméterek figyelési és véleményezési és dokumentálási feladataira köteles egy belső szakembert kinevezni, aki a kivételes esetekben tájékoztatja.

Környezet

A számítógépek és tartozékaik a vagyonvédelmi részben foglalt környezeti követelményeknek megfelelő helyiségbe telepíthetők és üzemeltethetők.

A körülményekben beállt változást az informatikai szervezet felé jelezni kell.

A hordozható és az otthon használt számítógépek és egyéb eszközök elhelyezéséért az a személy felel, akinek azok használatra ki lettek adva.

Technológia

A számítástechnikai eszközöket és berendezéseket, valamint alkalmazási területeket üzemi fontosságuk szerint szakmai megfontolások alapján csoportosítani kell A, B, C kategóriákba:

- A kategória: kulcsfontosságú berendezések és területek, melyek kiesése a szervezet komoly működési zavarait okozza, vagy a fő üzleti folyamatok követését és irányítását megakadályozza és kiváltása azonnal nem megoldható (pl rendszer, szerverek, aktív hálózati elemek, összeköttetés, stb.)

- B kategória: Az "A" kategóriába sorolandó de gyorsan kiváltható nem különösen nagy értékű, illetve csak lokális működési zavarokat okozó berendezések (pl. nagy terheltségű hálózati

nyomtatók, hálózati passzív elemek, modemek, kiegészítő egyedi alkalmazások, nagy terhelésű munkaállomás, stb.).

- C kategória: Berendezések tartozékai, perifériák, kiegészítő eszközök, azonnal telepíthető standard szoftverek, melyek meghibásodása nem okoz jelentős fennakadást, értéke nem jelentős, beszerzése vagy raktárról való pótlása nem igényel hosszabb időt (képernyő, helyi nyomtató, egér, billentyűzet, irodai szoftverek, stb.)

A különböző kategóriák meghibásodása esetén a hiba megszüntetése érdekében szükséges eljárások különbözők. Minden esetben az elsődleges szempont a kieső idő csökkentése, a rendszer legteljesebb működőképességének biztosítása.

Az "A kategória" berendezéseinek meghibásodása esetén:

- Az eset körülményeiről jegyzőkönyvet kell, felvenni időpontok, kieső idők, pontos műszaki leírás tartalommal, és minden külső és belső szakember tevékenységét abban rögzíteni,
- Azonnal meg kell kezdeni a hiba elhárítását saját erőből, amennyiben erre lehetőség van (csere, tanácsadás, javítás),
- Helyette vagy párhuzamosan a külső szolgáltatóval kötött érvényes karbantartási és hibaelhárítási szerződés szerint is el kell járni.

A "B kategória" berendezéseinek meghibásodása esetén:

- Szükség szerint, jegyzőkönyvet kiállítania fenti tartalommal, mérlegelve a folyó tevékenységeket, a lehető leghamarabb be kell sorolni a hiba elhárításának megkezdését.
- Raktáron lévő berendezés csere lehetőségének esetén a cserét azonnal el kell kezdeni,
- Azonnali beszerzési szükségszerűség esetén a gyorsított beszerzést elindítani,
- Egyéb esetekben az érvényes karbantartási és hibaelhárítási szerződés szerint kell eljárni.

A "C kategória" berendezéseinek meghibásodása esetén:

- A felhasználási terület fontosságának mérlegelése után a hibaelhárítást a lehetőségek szerint kell elvégezni.
- Csere esetén a munkát azonnal raktárról, vagy beszerzés után el kell végezni.

Karbantartás

Az üzembiztonság legfontosabb kérdése az állapotfigyelés és a karbantartás. Az informatikai rendszer különböző pontjain a fontosságnak megfelelően üzembiztos berendezéseknek kell működni. Költség szempontok figyelembevételével is raktáron kell tartani azokat a kisebb részegységeket és perifériákat, melyek meghibásodása gyakori, és cseréje nem igényel külső segítséget. Az eszközök állapotát azok jellegétől függő módszerekkel állandóan figyelni kell, hogy jelentős romlás esetén a pótlás, felújítás időben elkezdhető legyen.

Informatikai vezető
(Becsei Sándor)

ügyvezető
(Szécsi Rezső)

Budapest, 2015.01.01.