Fogalommagyarázatok és definíciók

(az informatikai szabályzatokhoz)

Készült: 2006. május 25.

Adat
Az információ megjelenési formája, azaz a tények, elképzelések nem értelmezett, de értelmezhető közlési formája.

Adatállomány
Valamely informatikai rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek. Ezen a néven keresztül férhetünk hozzá a tartalmazott adatokhoz.

Adatátvitel
Adatok informatikai rendszerek, rendszerelemek közötti továbbítása.

Adatbiztonság
Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

Adatkezelés
Adatok feltérképezése, gyűjtése, felvétele, tárolása, rendszerezése, feldolgozása, hasznosítása, sokszorosítása, továbbítása (hozzáférhetővé tétele harmadik fél számára), átadása, ábrázolása, nyilvánosságra hozatala, bárminemű megváltoztatása, további felhasználásuk megakadályozása, illetve törlése – a jogszabályi és a belső szabályozási követelmények betartásával.

Adatok biztonsági osztályba sorolása
Az adatok tudatos értékelése és minősítése az érzékenységi fok és a kritikusság alapján.
Az egyes biztonsági osztályok:
- alapbiztonsági osztály,
- fokozott biztonsági osztály,
- kiemelt biztonsági osztály.

Minden rendszert minősíteni kell az általa kezelt adatok minősítésének figyelembe vételével.
Amennyiben egy rendszer több kategóriába eső adatot kezel, a legmagasabb kategóriát kell a rendszer minősítésének tekinteni.

Adatvédelem
Az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során az érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségeire vonatkozik.

Alapfenyegetettség
A fenyegető tényezők olyan csoportosítása, amely a biztonsági alapfunkciók valamelyikének kiesését okozza:
- a működőképesség elvesztése;
- a hitelesség elvesztése;
- a bizalmasság – titkosság elvesztése;
- a sértetlenség – integritás elvesztése;
- a rendelkezésre állás elvesztése.

Alkalmazás
Olyan program, amelyet az alkalmazó saját igényei, céljai érdekében használ, és amely a hardver és az üzemi rendszer funkcióit használja.

Alkalmazásgazda
Az üzemeltetés belső szabályozásában meghatározott értelemben.
Alkalmazói program (alkalmazói szoftver, alkalmazás, felhasználói program)
Olyan program, amelyet az alkalmazó saját speciális céljai érdekében vezet be, és amely a hardver és az üzemi rendszer funkcióit használja.

Állásidő
Az a teljes időtartam, amely alatt egy szolgáltatás, vagy komponens nem működik a megállapodott szolgáltatási időn belül. A szolgáltatás, vagy komponens meghibásodásától a normális működés újraindulásáig mérik.

Archiválás
Inaktív adatoknak eredetitől eltérő – általában egyszer írható – médiára való másolása hosszú távú megőrzés céljából. Gyakran együtt jár az adatok eredeti példányának törlésével.

Archívum
Dokumentációs gyűjtemény, irattár.
Informatikai értelemben: a mindennapi működés során (már) nem használt dokumentumok tárolására szolgáló informatikai rendszer, amelyben a dokumentumokat fizikailag egy példányban, nem módosítható formában, eredeti példányként tárolják, biztosítva későbbi a visszaolvashatóságot.

Back-up rendszer
Az adatbiztosítás során az adatok rendelkezésre állását lehetővé tevő másolatokat őrző rendszer. Rendszerint minimális tartalékkal rendelkező informatikai rendszert is értenek alatta.

Bejelentkezés
A felhasználótól kapcsolatot kezdeményez az informatikai rendszer irányába, amelynek során az informatikai rendszer azon funkcióinak használata lehetővé válik, amelyekhez jogosultsággal rendelkezik.

Belépés
Személyek belépése olyan területekre, például helyiségekbe, amelyekben az informatikai rendszert, illetve egyes elemit tárolják, vagy használják.

Bizalmasság – titkosság
Az információhoz csak azok a természetes és jogi személyek férhetnek hozzá, akiket erre feljogosítottak, és azok is csak az előírt módon. Az adatok biztonsági osztályba sorolása meghatározza azok kezelési módját a bizalmasság – titkosság vonatkozásában is.

Biztonság
Veszélyektől vagy bántódástól mentes (zavartalan) állapot. A rendszerek szabályszerű működésének és a működőképesség fennmaradásának kedvező állapota. Lásd még: Informatikai biztonság.

Biztonsági esemény
A szabályszerű működés sérülése, olyan kedvezőtlen változás, amelynek hatására a biztonság állapota sérül. Fenyegetés a biztonságra nézve, illetőleg figyelmeztető jel a fenyegetésre vagy annak lehetőségére.
Informatika értelemben: az adatok, információk bizalmasságának – titkosságának és / vagy sértetlenségének és / vagy rendelkezésre állásának megsérülése vagy a sérülés lehetősége.

Biztonsági környezet
A szervezet működésének, fejlődésének és fennmaradásának, az erőforrások felhasználásának és a termékek / szolgáltatások létrehozásának keretrendszere, amely a külső jogi és egyéb szabályozások, a szervezet belső szabályai, szokásai, normái, az ott dolgozók szakértelme és tudása, valamint egyéb külső elemek összessége által meghatározott módon működik. Vagyis a tágan értelmezett szervezeti környezet egészére figyelemmel kell lenni a biztonsági kérdések megválaszolásakor.

Biztonsági követelmények
A kockázatelemzés eredményeként meghatározott fenyegető tényezők ellen irányuló biztonsági szükségletek együttese.

Biztonsági tudatosság
A szervezet kultúrájának része, olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a munkatársak személyes elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják azokat, és másokkal is megismertetik, illetve betartatják ezeket.

Egyenszilárdságú biztonság
A szervezet valamennyi tevékenységét átfogó, minden ponton (közel) azonos erősségű biztonság.
EFK - Egészségügyi Főiskolai Kar
EKG - Elektronikus Kormányzati Gerinchálózat

Elektronikus aláírás
A levelezőrendszer azon szolgáltatása, melynek segítségével a levél címzettje megbizonyosodhat a küldő személyéről, arról, hogy a levelet a továbbítás során senki sem módosította, valamint a küldő sem tagadhatja le a levél elküldésének tényét.

Eseménynaplózás
Tevékenységek időrendi rögzítése, regisztrálása, illetve a készített naplók megőrzése. Annak biztosítása, hogy a megtörtént események, végrehajtott műveletek, lezajlott eljárások utólag rekonstruálhatóak és elemezhetőek legyenek, azért, hogy az illegális vagy nem megfelelő tevékenységek feltárásra, jelentésre, illetve bizonyításra kerülhessenek.
Az eseménynaplózáskor rögzíteni kell:
- a tevékenység azonosítását;
- amennyiben a tevékenység hozzáféréssel kapcsolatos, akkor a felhasználó és a végberendezés azonosítását;
- a bejelentkezés és a kijelentkezés dátumát és időpontját;
- továbbá a sikeres mellett a sikertelen rendszer-, adat- és erőforrás-elérési kísérleteket is.

Eszkaláció
Egy incidensről, problémáról, vagy változtatásról szóló információ továbbadása és/vagy intézkedés kérése a rangidős személyzettől (hierarchikus eszkaláció), vagy más szakértőtől (funkcionális eszkaláció). Az eszkalációs szabályokat a prioritási célokhoz kapcsolják.

Eszköz
Szó szerinti jelentése tulajdonolt értékes személy, vagy tárgy; az eszközök gyakran megjelennek a mérlegben, mint a szervezet kötelezettségeivel szembeállított tételek.
Az informatika-szolgáltatás folytonosságának biztosításában, a biztonsági átvizsgálásban és menedzsmentben az eszköz olyan tétel, amellyel kapcsolatban fenyegetések és sebezhetőségek azonosíthatók, számolhatók, a kockázatelemzés elkészítésének céljából. Ebben az értelemben a szolgáltatások vizsgálatában az eszköz fontossága számít és nem annak a költsége.

Észlelés
Az incidens életciklusának második állomása az előfordulás után, amikor a szolgáltatás hibája ismertté válik az informatikai szervezet számára.

Feladatkör
Valamely természetes vagy jogi személyre háruló, összetartozó feladatok (vagyis kötelességszerűen elvégzendő dolgok) összessége.

Feladatmegosztás
Az informatikai rendszereket használó és üzemeltető személyek feladatköreit úgy kell meghatározni, hogy azzal minimalizáljuk a mulasztások és szándékos visszaélések kockázatát, ugyanakkor biztosítsuk a minél teljesebb körű helyettesítés vagy kiváltás lehetőségét. Célja, hogy minden folyamat lefutásába beleépüljön a kontroll – vagyis egyetlen személy se tudja (szándékosan vagy gondatlanságból) megakadályozni valamely folyamat lefutását, illetve a szervezet számára károsan eltéríteni azt eredeti rendeltetésétől. A feladatmegosztás kialakítása biztonsági vezetői feladat.

Feladatelhatárolás
Az informatikai biztonság szempontjából összeférhetetlen munkakörök szétválasztása a szükséges tudás elve alapján, vagyis: a kiemelt biztonsági osztályba tartozó vagyon tulajdonosa meghatározza a felhasználók számára hivatali kötelezettségeik függvényében jogosultságaikat (az adatkezelésre, információkezelésre, rendszerek esetében ezek használatára vonatkozóan). A feladatelhatárolások kialakítása biztonsági vezetői feladat.

Felelős
A rábízott dolgokról, személyekről, feladatokról számot adni, a velük kapcsolatos anyagi, jogi stb. következményeket viselni köteles természetes vagy jogi személy.

Felhasználó
Az a személy, vagy szervezet, aki, amely egy, vagy több informatikai rendszert használ feladatai ellátásához.

Felhasználói azonosítás és hitelesítés
A felhasználói azonosítás és hitelesítés jelenti a rendszerekhez, adatokhoz, adatkezelési formákhoz történő hozzáférés alapját.
- Felhasználói azonosítás: az informatikai rendszer minden felhasználóját egyedi azonosítóval kell ellátni az eseménynaplózás céljainak érdekében. Egyes kivételes esetekben kiadható osztott azonosító is egy használói csoport számára.

– Felhasználói hitelesítés: folyamat, melynek során megtörténik az azonosított felhasználó hitelességének ellenőrzése, annak igazolása, hogy ténylegesen az-e, akinek állítja magát, s ha tényleg az, akkor megtörténik jogainak érvényesítése.

Fizikai biztonság
A fizikai erőforrások szabályszerű működésének és a működőképesség fennmaradásának kedvező állapota.
Informatikai értelemben: az információ bizalmasságának – titkosságának, sértetlenségének – integritásának és rendelkezésre állásának megőrzése – fizikai oldalról. Pl. belépési engedélyek és korlátozások, zárrendszerek, tűzvédelmi rendszerek, robbanás- és földrengésvédett kialakítás, lopás és rongálás elleni védelem révén.

Funkcionalitás
Mindazon tevékenység, rendeltetés és feladat, amit egy adott rendszer, program vagy eszköz képes nyújtani, illetve elvégezni a felhasználó számára. Az informatikai rendszerek esetében a különböző adatok kezelésének, az eljárások végrehajtásának biztosítása a működési folyamatok támogatására – melyet a rendszer megfelelő tervezése és hatékony működtetése tesz lehetővé.

Gépterem
Szervert, vagy az IT-infrastruktúra szempontjából kiemelkedő fontosságú berendezést (pl. switchet) is tartalmazó, de nem kizárólag ezek tárolására használt terem. Ilyen pl. az olyan rendszergazdai szoba, melyben szerver működik.

Harmadik fél
Az adatkezelés kapcsán harmadik félnek minősül az a szervezet állományába nem tartozó, külső természetes vagy jogi személy:
– akire a szervezet birtokában lévő adatok vonatkoznak;
– vagy akik valamilyen szerződéses vagy egyéb jogilag szabályozott kapcsolat keretében a szervezet valamely adataival kapcsolatban adatkezelést végeznek.

Hardver
Az informatikai rendszer eszközeit, fizikai elemeit alkotó részei.

Hatáskör
Intézkedési jog köre, érvényességi határa. A munkakör betöltőjének a feladatai ellátása érdekében szükséges cselekvési jogosultságai. Fajtái:
– döntési,
– véleményezési,
– javaslattételi,
– információadásra vonatkozó,
– valamint információ megkapására vonatkozó.

Hálózat
Két vagy több számítógép, vagy általánosabban informatikai rendszerek összekapcsolása, amely informatikai rendszerek legkülönbözőbb komponensei között adatcserét tesz lehetővé.

Hálózatmenedzser
Az üzemeltetés belső szabályozásában meghatározott értelemben.

Helyi rendszer
Használata, üzemeltetése egy intézetre korlátozódik.

Helyreállítási idő
Valamely informatikai szolgáltatás vagy információtechnológiai komponens hibája esetén a normál működés állapotába történő visszaállításhoz szükséges időtartam.

Hiba
Az a körülmény, amely előidézi, hogy egy funkcionális egység képtelen lesz a tőle megkívánt funkció ellátására.

Hitelesség
Az adatnak az a tulajdonsága, amely megmutatja, hogy bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik-e.

Hozzáférés
Olyan eljárás, amelynek révén az arra jogosult személy számára elérhetővé válik, amire szüksége van. A hozzáférés jog, mely felelősséggel jár.
Informatikai értelemben: a hozzáférés eljárásán keresztül az informatikai rendszer jogosult használója számára – jogosultságainak megfelelően – elérhetővé válnak a rendszerben tárolt adatok, valamint az ezeken történő adatkezelés. Az adatokhoz, információkhoz és rendszerekhez való hozzáférést az üzemeltetési és a biztonsági követelmények alapján ajánlatos kialakítani, ellenőrzés alatt tartani és menedzselni.

A hozzáférés két fajtája:
- fizikai hozzáférés: olyan eljárás, amelynek révén az arra jogosult személy számára elérhetővé válnak az informatikai rendszer meghatározott hardver elemei;
- logikai hozzáférés: olyan eljárás, amelynek révén az arra jogosult személy számára elérhetővé válnak az informatikai rendszer meghatározott szoftver elemei.

Humán biztonság
A humán erőforrásokkal kapcsolatban álló rendszerek szabályszerű működésének és a működőképesség fennmaradásának kedvező állapota.
Informatikai értelemben: az információ bizalmasságának – titkosságának, sértetlenségének – integritásának és rendelkezésre állásának megőrzése – humán oldalról. Pl. az alkalmazotti és egyéb szerződések előtti informálódás, a szerződés létrejöttekor titoktartási megállapodás megkötése, a munkaköröknél a biztonsági feladatok, hatáskörök és felelősségek rögzítése révén.

Informatika
A számítógépes információrendszerek tudománya, amely elméletet, szemléletet és módszertant ad a számítógépes információrendszerek tervezéséhez, fejlesztéséhez, szervezéséhez és működtetéséhez.

Informatikai biztonság
Olyan állapot, amelyben az informatikai rendszer védelme – a rendszer által kezelt adatok bizalmassága, sértetlensége, hitelessége, illetve rendelkezésre állása és működőképessége szempontjából – zárt, teljes körű, folyamatos és a kockázatokkal arányos.
A védelem zárt, ha az összes releváns tényezőt figyelembe veszi. Teljes körű a védelem, ha a védelmi intézkedések az összes rendszerelemre kiterjednek. A folyamatos védelem jellemzője, hogy az időben változó körülmények ellenére megszakítás nélkül, állandóan megfelelő mértékű védelmet nyújt. Ha a védelem a kockázattal arányos, akkor hosszú távon a védelem költségei arányosak a potenciális kárértékkel. Ezt az arányt a Biztonsági Politika határozza meg.

Informatikai infrastruktúra
Az információ áramoltatását és feldolgozását lehetővé tevő, a számítógépek és felhasználók összekapcsolására szolgáló fizikai hardver és szoftver. Tartalmazza az adatátviteli közeget, pl. telefonvonalakat, kábeltelevíziós vonalakat, műholdakat és antennákat, továbbá routereket, és más számítógép-hálózati aktív elemeket és egyéb, az adatátvitelt vezérlő berendezéseket. Tartalmazza továbbá a továbbított jelek küldéséhez, fogadásához és kezeléséhez szükséges szoftvereket.

Informatikai rendszer
A hardverek és szoftverek olyan kombinációjából álló rendszer, amit az adat- illetve információkezelés különböző feladatainak elvégzésére alkalmazunk, ezáltal támogatva a szervezet működési folyamatait.
Az informatikai rendszer elemei, melyek részt vesznek a biztonságos működés megvalósításában és fenntartásában, illetve amelyek a veszélyek által érintettek lehetnek.
Ezek:
- az informatikai infrastruktúra:
  - a szervezet,
  - a számítógépek (célszámítógépek, illetve általános célú számítógépek),
  - a hálózat,
  - a hardver elemek,
  - a szoftver elemek,
  - illetve a szoftverrel kapcsolatos telekommunikáció,
- az egyéb (pl. telekommunikáció),
- a dokumentációk,
- valamint a humán elemek: az informatikai rendszerrel – az informatikai szervezet állományán kívül – kapcsolatba kerülő természetes és jogi személyek, valamint jogi személyiség nélküli gazdasági társaságok.

Az informatikai rendszerek különleges tulajdonsága a szabad programozhatóság.

Informatikai szervezet
Ide értendő minden informatikával foglalkozó szervezet, függetlenül nagyságától, hatásköreitől, intézetben elfoglalt helyétől. (pl.: informatikai csoport, osztály, informatikai központ).

Informatika-szolgáltatás
Létező informatikai rendszerek működtetésének és hozzáférhetőségük biztosításának tevékenységköre. Szűkebb, mint az informatikai szolgáltatások tevékenységköre.

Integritás
Teljesség és épség. Ezek fenntartása megkívánja az adatok védelmét a nem engedélyezett változtatástól és rongálódástól.

Informatikai szolgáltatás
Szolgáltatási tevékenység az informatika területén. Információtechnológián alapuló rendszerek által működtetett kapcsolódó funkciók rendszere, amely egy vagy több szervezeti tevékenységet támogat. Bár számos hardver, szoftver, telekommunikációs elem alkotja, a felhasználó számára koherens és önálló entitásként érzékelhető.
Informatikai szolgáltatás lehet valamely egyszerű alkalmazás, (pl. egy főkönyvi rendszer elérése, de lehet egy komplex, számos alkalmazást tömörítő csomag, pl. iroda- automatizáció).
Tágabb tevékenységkör, mint az informatikaszolgáltatás, mert ezen túlmenően tartalmazza az új informatikai rendszerek létrehozására irányuló szolgáltatásokat (pl. rendszerintegráció, alkalmazásfejlesztés és –integráció), valamint az informatikai tanácsadás és oktatás tevékenységeit is.
Az informatikai szolgáltatási egység vezetője felel a szolgáltatás minőségéért. Egyenrangú az alkalmazásfejlesztési vezetővel, valamint a pénzügyi és adminisztrációs vezetővel.

Informatikai védelmi intézkedés
Mindazon fizikai, logikai, valamint humán alapú óvintézkedések (technológiai, belső szabályozási, jogi stb. megoldások révén)
- amelyek csökkentik az informatikai biztonság sérülésének lehetőségét;
- illetőleg amelyek a sérülés bekövetkeztekor csökkentik a felmerülő károkat.

Információ
Bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságot csökkent vagy szüntet meg.

Információkezelés
Az adatkezelés definíciójából levezethető.

Internet
TCP/IP protokollon alapuló, nyilvános, világméretű számítógépes hálózat.
Az egész világot behálózó kommunikációs közeg, melyben hálózatok és számítógépek csatlakoznak egymáshoz (hálózatok hálózata) és amelyen emberek és alkalmazások információt cserélnek egymással.
Az Internetnek talán legismertebb része a Web (WWW), további részei: Usenet, Arpanet, Bulettin Boards, különböző on-line szolgáltatások és egyéb hálózatok.

Ismert hiba
Egy konfigurációs elem hibája, amelyet egy probléma sikeres diagnózisa felismert, és amelyhez egy ideiglenes megkerülő megoldást, vagy egy végleges megoldást találtak. Az ismert hiba és a konfigurációs elem kapcsolata eredhet egy probléma helyi diagnózisából, de származhat külső forrásból is. Fontos, hogy minden lényeges ismert hibát rögzítsünk a konfigurációkezelés adatbázisába (CMDB), bár az nyilván nem az ismert hibák adatainak egyetlen forrása. Mivel sok problémának több kiváltó oka lehet, az egyes problémák és az egyes ismert hibák közötti kapcsolat esetenként igen komplex. (Jó példa egy ismert hibára, amikor a hibát az adott szoftver következő kiadásában fogják csak kijavítani, addig együtt kell élni vele.)

IT
Informatika
ITIL (Mozaikszó: Information Technology Infrastructure Library)
Az informatikai szolgáltatás menedzsment módszertana.

Jogosultság
Valamire jogosító jogi helyzet, állapot. A lehetőség megléte valamely tevékenység végrehajtására.
Informatikai értelemben: a jogosultság jog az adatkezelésre, információkezelésre, illetve a különböző rendszerek, programok, eszközök használatára.

Jogosultsági rendszer
A szervezethez tartozó belső és külső felek jogosultságainak rendszere (felhasználói csoportok, illetve az általuk végezhető műveletek rendszere), illetve az e rendszer menedzseléséhez kapcsolódó feladatok összessége.
A jogosultsági rendszer értelmezhető egy-egy alkalmazás szintjén is (pl. egy levelezési rendszerre).

Kapacitásmenedzsment
Az a szolgáltatásirányítási folyamat, amelynek feladata az informatikai kapacitásra vonatkozó üzleti igények meghatározása, mind technikai, mind üzleti értelemben, valamint annak megértése és bemutatása, hogy e tevékenységmennyiségeknek az informatikai infrastruktúrán a megfelelő időben és optimális költséggel történő megtermelése milyen következményekkel jár.
Katasztrófa
Informatikai rendszer, rendelkezésre állásának megszűnése, vagy nagy mértékű csökkenése.

Katasztrófa-elhárítási terv
A katasztrófa elhárítási terv – informatikai vonatkozásban – tartalmazza mindazokat az információkat, melyek szükségesek egy esetleges katasztrófa bekövetkezte után az informatikai szolgáltatások ellenőrzött, egy előre megállapított szinten történő helyreállításához. A terv világos útmutatást ad érvényes a személyi felelősségekre, illetve az elvégzendő tevékenységekre vonatkozóan, illetve arra is, hogy hogyan, és mikor kell használni.

Kijelentkezés
A felhasználótól kezdeményezésére az informatikai rendszer irányába, amelynek során az informatikai rendszer számára biztosított funkcióinak használata lehetővé válik.

Kockázat
Valamely cselekvéssel járó veszély, veszteség lehetősége. A fenyegetettség mértéke, amely valamely fenyegető tényezőből ered, és amelyet a kockázatelemzés során a fenyegető tényezők értékelése révén tárunk fel. A kockázat a kárnagyság és a bekövetkezési valószínűség (gyakoriság) szorzata.

Kockázatértékelés
Az információ és az informatikai eszközök fenyegetettségének, sérülékenységének és befolyásolhatóságának, valamint ezek előfordulása valószínűségének felbecslése, vagyis:
- a kockázati tényezők feltárása;
- a feltárt tényezők kvalitatív értékelése;
- a kritikus tényezők kiválasztása;
- szükség esetén a kritikus tényezők mélyebb értékelése.

Kockázatkezelés
Az informatikai rendszerre hatással bíró biztonsági kockázatok kezelése, minimalizálása, megszüntetése érdekben elfogadható költségen kockázatmenedzsment rendszer működtetése, ennek keretében:
- az informatikai kockázatkezelési stratégia meghatározása;
- az informatikai kockázatkezelés kereteinek kijelölése;
- az informatikai kockázatkezelési kontroll működtetése:
  - a kockázatok azonosítása;
  - a kockázatok elemzése;
  - az eredmények értékelése – a kockázatok „irányítása”;
  - a kockázatok monitorozása, megfigyelése;
- valamint e rendszer felülvizsgálata, fejlesztése, megismertetése a szervezettel,
- illetve a közreműködők képzése.

Konfigurációkezelés
A konfigurációs elem azonosításának, felügyeletének és ellenőrzésének folyamata egy szolgáltatáson belül, állapotának feljegyzése, jelentése, a változáskezelés támogatására annak felmérése, hogy az elemek megváltoztatásának milyen potenciális informatikai hatása van.

Konfigurációs állomány
A konfigurációs elemek adatait tartalmazó, eszköz funkciónként különböző állomány. Ezeket a konfigurációkezelési könyvtárban kell elhelyezni.

Konfigurációs elem
A konfigurációs elem egy informatikai infrastruktúra bármely komponense lehet, beleértve a dokumentációs elemeket is, mint például egy szolgáltatási megállapodás, vagy egy változtatási kérelem, amely a konfigurációkezelés felügyelete alatt áll (vagy kell állnia), és így a változás-felügyelet hatáskörébe tartozik. Legalacsonyabb szintű konfigurációs elem rendszerint az a legkisebb egység, amely a többi összetevőtől függetlenül megváltoztatható. A konfigurációs elemek bonyolultságban, méretben és típusban széleskörűen eltérhetnek, egy teljes szolgáltatástól (beleértve az összes hardvert, szoftvert, dokumentációt, stb.) egy programmodulon át egy kisebb hardverösszetevőig. Az összes meglévő vagy potenciális szolgáltatási probléma kapcsolható kell, hogy legyen egy, vagy több konfigurációs elemhez.

Központi rendszer
Azon rendszer, amelyik kilép egy Intézet keretei közül.
LAN (Local Area Network): Helyi hálózat.

Logikai biztonság
Logikai (szoftver) erőforrások szabályszerű működésének és a működőképesség fennmaradásának kedvező állapota.
Informatikai értelemben: az információ bizalmasságának – titkosságának, sértetlenségének – integritásának és rendelkezésre állásának megőrzése – logikai oldalról. Pl. azonosítók, jelszavak, hozzáférési jogok és jogosultsági szintek révén.

Meghibásodás
Meghibásodás akkor történik, amikor a funkcionális egység már nem felel meg a céljának.

Megbízhatóság
Egy informatikai összetevő azon képessége, hogy ellásson egy tőle jogosan elvárt funkciót meghatározott körülmények között, egy meghatározott időtartamra.

Megkerülő megoldás
Eljárás egy incidens, vagy probléma elkerülésére, egy ideiglenes javítással, vagy egy olyan technikával, amely azt eredményezi, hogy az ügyfél nem függ attól a konfigurációs elemtől, amely ismerten hibát okoz.

Megoldás
Az a tevékenység, amely elhárít egy incidenst, vagyis lehetővé teszi a felhasználók számára munkájuk folytatását. Lehet ideiglenes megkerülő megoldás, vagy a hibás konfigurációs elem végleges megjavítása vagy cseréje.

Mentés
Aktív adatoknak az eredetitől eltérő adathordozóra másolása, biztonsági megőrzés, valamint meghibásodás, vagy katasztrófa bekövetkezése után az eredeti állapot visszaállításának megvalósíthatósága céljából.

Munkakörökhöz tartozó érzékenységi szint
A feladatmegosztás és feladatelhatárolás elveiből levezethető az egyes munkakörök érzékenységi szintje – a munkakörhöz kapcsolódó adatok, információk és rendszerek biztonsági osztályokhoz való tartozása alapján. Az IT biztonsági vezető jóváhagyja, véglegesíti a kategóriákat és besorolásokat.
Részletesen lásd erről a Személyzet biztonsága c. részben (5. fejezet).

Probléma
Megoldásra váró elméleti, gyakorlati kérdés. Egy, vagy több létező, vagy potenciális incidens ismeretlen eredeti oka. Nehezen megoldható kérdés, felmerült gond. Vagy egy egyedi, jelentős hatású esemény, amelynek hatása nagymértékben rontja a felhasználók számára nyújtott szolgáltatás minőségét; vagy megegyező tüneteket mutató események sorozata, amelyek valamilyen közös, de ismeretlen eredetű okra vezethetők vissza.

Problémakezelés
Az a folyamat, amely a tényleges és potenciális meghibásodások eredeti okát felismeri. Elsődleges célja annak biztosítása, hogy a szolgáltatások biztosak, pontosak legyenek és a problémák bekövetkezésének, illetve ismétlődésének esélye csekély legyen. A folyamat fejlettségét a probléma megelőzésre való képessége mutatja.

Program
Egy számítógép műveleteinek típusát és sorrendjét meghatározó utasítások sorozata. Eljárási leírás, amely valamely informatikai rendszer által közvetlenül vagy átalakítást követően végrehajtható.

Rendelkezés
Utasítás, intézkedés. Az a lehetőség, hogy valaki rendelkezhet valakivel, valamivel, utasítást adhat, munkát irányíthat, dönthet valamiben.

Rendelkezésre állás
Az a tényleges állapot, amikor is egy informatikai rendszer szolgáltatásai – amely szolgáltatások különbözők lehetnek – állandóan, illetve egy meghatározott időben rendelkezésre állnak és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.
Ebben az összefüggésben jelentősége van az információ vagy adatok rendelkezésre állásának, elérhetőségének is.

Rendelkezésre-állási arány
Annak az időnek az aránya, amely alatt a szolgáltatás ténylegesen elérhető a felhasználó számára az elfogadott szolgáltatási időn belül.
Az elfogadott szolgáltatási időszakot a Szolgáltatási Szint Megállapodás tartalmazza). Rendelkezésre állás (%) = rendelkezésre állási idő / elfogadott szolgáltatási időszak. (Pl. ha egy szolgáltatás a 40 órás szolgáltatási periódusban 39 órán keresztül áll rendelkezésre, akkor a rendelkezésre állás ez esetben 97.5%).

Rendszer
A rendszer egynemű vagy összetartozó dolgoknak, jelenségeknek, cselekvéseknek, tevékenységeknek bizonyos törvényszerűségeket mutató, bizonyos elvekhez igazodó rendezett egésze.

Rendszergazda
Az üzemeltetés belső szabályozásában meghatározott értelemben.

Rendszerelemek
Az informatikai rendszer részét képező elemek.

Rendszerelem csoportok:
- az informatikai rendszer környezetét alkotó infrastruktúra,
- az informatikai rendszer hardverelemei,
- az informatikai rendszer szoftverelemei,
- az informatikai rendszer kommunikációs elemei,
- adathordozók,
- az informatikai rendszerre vonatkozó dokumentációk,
- az informatikai rendszerben részt vevő emberi erőforrások.

Rendszer-monitorozó eszközök
Az egész rendszerről gyűjtenek információt, illetve valamilyen csoportosító szempont alapján.

Rendszerprogram (rendszer szoftver)
Olyan alapszoftver, amelyre szükség van, hogy valamely informatikai rendszer hardvereit használhassuk, és az alkalmazói programokat működtessük. A rendszerprogramok legnagyobb részét az operációs rendszerek alkotják.

Rendszerszoftver
A számítógépek működéséhez szükséges, elengedhetetlen, alapvető programok. (pl.: operációs rendszer, víruskereső, e-mail kliens, webböngésző, stb.)

Riasztás
Egy küszöbérték eléréséről (amely hiba megtörténtét vagy valószínű bekövetkezését jelzi) vagy más eseményről (betörési kísérlet, kommunikációs kapcsolat lebontása, stb.) történő jelzés.

Sebezhetőség
Valamilyen támadás esetén az erőforrások sérülésének lehetősége.

Sértetlenség – Integritás
Eredeti teljesség, épség, sértetlenség. Az adat / információ / rendszer hitelességének, pontosságának, teljességének állapota.
A sértetlenséget általában az információkra, adatokra illetve a programokra értelmezik. Az információk sértetlensége alatt azt értjük, hogy az információkat csak az arra jogosultak változtathatják meg, illetve, hogy azok véletlenül nem módosulhatnak. Ez az alap veszélyforrás a programokat is érinti, mivel az adatok sértetlenségét csak rendeltetésszerű feldolgozás és átvitel esetén lehet biztosítani.
A sértetlenség fogalma alatt gyakran értik a sértetlenségen túl a teljességet, továbbá az ellentmondás-mentességet és a korrektséget – együttesen: az integritást. Az integritás ebben az összefüggésben azt jelenti, hogy az információ valamennyi része rendelkezésre áll, elérhető. Korrektek azok az információk, amelyek a valós dologi vagy – pl. modellezésnél – feltételezett állapotot helyesen írják le.

SE-IÜSZ
Mozaikszó, a Semmelweis Egyetem Informatikai Üzemeltetési Szabályzatát takarja.

Sürgősség
Olyan incidens, probléma vagy változtatás üzleti kritikusságának mértéke, amelynek hatása van az üzleti határidőkre. A sürgősség tükrözi a javításra vagy megkerülésre rendelkezésre álló időt, amelyből való kicsúszás hatását az üzlet megérzi. A hatással és talán a műszaki súlyossággal együtt ez a legfőbb eszköz az incidensek, problémák vagy változtatások prioritásának meghatározására.

Számonkérhetőség
Az eseménynaplózás, valamint tágabb értelemben a különböző kontroll-mechanizmusok révén annak biztosítása, hogy a megtörtént események, végrehajtott műveletek, lezajlott eljárások utólag rekonstruálhatóak és elemezhetőek legyenek, azért, hogy az illegális vagy nem megfelelő tevékenységek feltárásra, jelentésre, illetve bizonyításra kerülhessenek.

Szerep
Foglalkozással, feladatkörrel kapcsolatos, illetve az egyéniségből folyó szokásos magatartás. Valamely folyamatban betöltött működési kör, megvalósított feladat, valaminek jutó rész.

Szoftver
Valamely informatikai rendszer olyan logikai része, amely a működtetés vezérléséhez szükséges.

Szerverterem
Szervert és/vagy az IT infrastruktúra szempontjából kiemelkedő fontosságú berendezést (pl. switchet) tartalmazó, és kizárólag ezek tárolásra használt terem.

Szoftverzavar
Nyilvánvalóan hibás szoftverműködés. Pl. „kék-halál”, értelmezhetetlen hibaüzenet.

Szolgáltatási időszak
Azok az időszakok, melyekben egy meghatározott informatikai rendszer vagy szolgáltatás elérhető a felhasználó számára.
Szolgáltatási megállapodás (SLA: Service Level Agreement.)
Részletesen tartalmazza az IT-szolgáltató és ügyfele közötti megállapodásokat az egyes szolgáltatások minőségére (szintjére) vonatkozóan.

Szolgáltatási szint megállapodás (SLA)
Írott megállapodás (szerződés) a felhasználói közösség és az informatikai szolgáltató egység között, amely dokumentálja az elfogadott szolgáltatási szintet valamely informatikai szolgáltatás kapcsán.
Tipikusan kiterjed:
- a szolgáltatási időszakra;
- a szolgáltatás rendelkezésre-állására;
- a felhasználói támogatás szintjére;
- a terminál válaszidőkre;
- a különféle korlátozásokra;
- a funkcionalitásra
- és a katasztrófaszituáció esetén nyújtandó szolgáltatási szintre.

Tartalmazhatja továbbá:
- a biztonsági
- és az esetleges számlázási elveket is.

Szolgáltatási szint menedzsment
Az ügyfeleknek nyújtott szolgáltatási szintek menedzselésének és az elvárt és megvalósított szolgáltatási szintek összevetésének folyamata.

Szolgáltatáskatalógus
Az adott szervezet által másoknak nyújtott szolgáltatások definiálása, dokumentálása, pl. ki az adott szolgáltatás menedzsere, mely munkacsoport felelős érte.

Szolgáltatásmenedzsment
Az üzlet-informatika összehangolás egyik eleme. Az a magas szintű folyamat, amely irányítja az informatikai szolgáltatást az ügyfelek nevében. Jogköre van döntéseket hozni az informatikai szolgáltatás teljes portfoliójának nyújtásáról. Az ITIL úgy tekinti a szolgáltatásmenedzsmentet, mint egy átfogó filozófiát, amely áthatja az egyedi ITIL folyamatok működtetését.

Szolgáltató
Egy szervezet, amely szolgáltatásokat vagy termékeket nyújt vevőknek. A szolgáltató lehet belső vagy külső is.

Teszt-környezet
Itt történnek az éles kiadás terítése előtti tesztelések – az éles környezethez hasonló körülmények között.

Titkosítás
Adatok megváltozatása (lefordítás titkos, nem érthető formába, tárolás ebben a formában, valamint visszaalakítás érhető formába) abból a célból, hogy csak a jogosultak ismerhessék meg az adat tartalmát. (Nem tévesztendő össze a titkos adatkezeléssel.)
Jelen szabályzatban nem teszünk különbséget a rejtjelezés (encipherment) és titkosítás (encryption), illetve a rejtjelmegfejtés (decipherment) és a titkosítás visszafejtése (decryption) között.
TSK – Testnevelési és Sporttudományi Kar

Tulajdonos
Rendelkezési joggal (adott esetben: kizárólagos rendelkezési joggal) bíró természetes vagy jogi személy.
Informatikai értelemben: egy meghatározott informatikai vagyonelem (hardver, szoftver, információ) felett rendelkezési joggal bíró természetes vagy jogi személy.

Tűzfal
Olyan kapcsolódó programok összessége, amelyek egy hálózati átjáró szerveren működve védik a saját (védeni kívánt) hálózat erőforrásait a külső hálózatoktól, illetve ezek felhasználóitól.
A tűzfal célja, hogy a rajta keresztül haladó forgalom engedélyezésén, megtagadásán vagy visszairányításán keresztül naplózza, ellenőrizze és kontrollálja a hálózatokhoz kapcsolódó tevékenységeket.

Ügyfélszolgálat - Help Desk
A kapcsolat az informatika és felhasználói között. Alapfolyamatai az incidenskezelés és a felhasználói igények kezelése, biztosítva, hogy egy hívás (bejelentés) vagy incidens sem marad feldolgozatlanul (nem felejtik el vagy hagyják figyelmen kívül), és hogy a szolgáltatást visszaállítják, amilyen gyorsan csak lehet. Az ITIL új kiadása a segélyszolgálatot kettéosztotta ügyfélszolgálati funkcióra és incidenskezelési folyamatra.

Üzemeltetés-vezető
Az üzemeltetés belső szabályozásában meghatározott értelemben.

Üzemeltetés felügyeleti szoftver
Az informatikai rendszer működésének ellenőrzésére, felügyeletére szolgáló szoftver.

Változás
A menedzselt infrastruktúrában, vagy egy adott szolgáltatás nyújtásához szükséges bármilyen funkcionális egységben bekövetkezett változtatások (több kisebb lépésből álló folyamat) részletes leírása.

Változás-felügyelet
Azok az eljárások, amelyek biztosítják, hogy minden változtatás felügyelt legyen, beleértve a változtatáskérelem benyújtását, naplózását, elemzését, a döntéshozást, jóváhagyást, megvalósítást és a megvalósítás utáni áttekintést is.

Változtatás-kérelem
Az informatikai infrastruktúra bármely összetevőjének vagy az informatikai szolgáltatás bármely jellegének megváltoztatására tett javaslat. Lehet egy dokumentum vagy egy feljegyzés, amelyben szerepel a javasolt változtatás természete, részletei, indoklása és engedélyezése.

Változáskezelés
A változási folyamatok kezeléséhez és dokumentáláshoz nyújt segítséget. Végigkíséri a változásokat azok bejelentésétől a lezárásukig. Több változás projektbe szervezhető és együtt menedzselhető.

Veszélyforrás
Veszélyforrásnak tekintendő mindaz, amelynek hatására, illetve bekövetkeztekor az informatika biztonság sérül: egy vagy több informatikai rendszerelem működésében nem kívánt változás áll be.
A támadás az informatika biztonság valamely pillére ellen ható, valamely veszélyforrásból kiinduló folyamat.

Vírus
Olyan programtörzs, amely illegálisan készült egy felhasználói program részeként. A felhasználói program alkalmazása során átterjedhet, "megfertőzhet" más, az informatikai rendszerben lévő rendszer-, illetve felhasználói programot, sokszorozva önmagát (ami lehet mutáns is) és a logikai bomba hatás révén egy beépített feltételhez kötötten (pl. konkrét időpont, szabad lemezterületi helyek száma stb.) trójai faló hatást indít el.

VPN (Virtual Private Network)
Virtuális magánhálózat. Magánhálózatok összekapcsolása (Site-to-Site VPN), vagy távoli dolgozóknak cégük hálózatához történő kapcsolódása (Remote Access VPN) olyan módon, hogy ennek megvalósításához nyilvános hálózatot (pl. internetet) vesznek igénybe és adataik sértetlenségének, hitelességének és bizalmasságának megteremtésére titkosítást és egyéb védelmet alkalmaznak.

WAN
Wide Area Network. Egy régióra kiterjedő, de gyakran földrészre kiterjedő számítógépes hálózat (pl. Semmelweis Egyetem informatikai hálózata).

Felhasznált irodalom

Muha Lajos: Fogalmak és definíciók: 2.4., In: Muha Lajos (szerk.) Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig., Budapest: Verlag Dashöfer, 2004. pp. 1-37., (ISBN:9639313 12 2)