ÖK - 90 | 2024

HUN REN ÖKOLÓGIAI KUTATÓKÖZPONT

Adatvédelmi és Információbiztonsági Szabályzat

Engedélyezés

Készítő	
Név:	Euline 9001:2001 Kft.
Beosztás:	irányítási szervezet tanácsadó
Dátum:	2024.03.01.

Ellenőrizte		Dokumentum jóváhagyás	
Név:	Karoliny Diána	Név:	Dr. Garamszegi László Zsolt
Beosztás:	ügyviteli osztályvezető	Beosztás:	főigazgató
Dátum:	2024.03.11.	Dátum:	2024.03. 26.

HUN-REN Ökológiai Kutatóközpont HUN REN 1.

Dokumentumtörténet

Verzió	Hatályba lépés / változás dátuma	Módosítás rövid leírása
1.0	2024.03. 26.	Első kiadás

Dokumentum adatvédelmi besorolása

Minősítés
Alap üzleti titok

1. Bevezető és értelmező rendelkezések

A fent nevezett szervezet a továbbiakban „**adatkezelő**”-ként, vagy „HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT”-ként, vagy „szervezet”-ként kerül megnevezésre a jelen szabályzatban.

1.1 A Szabályzat célja

A jelen Adatvédelmi és **Információbiztonsági Szabályzat** (a továbbiakban **IBSZ**) a szervezetnél működtetett informatikai rendszerek tekintetében a biztonsági intézkedéseket szabályozza, meghatározza a számítástechnikai eszközök használatának, az adatkezelés folyamatának biztonsági szabályait, továbbá az informatikai szerepköröket, és előírja az egyes szereplők **informatikai biztonságot érintő feladatait.**

- Szervezetbiztonság - intézkedések
- Kockázatkezelés – kockázati mátrix
- Munkatársaink információbiztonsági szerepe - oktatások
- Fizikai és környezeti biztonság - intézkedések
- Kommunikáció és az üzemeletetés irányítása - szabályzatok
- Hozzáférések – hozzáférési szabályzat, jogosultságok
- Az információs rendszerek beszerzése, fejlesztése, és fenntartása
- Információbiztonsági incidensek kezelése – incidenskezelési módszerek
- Az üzletmenet-folytonoság biztosítása – BCP-DRP

1.2 A Szabályzat hatálya személyi hatálya

Kiterjed a szervezet valamennyi, munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban álló személyekre, valamint azon személyekre, akik –munkatapasztalat-szerzési, kutatási vagy képzési célból – szakmai gyakorlatukat akutatóhelynél töltik (pl.: egyetemi vagy PhD hallgatók, vendégkutatók stb.), (atovábbiakban együttesen: foglalkoztatottak), továbbá minden személyre, aki a szervezeti hatály informatikai vagy azzal összefüggő rendszerét, szolgáltatásait igénybe veszi, informatikai struktúráját és annak eszközeit üzemelteti vagy használja, függetlenül a kutatóhelyhez kapcsolódó jogviszonyától, a vele kötött szerződésben vagy a részére kiadott engedélyben rögzített mértékben, feltéve, hogy a keretszabályzat tartalmát számukra megismerhetővé tették.

1.2.1 Informatikai és Információbiztonsági Szabályzat és Irányelvek Felhasználóknak

A jelen IBSZ előírásai alaján a szervezetnek egy „kivonatot” készít a munkavállalói részére, amely a munkatársakra vonatkozó legfontososabb követelményeket és előírásokat rögzíti.

1.2.2 Informatikai és Információbiztonsági Szabályzat külsős partnerek részére

Szükség esetén a szervezet a külsős pratnerek részére is kivonatot készít az őket érintő információbiztonsági kérdésekben, illetve a szerződéses pontokban rögzíti azokat!

*1.3*A Szabályzat tárgyi hatálya

- A szervezeténél lévő adatok teljes körére, keletkezésük, felhasználásuk, feldolgozási helyük és megjelenési formájuktól függetlenül, továbbá bármely szervezeti egység birtokában szereplő hardver- és szoftver eszközre, beleértve az eszközök műszaki dokumentációját is.
- A szervezet tulajdonában lévő, vagy általuk tárolt valamennyi informatikai berendezésre, beleértve a berendezések műszaki dokumentációját is;
- A rendszerprogramokra és a felhasználói programokra;
- A védelmet élvező adatok teljes körére, keletkezésük és felhasználásuk, valamint feldolgozásuk helyétől, továbbá a megjelenési formájuktól függetlenül;
- Az adathordozókra, azok tárolására és felhasználására, beleértve a feldolgozásra beérkezés és a felhasználókhoz történő eljuttatás folyamatait is;
- Az informatikai folyamatban szereplő valamennyi dokumentációra;
- Az adatok felhasználására vonatkozó utasításokra.

*1.4*A szabályzat alkalmazása

Az **IBSZ** rendelkezéseit minden létesített informatikai rendszer esetében és az információbiztonság tekintetében teljes körűen alkalmazni kell.

Az **IBSZ** gazdája köteles gondoskodni a szabályzat aktualizálásáról, naprakészen tartásáról és meghatározott rendszerességgel a felülvizsgálati eljárás szerinti felülvizsgálatáról. Ez vonakozik minden információbiztonsághoz kapcsolódó dokumentumra, szabályzatra!

A felülvizsgálat során, a gyakorlati tapasztalatok, az előfordult biztonsági események, a jogszabályi környezet változásai, a technikai fejlődés, az alkalmazott új informatikai eszközök, új programrendszerek, fejlesztési és védelmi eljárások, stb. miatt szükségessé váló módosításokat el kell végezni.

- figyelembe kell venni a szervezeti követelmények és prioritások változásait,
- meg kell fontolni az új fenyegetéseket és sebezhetőségeket,
- visszaigazolást kell szerezni arról, hogy az óvintézkedések hatékonyak és megfelelőek maradtak-e.

Rendkívüli felülvizsgálatot kell tartani, ha:

- az informatikai biztonságot, valamint az IBSZ tartalmát érintő jelentős változás következett be;
- a jogszabályi környezetben jelentős változás következett be;

- új, lényeges kockázatok válnak ismertté;
- súlyos informatikai biztonsági incidens következett be.

*1.5*Érvényesítés

A HUN-REN ÖKOLÓGIAI KUTATÓKÖZPONT megköveteli munkavállalóitól, a partnerektől és a felhasználó harmadik felektől, hogy az információbiztonságot a szervezet által az **IBSZ**-ben (és kapcsolódó dokumentumokban) rögzítetteknek, valamint a további vonatkozó külső-belső szabályzatokban leírtaknak megfelelően alkalmazzák.

Az **IBSZ** jóváhagyásáért, valamint kidolgozásának és alkalmazásának elrendeléséért az **első számú vezető** a felelős. Az információbiztonsági tevékenységek koordinálásáért felelősöket jelöl ki!

*1.6*Az IBSZ kapcsolódó dokumentumai

Az **IBSZ**-t a terjedelme, rugalmas használata és az áttekinthetősége miatt további szabályzatokra osztható fel, amelyek az **IBSZ** elengedhetetlen részei, vele együtt kell kezelni egységben. Ezekről **a dokumentum végén** kötelező listát kell vezetni, illetve szükség szerint azokat is pubikálni az érintettek felé.

Legfontosabb *felhasználói alapdokumentum a* ***„Munkavállalói Nyilatkozat”****, melyet minden munkatársnak kötelező aláírnia és betartania, aki az adatvédelem és információbiztonság hatálya alá tartozik.*

2.Alapelvek

A szervezet által kezelt adatok védelmét a bizalmasság, sértetlenség és a rendelkezésre állás szempontjából úgy kell megvalósítani, hogy az információk és informatikai környezetének védelme folytonos, teljes körű, zárt, valamint a kockázatokkal arányos legyen.

A védelem zártsága akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni védelmi intézkedések megvalósulnak. A védelem akkor kockázatarányos, ha az informatikai rendszerek által kezelt adatok védelmének erőssége és költségei a felmért kockázatokkal arányban állnak.

Ezeknek megfelelően a szervezetben az információbiztonsági szempontból az a legfontosabb, hogy a szervereket megfelelően védjék a sértetlenség, a rendelkezésre állás és a bizalmasság tekintetében, mivel az összes fontos információt itt kezelik.

Az informatikai eszközök és rendszerek folyamatos működőképessége és a biztonsági követelmények érvényesülése elsőrendű szervezeti érdek, így minden érintett kötelessége ennek szellemében tevékenykedni.

Az információbiztonság kialakítását és működtetését befolyásolják a szervezet igényei és céljai, biztonsági követelményei, a működtetett szervezeti folyamatok, valamint a szervezet mérete és felépítése.

A szervezet informatikai rendszereire és annak működtetésére vonatkozó szabályok és előírások maguk is védendő információk, ezért az **IBSZ-t nyilvánosan nem terjesztendőként** kell kezelni.

3. Szoftverhasználói Politika

A szoftverek használatát illetően a szervezet a következő Szoftverhasználói Politikát követi:

A szerzői jog által védett számítógépes szoftverek illegális használata és másolása törvénybe ütköző cselekedet, és ellenkezik a szervezet Szoftverhasználói Politikájával. Az ilyen jellegű szoftvermásolást helytelenítjük és elítéljük, ezért ennek megakadályozására a szervezet a következő alapelveket fogadja el:

- Semmilyen körülmények között nem ösztönözzük, és nem tűrjük el az illegális szoftvermásolatok készítését vagy használatát.
- Minden indokolt szoftverigény kielégítésére a szervezet jogtiszta szoftvert biztosít az összes számítógépre, a megfelelő időben, és a szükséges mennyiségben.
- Eleget teszünk minden olyan licence vagy vásárlási feltételnek, amely az általunk beszerzett vagy használt szoftverek felhasználását szabályozza.

4. Szakkifejezések és meghatározásuk

Az IBSZ, a keretszabályzat szakkifejezés-készletre épül. A *Szabályzatban* leírtak értelmezéséhez és annak alkalmazásához ezen szakkifejezések ismerete és következetes értelmezése elengedhetetlen.

E dokumentumra a következő szakkifejezések és meghatározások érvényesek:

- (1) alapvető adat: a kutatóhely szempontjából jelentős értékkel bíró információs

  adatvagyonelem; alapvető adatok különösen: személyes adatok, üzleti titkok,

  államháztartással vagy gazdálkodással kapcsolatos adatok, továbbá azok az adatok, amelyeket a kutatóhely vezetője vagy az adatgazdák alapvető adatnak nyilvánítanak (pl.: nem nyilvános új kutatási vagy tudományos adatok);
- (2) alapvető információs eszköz: olyan eszköz, amely alapvető adatot kezel, vagy alapvető információhoz biztosít hozzáférést (vagy azon eszközök, melyek az alapvető adatok információs vagyonához vannak rendelve);
- (3) alapvető szolgáltatás: alapvető információs eszköz szolgáltatása;
- (4) alkalmazás: meghatározott célfeladatot megvalósító szoftverekkel nyújtott szolgáltatás, amely támogatja a feladatellátással összefüggő és a szervezeti folyamatok lebonyolítását, valamint az azokhoz szükséges adatok, információk rendszerezett tárolását, feldolgozását és visszakereshetőségét;
- (5) bizalmasság: az információs eszköz azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a

jogosultságuk szintje szerint ismerhetik meg, használhatják fel, továbbá rendelkezhetnek a felhasználásáról;

- (6) biztonsági esemény: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az információs adatvagyonban kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az információs eszköz által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész vagy megsérül;
- (7) célnak megfelelő használat biztosítása: az adat kezelésének, valamint az információs eszköz ezzel összefüggő funkciójának megvalósíthatósága;
- (8) HUN-REN Központ: központi finanszírozású, a HUN-REN Kutatóhálózat irányítására és működtetésére létrehozott, az Országgyűlés által alapított központi költségvetési szerv;
- (9) észlelés: a biztonsági esemény bekövetkezésének felismerése;
- (10) felhasználó: a kutatóhely információs adat- és eszközvagyonához hozzáférő természetes személy vagy természetes személyhez közvetlenül nem köthető gépi ügyfél (technikai felhasználó);
- (11) felhasználói dokumentáció: az információs eszköz, annak eleme vagy a rendszerszolgáltatás biztonságos és hatékony használatának módszereit tartalmazó leírás;
- (12) fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az információs adatvagyon vagy az információs eszköz biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az információs adatvagyon biztonságát;
- (13) fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az előerős védelem, a beléptetőrendszer, a megfigyelőrendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;
- (14) folytonos védelem: az időben változó körülmények és viszonyok között is megszakítás nélkül megvalósuló védelem;
- (15) hitelesség: annak bizonyossága, hogy az adat egy elvárt forrásból származik;
- (16) informatikai biztonsági incidens: olyan informatikai biztonsági esemény, amely bekövetkezése esetén az alapvető adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, bizalomvesztés következhet be az érintett szervezettel szemben;
- (17) informatikai veszélyhelyzet (katasztrófahelyzet): olyan informatikai üzemzavar, amely nem szüntethető meg az elvárt visszaállítási időn belül, vagy nyilvánvalóan katasztrófahelyzet alakult ki (tűz, robbanás stb.);
- (18) információs adatvagyon: a kutatóhely által, annak tevékenységi körében kezelt kutatási adatok, valamint a kutatóhely által, annak jogszerű működése során kezelt adatok összessége;
- (19) információs eszköz: az információs eszközvagyon egy eleme; Az Ibtv. hatálya alá tartozó kutatóhelyek esetében az információs eszköz szélesebb körben értelmezendő, az elektronikus információs rendszer értendő alatta.
- (20) információs eszközvagyon: a kutatóhely által vagy annak érdekében működtetett informatikai eszközök (hardver, szoftver,

kommunikációs hálózat), ezen informatikai eszközök által nyújtott vagy igénybe vett szolgáltatások, valamint a kutatóhely által igénybe vett külső (pl.: felhőalapú) informatikai szolgáltatások összessége;

- (21) kockázat: a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ez által okozott kár nagyságának a függvénye;
- (22) kockázatelemzés: az információs adatvagyon értékének, sérülékenységének (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek gyakoriságának felmérése útján a kockázatok feltárása és értékelése;
- (23) kockázatokkal arányos védelem: az információs eszköz vagy adat olyan mértékű védelme, amelynek költségei arányosak a fenyegetések által várhatóan okozható károk összesített mértékével;
- (24) kutatóhely vagy kutatóhelyek: a HUN-REN kutatóközpontjai és önálló kutatóintézetei, valamint a HUN-REN Központ;
- (25) kriptográfia (titkosítás): az adatok valamely matematikai algoritmus szerinti megváltoztatása abból a célból, hogy csak a jogosultak ismerhessék meg azok tartalmát; a kriptográfia valamely adat sértetlenségének és hitelességének a bizonyítására is szolgál;
- (26) letagadhatatlanság: az adat származásának ellenőrizhetősége, bizonyossága;
- (27) logikai védelem: az információs adatvagyonban információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;
- (28) meghibásodás: minden olyan felhasználói számítógépet érintő hiba vagy a hálózati eszközök, valamint központi munkaállomások rövid idejű leállása, amely számottevően nem zavarja a normális munkavégzést, és a napi üzemeltetési feladatok során gyorsan kijavítható;
- (29) méretarányosság: az információbiztonsági védelmi intézkedések adott szervezet méretéhez, műszaki és gazdasági lehetőségeihez, valamint személyi erőforrásaihoz illeszkedő megvalósítása;
- (30) reagálás: bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedés;
- (31) rendelkezésre állás: az információs eszközök szolgáltatásai, valamint az ezek által kezelt adatok az arra jogosultak számára a szükséges időben elérhetők;
- (32) sértetlenség: az adat azon tulajdonsága, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, valamint az információs eszköz azon tulajdonsága, hogy az rendeltetésének megfelelően használható;
- (33) sérülékenységvizsgálat: az információs adatvagyon gyenge pontjainak (biztonsági rések) és az ezeken keresztül fenyegető biztonsági eseményeknek a feltárása;
- (34) személyes adat: az Info tv. által a személyes adatok körébe sorolt adat vagy információ;
- (35) teljes körű védelem: az információs eszköz valamennyi elemére kiterjedő védelem;

- (36) törzsadat: olyan kiegészítő adatok, melyek az objektumok azon tulajdonságait írják le, melyek menet közben jellemzően nem változnak;
- (37) zárt védelem: az összes számításba vehető fenyegetést figyelembe vevő védelem.

5. Titoktartási megállapodások

A titoktartási megállapodás arra szolgál, hogy kötelezzen az adott információ bizalmasságának, vagy titkosságának megtartására. Az alkalmazottak, munkatársak rendszerint az ilyen megállapodást alkalmazásuk feltételei keretében írják alá.

A munkavállalóinkkal a „Munakvállalói Nyilatkozat” tartalmazza a titoktartásra vonatkozó részeket.

Alkalmi munkaerőnek és a külső fél felhasználóinak, munkatársainak, akikről a meglévő, a titoktartási megállapodást is tartalmazó szerződés nem intézkedik, külön titoktartásra vonatkozó megállapodást kell aláírniuk, még mielőtt az információ-feldolgozó eszközökhöz hozzáférést nyernének.

A titoktartási megállapodást felül kell vizsgálni a megfelelőség tekintetében, ha az alkalmazási feltételek megváltoznak, különösen pedig akkor, amikor az alkalmazottak arra készülnek, hogy kilépjenek a munkahelyükről, vagy ha közeleg az alvállalkozói vagy munkaszerződések lejárta.

6. Szerződések

6.1 Beszállítói és szolgáltatói szerződések

Bizonyos beszállítónak, és egyes munkatársainak külön-külön titoktartási nyilatkozatot kell tennie a szerződésben, vagy különálló dokumentumban, amelyben a beszállító felelősséget vállal arra, hogy az általa szállított megoldásokról, illetve az ágazatból tudomására jutott egyéb információkról nem ad tájékoztatást harmadik félnek.

Bizonyos szolgáltatói szerződésekben meg kell határozni a határozni a garanciára, a támogatásra, szolgáltatásra, az SLA-ra vonatkozó, illetve a szolgáltatói fél rendelkezésre állásának követelményeit, valamint a szolgáltatás tárgyát képező eszközökkel kapcsolatos rendelkezésre állási követelményeket. Szükség esetén ki kell térni a szellemi tulajdonjogok tisztázására.

A szerződéskötést megelőzően, ahol lehetséges, ott szolgáltatásonként kontrollokat kell felállítani, minimális kontrollok az alábbiak:

- Szolgáltatás minőségére vonatkozó kontrollok.
- A szolgáltatás rendelkezésre-állása (Pl.: Internet esetén kiesett órák száma).
- A szolgáltatás minősége (Pl. Internet esetén sávszélesség).
- A szolgáltató megbízhatóságára vonatkozó kontrollok.
- A szolgáltató rendelkezésre állása.
- A szolgáltató együttműködési készsége.
- A szolgáltató szakmai kompetenciája.

7. Adatvagyon

Az adatvagyon besorolásának célja a szervezeti vagyon védelmének megfelelő fenntartása.

7.1 Személyes adatok az adatvagyonban

A jelen IBSZ a GDPR Rendelet megfelelését is figyelembevéve a következő elvet alkalmazza, miszerint a kezelt ***személyes adatokat tartalmazó adatvagyonok külön besorolás nélkül alapesetben a BIZALMAS, illetve különleges személyes adatok esetében SZIGORÚAN BIZALMAS kategóriában*** vannak.

7.2 Felelősök

Az információkkal kapcsolatos kockázatok értékeléséért az **információbiztonságért felelős személy felel**, az alkalmazandó kontroll és hozzáférési korlátozások szintje a jogosultási rendszerben meghatározott .

7.2.1 Besorolási irányelvek

Feltétel	Magyarázat
Bizalmasság	Annak biztosítása, hogy az információ csak a hozzáférésre jogosítottak számára legyen hozzáférhető.
Sértetlenség	Az információ pontosságának és teljességének biztosítása
Rendelkezésre állás	Annak biztosítása, hogy a hozzáférési jogosultságokkal rendelkezők akkor férjenek hozzá az információkhoz, amikor szükséges.

7.2.2 Bizalmasság

Szint	Értéke	Meghatározás
Szigorúan bizalmas	**9**	Azon információk, amelyek közreadása a szervezetre, üzleti partnereire, alkalmazottjaira, ügyfeleire jelentős kedvezőtlen hatást gyakorolhatna. (pl.: üzleti titokkal, banktitokkal kapcsolatos adatok, nem nyilvános pénzügyi kimutatások)
Bizalmas	**6**	Olyan, érzékenynek tekintendő információk, amelynek közzététele kedvezőtlen hatást gyakorolhatna a szervezet szervezeti egységeire, üzleti partnereire alkalmazottjaira, ügyfeleire. Ebbe a körbe a szigorú nemzeti jogi szabályok (például adatvédelmi törvények) által szabályozott információk tartoznak. (pl.: béradatok, szerződések feltételei)
Belső használatra	**3**	Minden egyéb olyan adat, amely nem tartozik a bizalmas és a szigorúan bizalmas adatok körébe. A szervezet tulajdonát alkotó adatok. Jóllehet engedély nélküli közzétételük szabályellenes,

		mégse gyakorolna kedvezőtlen hatást a szervezetre, üzleti partnereire, alkalmazottjaira, ügyfeleire. (pl.: céges telefonszámok)
Nyilvános	**1**	A nyilvános forrásokból származó adatok. A szervezet által a nyilvánosság rendelkezésére bocsátott adatok. (pl.: közzétett vállalati pénzügyi kimutatások)

7.2.3 Sértetlenség

Szint		Meghatározás
Magas	**9**	Abszolút pontosságot és a legmagasabb fokú ellenőrzést igénylő információk. Ha az ilyen adatok pontatlannak bizonyulnak, ez jelentős és kedvezőtlen hatást gyakorolhatna a szervezetre, üzleti partnereire, alkalmazottaira, ügyfeleire. (pl.: üzleti titokkal, banktitokkal kapcsolatos adatok, jelentős pénzügyi kimutatások)
Közepes	**3**	Mindazon adatok, amelyek esetében nem fontos az abszolút pontosság, de amelyek pontatlanságával kapcsolatosan jelentős, de korlátozott kockázat merül fel. (pl.: alkalmazottak személyes adatai)
Alacsony	**1**	Mindazon adatok, amelyek esetleges pontatlansága nem jár jelentős kockázattal. (pl.: belső kiadványok)

7.2.4 Rendelkezésre állás

Szint		Meghatározás
Magas rendelkezésre állás	**9**	Mindazon adatok, amelyek rövid ideig tartó elérhetetlensége jelentős pénzügyi veszteséget vagy jogkövetési problémákat okozhat. (pl.: üzleti titokkal, banktitokkal kapcsolatos adatok)
Közepes rendelkezésre állás	**3**	Mindazon adatok, amelyek korlátozott ideig tartó elérhetetlensége elfogadható mértékű kockázathoz vezet. (pl.: béradatok, pénzügyi adatok)
Alacsony rendelkezésre állás	**1**	Mindazon adatok, amelyek hosszabb ideig tartó elérhetetlensége nem érinti az üzleti tevékenységet. (pl.: belső közlemények)

7.3 Védelmi besorolás

7.3.1 Adatvagyon értékének számítása

A 7.3.1, a 7.3.2 és a 7.3.3 táblázatokban megállapított értékek szorzata az adatvagyon értéke. Ezt az értéket kell figyelembe venni a védelmi besorolás osztályozásánál.

7.3.2 Az adatvagyon védelmi besorolása

Védelmi osztály	Alkalmazás	Meghatározás	Érték
A	Kiemelten értékes	Stratégiai adatokat (pl. forráskódok), nem nyilvános pénzügyi adatokat és egyéb üzleti és banktitkot kezelő rendszer, alkalmazás	27-22
B	Értékes	Személyes adatokat kezelő rendszer, alkalmazás	21-15
C	Közepesen értékes	Belső használatra besorolású adatokat kezelő rendszer, alkalmazás	14-9
D	Alacsony értékű	Nyilvános adatokat kezelő rendszer, alkalmazás	8-0

7.3.3 Eszközök

Védelmi osztály	Meghatározás
A	Speciális hardver
B	Speciális rendszerszoftver
C	Egyéb hardver, rendszerszoftver, irodatechnikai eszköz
D	Közterületen elhelyezett, üzemeltetett eszköz

A hardver és szoftver, illetve irodatechnikai eszközök besorolása meghatározza, hogy az adott eszköz és bizalmasságát és sértetlenségét mennyire kell védeni.

7.3.4 Helyiségek

Védelmi osztály	Meghatározás
A	Szerverszoba, internetet és hálózati kapcsolatot biztosító helyiség
B	Telekommunikációs csomópontok
C	Irodahelységek
D	Tárgyaló

A helyiségek osztályozásánál a helységben végzett tevékenység, az ott található eszközök, valamint az eszközök funkciója, azok adattartalma figyelembevételével kell a védelmi szintet meghatározni.

7.4 Vagyonelemek adatkezelése

7.4.1 „Kiemelten értékes” besorolású információk

Tevékenység	Eszköz	Kezelési eljárás
Másolás	Minden	Az adatok másolásához az adatvagyon gazdájának engedélye szükséges és csak felügyelet és ellenőrzés alatt végezhető.
Tárolás	Elektronikus	Az adatokat biztonságos és meghatározott személyek által hozzáférhető hálózati területeken kell tárolni. Az információ csak logikai védelem és titkosítás alatt tárolható laptopon vagy más hordozható eszközön.
	Fizikai	Az információt biztonsági területen, vagy a szervezet épületein belül zárt szekrényekben kell tárolni. Ezzel egyenértékű biztosításról kell gondoskodni, ha az adatok külső felek birtokában vannak. A külső feleknek titoktartási szerződést kell aláírniuk.
Továbbítás	Postai	Kettős, lezárt borítékban, ajánlott küldeményként vagy hasonló formában elküldve
	E-mail	Az információt titkosított, jelszóval védett formában kell továbbítani
	Szóban	Tilos
Megsemmisítés	Papír	Az adatokat felügyelet alatt zúzógépben kell megsemmisíteni.
	Adathordozó	Az adatokat törölni kell az adathordozóról, és a megsemmisítést és vagy formattálást akkor kell elvégezni, ha az adatok már nem szükségesek.

7.4.2 „Értékes” besorolású információk

Tevékenység	Eszköz	Kezelési eljárás
Másolás	Minden	Az adatok másolásához az adatvagyon gazdájának engedélye szükséges és csak felügyelet és ellenőrzés alatt végezhető.
Tárolás	Elektronikus	Az adatokat biztonságos és meghatározott személyek által hozzáférhető hálózati területeken kell tárolni. Az információ csak logikai védelem és titkosítás alatt tárolható laptopon vagy más hordozható eszközön.
	Fizikai	Az információt biztonsági területen, vagy a szervezet épületein belül zárt szekrényekben kell tárolni. Ezzel egyenértékű biztosításról kell gondoskodni, ha az adatok külső felek birtokában vannak. A külső feleknek

		titoktartási szerződést kell aláírniuk.
Továbbítás	Postai	Kettős, lezárt borítékban, ajánlott küldeményként vagy hasonló formában elküldve
	E-mail	Az információt titkosított, jelszóval védett formában kell továbbítani
	Szóban	Tilos
Megsemmisítés	Papír	Az adatokat felügyelet alatt zúzógépben kell megsemmisíteni.
	Adathordozó	Az adatokat törölni kell az adathordozóról, és a megsemmisítést és vagy formattálást akkor kell elvégezni, ha az adatok már nem szükségesek.

7.4.3 „Közepesen értékes" besorolású információk

Tevékenység	Eszköz	Kezelési eljárás
Másolás	Minden	Az adatok másolásához az adatvagyon gazdájának engedélye szükséges.
Tárolás	Elektronikus	Az adatokat biztonságos és meghatározott személyek által hozzáférhető hálózati területeken kell tárolni. Az információ másolata tárolható laptopon vagy más hordozható eszközön.
	Fizikai	Az információt a szervezet épületein belül kell tárolni. Szerződés esetén az adatok külső feleknél is tárolhatóak.
Továbbítás	Postai	Ajánlott küldeményként vagy hasonló formában elküldve
	E-mail	Az információt továbbítása engedélyezett.
	Szóban	Az információt továbbítása engedélyezett.
Megsemmisítés	Papír	Az adatokat zúzógépben kell megsemmisíteni.
	Adathordozó	Az adatokat törölni kell az adathordozóról, és a megsemmisítést és vagy formattálást akkor kell elvégezni, ha az adatok már nem szükségesek.

7.4.4 „Alacsony értékű" besorolású információk

Tevékenység	Eszköz	Kezelési eljárás

Másolás	Minden	Engedélyezett, nincs korlátozás
Tárolás	Elektronikus	Engedélyezett, nincs korlátozás
	Fizikai	Engedélyezett, nincs korlátozás
Továbbítás	Postai	Engedélyezett, nincs korlátozás
	E-mail	Engedélyezett, nincs korlátozás
	Szóban	Engedélyezett, nincs korlátozás
Megsemmisítés	Papír	Engedélyezett, nincs korlátozás
	Adathordozó	Engedélyezett, nincs korlátozás

7.5 Alkalmazások kezelése

Védelmi osztály	Hozzáférés	Tárolás	Mentés
A	Felhasználói azonosító/Jelszó a megfelelő jogosultsággal	Logikai védelem alatt	Zárt helyen, titkosítva
B	Felhasználói azonosító/Jelszó a megfelelő jogosultsággal	Meghatározott eszközökön	Zárt helyen, titkosítva
C	Felhasználói azonosító/Jelszó a megfelelő jogosultsággal	Meghatározott eszközökön	Belső eszközökön
D	Publikus	Publikus	Publikus

7.6 Helységek kezelése

Védelmi osztály	Helység védelme
A	Mechanikai és/vagy elektronikus védelemmel ellátott zárt terület
B	Mechanikai és/vagy elektronikus védelemmel ellátott zárt terület
C	Mechanikai és/vagy elektronikus védelemmel ellátott terület
D	Nem védett terület

7.7 Eszközök kezelése

Védelmi osztály	Eszköz védelme

A	Mechanikai és/vagy elektronikus védelemmel ellátott zárt terület
B	Mechanikai és/vagy elektronikus védelemmel ellátott zárt terület
C	Mechanikai és/vagy elektronikus védelemmel ellátott terület
D	Nem védett terület

7.8 SW és HW adatvagyon

- **szoftver-vagyon:** alkalmazási szoftverek, rendszerszoftver (SW leltár)
- **IT vagyontárgyak:** adatkezelésre alkalmas eszközök (tárolás, továbbítás, írás, olvaás), így számítógépek, laptopok, telefonok, adattovábbítú óeszközök, infokommunikációs eszközök

Ezekrül külön naprakész leltárt kell vezetni, illetve az adatvagyonok kezelési, előfordulási és alkalmazási helyeinek HW és SW alapján összerendelhetőnek kell lennie a kezelt információs adatvagyonnal.

8. Kockázatkezelés

A kockázatok felmérésének első lépéseként elkészítjük, illetve felülvizsgáljuk az ADATOKRA és INFORMÁCIÓKRA vonatkozó „Vagyonleltár”-t, amelyben pontosan meghatározásra kerül az információs adatvagyon értéke és azok a lehetséges pontok, ahol az adatvagyon a keletkezés/tárolás/felhasználás/továbbítás helyén ténylegesen sebezhető.

Ezt követően történik a tényleges, valós kockázatok felmérése és értékelése, amely a „Kockázati mátrix”-ban kerül dokumentálásra, így ezáltal a kockázatkezelési módszer képes lesz összehasonlítható és megismételhető eredmények előállítására.

A kockázatok felmérésének menete:

1. A lehetséges támadási pontok és a lehetséges fenyegetések mátrixba rendezése és a VALÓS kockázatok feltérképezése.
2. A mátrix alapján megállapított fenyegetések bekövetkezési **gyakoriságának** megállapítása, a táblázatban szereplő értékek segítségével:
3. A sérülékeny pont védelmének átvizsgálása az adott fenyegetésre vonatkozóan.
4. A sérülékeny pont átvizsgálásának eredményének dokumentálása az adott fenyegetés tekintetében. Lehetséges károk, hatások megállapítása
5. A fenti vizsgálat eredményeképpen meghatározni, hogy a fenyegetés milyen **valószínűséggel használhatja** ki a sérülékeny pontot.
6. Átvizsgálni a hatásokat, vagyis ha a bekövetkezett fenyegetés kihasználja a sérülékeny pontot, az milyen hatással lehet az ott kezelt adatvagyonok bizalmasságára, sértetlenségére és rendelkezésre állására külön-külön meghatározva.
7. Az átvizsgálás során be kell vonni az elkészült *„Vagyonleltár”* információit!

8. A fenti vizsgálat eredményeképpen meghatározni megállapítani a **hatás mértékét.**
9. A sebezhetőségek átvizsgálása és pontos meghatározása után lehet megállapítani a bekövetkezés lehetőségeinek figyelembevételével az okozott hatások mértékét.
10. Az adott sérülékeny pontra vonatkozó **kockázati érték kiszámítása**, az adott fenyegetés tekintetében = a támadás bekövetkezési **gyakorisága** X a **támadás eléri a támadható felületet** X **okozható hatás mértéke.**
11. Az értékek megállapítását és a számításokat és az összes sérülékeny pontra vonatkozóan meg kell határozni a konkrét felmért fenyegetések tekintetében.
12. A maradványkockázat kiszámítása a meghatározott intézkedések figyelembevételével történik a fent meghatározott lépések alapján.

A teljes folyamat a kockázati-mátrixban kerül dokumentálásra.

A Szervezetünk-nél az intézkedéseket úgy hozza meg az első számú vezető, hogy annak költségei egyensúlyban vannak a biztonsági meghibásodásokból valószínűleg származó üzleti veszteségekkel. A vezetőség mielőtt dönt egy kockázat javításáról, meghatározza, hogy a kockázatok elfogadhatók vagy nem. A kockázatok elfogadhatók, ha pl. úgy értékelik, hogy a kockázat csekély vagy a kezelés nem lenne költséghatékony a szervezet számára.

Azokra a kockázatokra, ahol a kockázatjavítási határozat az volt, ott megfelelő intézkedéseket kell a vezetőségnek megfogalmaznia. Az alkalmazott intézkedések biztosítják, hogy a kockázatok egy elfogadható szintre csökkenjenek.

A *kockázati-mátrix* kockázatjavítási tervében pontosan megállapításra kerül, hogy melyik **sérülékeny pontra** és melyik vonatkozó **fenyegetésre** hozunk intézkedési tervet. Ezt követően a következő pontok kerülnek meghatározásra:

- Támadható felület és a támadás jellege
- Státusz
- A sérülékeny pont átvizsgálásának eredménye a fenyegetés tekintetében. Lehetséges károk, hatások
- A támadás bekövetkezési gyakorisága
- Valószínűsége annak, hogy a bekövetkezett támadás eléri a támadási felületet
- Hatás mértéke
- Kockázati érték számítása Határérték: 81 felett
- Kockázatkezelés változata
    - A kockázat vállalása (V)
    - A kockázat elkerülése (E)
    - A kockázati forrás megszűntetése (MSZ)
    - A kockázat valószínűségének megváltoztatása (VV)
    - A kockázat következmények megváltoztatása (KV)
    - A kockázat áthárítása (ÁT)

- Intézkedési terv
- Intézkedési terv elfogadása dátum
- Eredeti kockázat értéke (legmagasabb érték)
- Maradvány kockázat értéke
- Magyarázat a maradványkockázat alakulására
- Szükséges erőforrások
- Várható teljesülés
- Felelősök
- Eredmények értékelése

9. Oktatások, képzések, az információbiztonság tudatosítása

Gondoskodni kell arról, hogy a felhasználók tudatában legyenek az informatikai biztonságot fenyegető és egyéb figyelmet igénylő tényezőknek, továbbá fel kell készíteni őket arra, hogy a szervezet biztonsági irányelveiben előírtakat szokásos napi munkájuk során betartsák.

A felhasználókat ki kell oktatni a biztonsági eljárásokról és az információ-feldolgozó eszközök helyes használatáról a lehetséges biztonsági kockázat minimalizálása érdekében.

Az informatikai biztonsággal összefüggő feladatokról rendszeresen központi és helyi szintű oktatásokat, illetve továbbképzéseket kell tartani. Az oktatások, képzések megszervezése az **információbiztonságért felelős személy** feladata. Az oktatások szakmai anyagának kidolgozása, a szükséges szakirodalom biztosításában segítséget nyújt az **IT üzemeltetést végző munkatárs.**

Az információbiztonsági biztonsági oktatásoknak, képzéseknek a következő témaköröket ajánlott lefedniük:

- általános információbiztonsági biztonsági oktatás (jelszómenedzsment, e-mail, Web etikus használata, az információ-feldolgozó és kommunikációs eszközök biztonságos használata, információbiztonsággal kapcsolatos előíró dokumentumok ismerete, stb.), minden új és minden hasonló oktatáson eddig részt nem vett felhasználó részére;
- vírusvédelemmel és a vírusvédelmi rendszerekkel kapcsolatos oktatás minden új, és eddig oktatáson részt nem vett felhasználó részére;
- a biztonsági események jelentésével, kezelésével kapcsolatos oktatás minden új, és eddig oktatáson részt nem vett felhasználó részére;
- új, bevezetésre kerülő rendszerekkel kapcsolatos biztonsági oktatás minden, a rendszer bevezetésében érintett felhasználó körében;
- az IT Akcióterv oktatása minden új, és eddig oktatáson részt nem vett felhasználó részére (csak a **tervben meghatározott feladataikra korlátozva**);

Az oktatásokon való részvételről az **adatvédelmi megbízottnak** nyilvántartást kell vezetnie, amely nyilvántartásokon a résztvevők aláírásukkal kötelesek tanúsítani megjelenésüket.

10. Belső személyzet információbiztonsága

Az **informatikai biztonság betartandó előírásait „Informatikai és Információbiztonsági Szabályzat és Irányelvek Felhasználóknak" szabályzat tartalmazza, illetve a „Munkavállalói Nyilatkozat"**, melynek **tudomásulvétele és aláírása az alkalmazás feltétele**.

10.1 A felhasználók jogai

Részletesen az ***Informatikai és Információbiztonsági Szabályzat Felhasználóknak*** dokumentumban került meghatározásra.

10.2 A munkakörök szétválasztása

A munkakörök szétválasztása az a módszer, amely minimalizálja a véletlen és a szándékos visszaélésekből, károkozásból eredő kockázatot. Meg kell vizsgálni az egyes munkakörök szétválasztását annak megfelelően, hogy egyes munkakörök vezetői feladatokat mások végrehajtói feladatokat fedjenek, illetve a feladat-, hatás-, és felelősségi-köröket annak érdekében, hogy az információ jogosulatlan módosításához vagy visszaéléshez vezető lehetőségek esélyét csökkentsük.

Különösen figyelni kell arra, nehogy csalást követhessenek el olyan munkatársak, akik kizárólagos felelősséggel, egyedül járnak el bizonyos ügyekben, illetve ne maradhasson felfedezetlen, ha mégis csalás történik. Bármely szervezeti (ügyviteli, gazdasági) esemény kezdeményezésének, függetlennek kell lenni az azt engedélyező lépésektől. A következő ellenőrzési mechanizmusok bevezetését kell megvizsgálni az egyes helyeken:

- Fontos az olyan tevékenységek elválasztása, amelyek összejátszással járhatnak azért, hogy megakadályozzuk az esetleges csalásokat, például megrendelés feladását és a beérkezett termékek átvételét ne végezhesse ugyanaz a személy.
- Ha fennáll az összejátszás veszélye, akkor olyan ellenőrzési mechanizmust kell kialakítani, amelyben két vagy három személynek kell részt vennie azért, hogy ezzel csökkenjen az összejátszás lehetősége.

10.3 IBIR csoport létrehozása

Az IBIR csoportnak az információbiztonság összehangolása során figyelembe kell vennie a szakértői jártasságot olyan területeken, mint jogi kérdések, információbiztonság, kibervédelem, IT technikai megoldások, rendszerszervezés vagy kockázatkezelés, ezért ennek megfelelően kell kiválssztani a csoport tagjait, akik külsős szerződéses jogviszonyban is alkalmazhatók.

Az IBIR csoport feladata:

- biztosítani, hogy a biztonsági tevékenységeket megfelelően végezzék;
- meghatározni, hogy hogyan kell kezelni a nemmegfelelőségeket;
- kidolgozni információbiztonság módszertanát és folyamatait;
- azonosítani kell a jelentős fenyegetéseket és az információ és információ-feldolgozó eszközök fenyegetésnek való kitettségét;
- felmérni az információbiztonsági intézkedések bevezetésének megfelelőségét;
- információbiztonsági képzés és a tudatosság elősegítése az egész szervezetben;
- az információbiztonsági incidensek figyelemmel kísérése és átvizsgálásából kapott információk alapján megfelelő beavatkozások meghatározása

10.4 A munkaerő kiválasztása

A biztonsági előírások betartásáért viselendő felelősséget és szabályokat már a munkaerő keresésénél és felvételi eljárás során közölni kell, a munkaszerződésben rögzíteni kell, és az egyén foglalkoztatásának ideje alatt figyelni kell a betartását. Ezzel csökkenthetők az emberi hibák, a szervezet eszközeivel kapcsolatos bűncselekmények bekövetkezésének kockázata, mint például a lopás, a csalás és a visszaélés.

A leendő új munkatársakról megfelelően tájékozódni kell, különösen a bizalmi munkakörökben. Az információ-feldolgozó eszközöket használó valamennyi alkalmazottat és a külső fél oldalán megjelenő felhasználókat is titoktartási megállapodás megkötésére kell kötelezni. Így a”**Munkavállalói Nyilatkozat**” minden esetben kötelező, ha a munkatárs az **adatvédelem** és az **információbiztonság** hatálya alá tartozik.

A vezetőknek tudatában kell lennie annak, hogy a munkatársak személyes körülményei hatással vannak a munkavégzésükre. Személyes, vagy pénzügyi nehézségek, viselkedésük vagy életvitelük változásai, gyakori hiányzások, nyilvánvaló stressz vagy depresszió az, ami csaláshoz, szervezeti vagyon elemek, eszközök eltulajdonításához és más biztonsági problémákhoz vezethetnek.

A személyes élethelyzetre vonatkozó információt a személyes adatok kezelésére és személyiségi jogok védelmére vonatkozó jogszabályokkal összhangban kell kezelni.

Az átvilágítások szükségességét, jogosságát és módszerét a megfelelő jogi szabályozással összhangban, a vonatkozó jogi illetékesség keretein belül végzi a szervezet, illetve a jelölteket előre tájékoztatják az átvilágítási tevékenységről.

A felvételre tervezett pályázók esetében a szervezet a lehetőségeinek függvényében és betöltött munkakörre vonatkozóan ellenőrzi:

- független azonossági ellenőrzést (személyi igazolvány, vagy vele egyenértékű fényképes igazolvány);
- a kérelmező önéletrajzának ellenőrzését (teljesség és pontosság szempontjából);
- a vonatkozó referenciák rendelkezésre állását;
- az igényelt felsőoktatási és szakmai minősítések megerősítését, valamint
- esetleges részletesebb ellenőrzéseket az előéletre és egyéb területekre (hitelképesség, büntetett előélet, stb…) vonatkozóan.

Az kijelölt felelős a munkatársak szakmai tevékenységét, felkészültségbeli változását folyamatosan figyelemmel kíséri. Az újonnan felvett munkatársakat fokozatosan kell bevezetni a fő- és üzleti folyamatokba és ennek megfelelően lehet csak biztosítani a szükséges információkhoz való hozzáférést.

Az első számú vezető feladata meghatározni az adott munkatársnál azokat az eljárásokat, amiket az átvilágítás során el kell végezni.

Az első számú vezető feladata a szerződő felekkel kapcsolatban meghatározni az ellenőrzés szükségességét, valamint az alkalmazott átvilágítási folyamat módszerét és gyakoriságát, mivel ennek felelőssége teljes mértékben az főigazgatóé.

A szervezetnélnél dolgozó személyekkel, illetve a külsős partnerekkel csak a megfelelő átvilágítási folyamatot követően kötnek szerződést. A munkatársakkal, illetve a partnerekkel kötött szerződéseket minden esetben az ügyvéd készíti elő.

Amikor egy munkatárs új munkakörbe, beosztásba (szervezeti pozícióba) kerül, - akár azért mert most újonnan nevezik ki az adott beosztásra, akár mert előléptetik - és az új munkakör magában foglalja a hozzáférést olyan információ-feldolgozó eszközökhöz, amelyek bizalmas, vagy személyes információkat, adatokat dolgoznak fel, a szervezet köteles a jogszabályok által előírt ellenőrzést lefolytatni. Ezt követően a **Jogosultsági és hozzáférési Szabályzat** alapján egy *jogosultság nyilvántartóban* rögzítésre kell, hogy kerüljön.

A foglalkoztatás feltételei között kell megállapítani a leendő munkatárs informatikai biztonságra vonatkozó kötelességeit. Ezeknek a kötelezettségeknek - egyes esetekben, ahol ez értelmes - meghatározott időtartamra ki kell terjedniük a foglalkoztatási időszakon túl is. E kötelezettségek közé kell belefoglalni azokat az intézkedéseket is, amelyek akkor lépnek életbe, ha az alkalmazott nem tartja be az előírt biztonsági követelményeket. A foglalkoztatási feltételeknek tartalmazniuk kell, hogy ezek a kötelezettségek fennállnak a szervezet működési helyein kívül is, sőt esetleg a rendes napi munkaidején túl is, például az otthoni munkavégzés alatt is.

Az alkalmazottak jogait és kötelességeit, - például a szerzői jogokra vagy a személyes adatok védelmére és a személyiségi jogokra vonatkozó jogszabályokra tekintettel -, tisztázni kell és fel kell sorolni a munkaszerződés feltételei között.

A vezetésének gondoskodnia kell arról, hogy a munkatársak tisztában legyenek az információs rendszerekkel kapcsolatos feladatokkal és felelősségekkel. A vezetésnek meg kell határoznia, hogy melyek a kulcsfontosságú informatikai beosztások és munkakörök.

Munkába álláskor minden munkatárs számára biztosítani kell az informatikai rendszerek adatvédelmével és biztonságával kapcsolatos oktatást, valamint az összes munkatárs számára a rendszeres továbbképzést. A rendszeres adatvédelmi továbbképzésről az **információbiztonságért felelős személynek** és az **IT üzemeltetést végző munkatársnak** kell gondoskodnia.

A szervezetnél nem kezdődhet munkavállalói viszony mielőtt annak feltételei nem kerültek előzetesen dokumentálásra. A munkatársak általános feladatait és felelősségeket a Munkaköri leírás, illetve az egyéb szervezeti szabályozó dokumentumai tartalmazzák.

A munkatársat érintő vonatkozó szabályozásokról a belépő munkavállalók a bevezető képzés során is tájékoztatást kapnak. A szervezet meghatározta a munkatársaival kapcsolatos titoktartási követelményeket. A munkavállalóknak mindezen mellett belépéskor kötelező aláírni a **Munkavállalói Nyilatkozatot**.

Minden belépő munkatárs esetén az adott személyhez rendeli a szükséges informatikai eszközöket és jogosultságokat, ezzel a felelősséget is! A „Jogosultság elrendelő” alapján adják ki a szükséges eszközöket és állítják be a jogosultságokat.

Az inforrmációbiztonságért felelős személy, vagy az általa megbízott munkatárs ezen információk alapján vezeti a jogosultságok, illetve a kiadott IT eszközök Az eszközök átadás-átvételi formanyomtatványon kerülnek átadásra és visszavételre.

A vezető feladata pontosan meghatározni, hogy milyen eszközöket és jogosultságokat kaphat a belépő munkatárs a következőkre vonatkozóan:

- Informatikai rendszerekhez, programokhoz való hozzáférés
- Munkavégzéshez szükséges eszközök biztosítása
- kódok, kulcsok, riasztó...

Az IT üzemeltetéssel megbízott cég feladatai:

- Információbiztonsági oktatások megtartása
- Az egységes telepítőkészletből a szükséges szoftverek feltelepítése, a konfiguráció elkészítése
- Jelszavak és jogosultságok beállítása
- Az adatok archiválása

Egyéb munkatársi feladatok:

- Egyéb kiadott irodai eszközök átadása:

  o mobiltelefon, laptop, vagy asztali gép, illetve kódok, belépési jogok egyéb eszközök, munkakörtől függően.

Eszközök átadása-átvétele, melynek igazolására átadás-átvételi jegyzőkönyv készül.

10.5 Belső oktatások

Az informatikai biztonság tudatosítása érdekében is oktatásokat, képzéseket biztosít a szervezet a következő témakörökben:

- A bevezetett információbiztonsági rendszer,
- általános informatikai biztonsági oktatás minden új és minden hasonló oktatáson eddig részt nem vett felhasználó részére
- új, bevezetésre kerülő rendszerekkel kapcsolatos oktatás minden, a rendszer bevezetésében érintett felhasználó körében,
- A felhasználó beosztásának, munkakörének megfelelő további informatikai biztonsági oktatás,
- a legfrissebb fenyegetésekkel, veszélyforrásokkal, a védelmet szolgáló biztonsági eszközökkel, vírusvédelmi rendszerekkel, védelmi technikákkal kapcsolatban az abban érintett felhasználók részére oktatás.

Az információbiztonságért felelős személy feladata a fent említett pontokkal kapcsolatban oktatásokat, képzéseket szervezni, az oktatások szakmai részét a helyi IT üzemeltető végzi az adott tematika függvényében.

Szükséges, hogy minden új munkavállaló megismerje oktatások keretei között a szervezet belső szabályzatait és elvárásait, mielőtt engedélyezik a hozzáférést az információhoz.

10.6 Fegyelmi eljárás

Olyan fegyelmi eljárást kell kialakítani a szervezet általános fegyelmi szabályain belül, amely azokra a munkatársakra vonatkozik, akik megsértették a szervezet biztonsági szabályzatait és eljárásait.

Hivatalos fegyelmi eljárást kell kezdeményezni az olyan esetek kezelésére, amikor a biztonsági események kivizsgálása során összegyűjtött bizonyítékok alapján egyértelműen meghatározható, hogy a biztonsági esemény a biztonsági szabályok szándékos vagy véletlen megsértésének következtében állt elő.

Az informatikai biztonsági előírások súlyos megsértése esetén fegyelmi eljárást kell indítani a szabálysértő személyével szemben, ha:

- a szabálysértés valamely rendszer hozzáférési adatainak illetéktelen személynek történő tudomására hozatalával (pl.: személyes jelszó elmondása, vagy hozzáférhető helyre történő feljegyzése) kapcsolatos.
- a szabálysértés következtében a „Kiemelten értékes" minősítésű adata, dokumentuma kerül illetéktelen kezekbe.
- a szabálysértés következtében az „Közepesen értékes", vagy annál magasabb szintű minősített adatát, dokumentumát szándékosan meghamisította.
- a szabálysértés következtében a szervezet biztonsági rendszerének védelmi megoldásai illetéktelenek kezébe jutottak
- törvénysértés esetén a szabálysértés következtében súlyosan sérülnek a személyes adatok védelméről, és nyilvánosságra hozataláról szóló jogszabályok.
- bűncselekmény gyanúja áll fenn.

Az informatikai biztonsággal kapcsolatos fegyelmi eljárás lefolytatását az alábbi személyekből álló bizottság hajtja végre:

- **első számú vezető** vagy az általa delegált személy,
- **adatvédelmi megbízott**, vagy az általa delegált személy,
- a szabálysértő személy közvetlen munkahelyi vezetője,
- **IT üzemeltetést végző munkatárs**
- **információbiztonságért felelős személy**

A deklarált követelmények, felelősségek, jogok az **Informatikai és Információbiztonsági Szabályzat és Irányelvek Felhasználóknak** dokumentumban kerülnek rögzítésre.

Amennyiben a fegyelmi eljárás a felsorolt személyek valamelyikére irányul, új tagságot kell kijelölni. Ha a felhasználó által okozott szabálysértés anyagi kárral is jár, anyagi felelősséget is meg kell állapítani, és az okozott kárt a törvényeknek megfelelően ki kell fizettetni a kár okozójával.

A biztonsági események kivizsgálásakor gondoskodni kell:

- az esetlegesen érintett személy személyes adatainak védelméről;
- az érintett, bizonyítékot szolgáltató naplóállományok kivizsgálás idejére történő megőrzéséről;
- a kivizsgálás pontos dokumentálásáról, amely vizsgálati dokumentumnak a következőket kell minimálisan tartalmaznia:
  - a vizsgálatot elrendelő irat másolatát,
  - a vizsgálat okát,
  - dátumát,
  - helyét (ez lehet a munkaállomás helye, de a szerver helye is),
  - időpontját,
  - a vizsgálatot végzők nevét, beosztását, aláírását,
  - a biztonsági esemény körülményeit,
  - a vizsgálat során vizsgált naplóállományok / könyvtárak /, állományok megnevezését,
  - a vizsgálat alapján megállapított (bizonyítható) tényeket,

azon okok megszüntetésére vonatkozó intézkedéseket, amelyekkel elkerülhetőek a későbbiekben a hasonló biztonsági események;

A biztonsági eseménnyel kapcsolatban gondoskodni kell az értesítendő hatóságok szükség szerinti értesítéséről és a szükséges kommunikációról.

11. Jogosultságok és hozzáférések kezelése

Ezt a területet a Jogosultság és Hozzáférési Szabályzat kezeli.

12. Információbiztonsági incidensek kezelése

Ezt a területet az Információbiztonsági Incidenskezelési Szabályzat kezeli.

13. Külső szervezet információbiztonsága

A szervezet információ-feldolgozó eszközeit ellenőrzött környezetben és módon lehet csak a külső fél számára hozzáférhetővé tenni. Ahol indokolt az, hogy külső fél számára hozzáférhetővé tegye a szervezet az informatikai- és információerő-forrásokat, azokon a területeken kockázatfelmérést, értékelést és elemzést kell végezni annak meghatározására, hogy milyen az információ-hozzáférhetőségének biztonsági kihatása és milyen ellenőrzési mechanizmusokat kell megvalósítani.

Az informatikai rendszeren történő munkavégzéshez hozzáférést csak a szerződésben rögzített munkához szükséges, és elégséges jogosultságokkal kell biztosítani. Külső személynek távoli elérés csak különösen indokolt esetben, a külső személy (cég) megbízhatóságáról történő meggyőződés után biztosítható.

A külső félnek adott hozzáférési engedély lehetővé teheti azt, hogy további partnerek is kaphassanak hozzáférési jogosultságokat. A külső féllel kötött szerződésnek ezért magában kell foglalnia azt az engedélyezési és jóváhagyási eljárást, amelynek révén a szervezet hozzájárul a külső szerződő félen keresztül megjelenő más partner szervezetek számára az esetleg szükséges hozzáférési jogosultságok megadásához és ezzel megszabja hozzájuk kapcsolódó feltételeket is.

A követelmények deklarálása **adatfeldolgozó** tekintetében külön kerül előírásra, a GDPR megfelelés érdekében.

Egyéb külső fél esetében **Titoktartási Nyilatkozat** kitöltésére **kötelezhető**.

Az információbiztonság területi hatálya alá bevont helyeken következetesen alkalmazni kell a beléptetéssel, illetve az ügyfelek, vendégek, kutatók mozgásával kapcsolatos szabályozás előírásait.

13.1 A hozzáférési jogosultságok típusai

A külső szervezetet számára engedélyezett **hozzáférési jogosultságok** kritikus fontosságú kockázati tényezőként jelentkeznek. A szabályozandó hozzáférési jogosultságok típusai a következők:

- **fizikai** hozzáférési jogosultságok: például az irodai helyiségekhez, számítógépteremhez, tároló szekrényhez;
- **logikai** hozzáférés: például a szervezet adatbázisaihoz, informatikai rendszereihez, információ-vagyonához.

13.2 A hozzáférési jogosultság engedélyezésének indokoltsága

Külső fél számára hozzáférési jogosultság iránti engedélyezési eljárást sokféle okból szokás indítani. Az **IBSZ** teljes körű, az összes lehetőséget kimerítő felsorolásra nem tud vállalkozni. Ezért az engedélyezési eljárásnak magának kell olyan ellenőrzési mechanizmusokat nyújtania, amelyek kellő garanciát adnak a szervezet informatikai biztonsági követelményeinek betartására.

Szükség esetén lehetnek akár egyedileg szabályozandó esetek, ha általános szabályozás nem létezik, mivel lehet olyan külső fél, amelyik a szervezetnek úgy nyújt szolgáltatást, hogy nem települ be annak telephelyére, de mégis szükséges valamilyen fizikai és logikai hozzáférési jogosultság a munkavégzéséhez, ilyenek lehetnek például:

- a hardver és a szoftvertámogatók személyzete, akiknek rendszerszintű vagy legalább is alsószintű alkalmazási funkcionális szolgáltatásokhoz történő hozzáférésre van szükségük;
- ügyfelek, partner szervezetek vagy a közigazgatás hatáskörébe tartozó vállalkozások, akik információt cserélhetnek a szervezet információrendszereivel, illetve akik hozzáférhetnek a szervezet informatikai rendszereihez vagy osztozhatnak a közös adatbázisokon.

A külső fél **hozzáférési jogosultsága** mindenképpen **biztonsági kockázatot jelent**, különösen magas a biztonsági kockázat akkor, ha nem megfelelő a külső fél biztonságirányítási, vezetési és ellenőrzési rendszere.

Mindenütt, ahol igény van arra, hogy külső fél hozzáférési jogosultságokat kapjon a szervezettől, kockázatfelmérést kell végezni, és a kockázatok értékelése és elemzése révén szükségessé váló külön óvintézkedéseket meg kell határozni és az ellenőrzési mechanizmusokat ki kell alakítani.

A kockázatok felmérésénél és értékelésénél célszerű figyelembe venni az elvárt hozzáférési jogosultság fajtáját, az információ értékét, a külső fél által használt óvintézkedéseket, valamint az adott szervezet információihoz történő hozzáférés hatását a biztonságra.

13.3 A szervezet működési helyeire betelepülő külső felek

Az olyan külső (szerződő) felek, amelyek szerződésükben meghatározott módon a szervezet egyes működési helyeire betelepültek, munkatársaik rendszeresen ott tartózkodnak, ugyancsak jelenthetnek gyenge biztonsági pontokat. A betelepült külső fél például olyan szolgáltatásokat nyújt, amelyekhez az alábbi munkatársait, alkalmazottainak helyszíni jelenlétét biztosítja:

- hardver- és szoftverkarbantartó és műszaki támogatás;
- takarítás, étkeztetés és őrző-védő szolgáltatások, valamint hasonló, a szervezet számára egyéb támogató szolgáltatásokat nyújtó, külső felek (lehetnek kiszervezett, kihelyezett szolgáltatások; vagy szolgáltatás vásárlás stb.)
- tanulók foglalkoztatása és más, eseti, rövididejű alkalmi munkavállalók;
- kutatók
- tanácsadók (vezetői, jogi, informatikai, műszaki stb.).

A külső féllel kötött szerződésben meg kell jeleníteni azokat a biztonsági előírásokat, követelményeket, amelyek a külső fél hozzáférési jogosultságainak engedélyezése miatt, mint betartandó szabályok jelennek meg. Ezek a szabályozások elsősorban az IBSZ-ből származnak, de a részleteket az IBSZ alá tartozó részletesebb utasítások, munkaköri leírások, nyilatkozatok, stb. is tartalmazhatják.

A bizalmas adatkezelés betartatásának egyik jogi eszköze az „**Adatfeldolgozói szerződés kiegészítés**” megkötése a külső féllel; illetve alkalmanként a munkavégzésre jelentkező külső fél munkatársai, partnerei és egyéb résztvevői számára egyénileg, jogilag kötelező módon egyéb nyilatkozatok, megállapodások létrehozása, és aláíratása.

A külső fél és munkatársai addig nem férhetnek hozzá az információhoz és az információ-feldolgozó eszközökhöz, amíg a szükséges óvintézkedéseket meg nem valósították és ki nem alakították a kellő ellenőrzési mechanizmusokat, továbbá a megfelelő jogi feltételek létre nem jöttek (szerződés hatályba lépése, titoktartási megállapodások aláírása).

14. Fizikai és környezeti biztonság

A szervezet helyiségeit és információit meg kell védeni a jogosulatlan hozzáféréstől, a károkozástól, valamint az illetéktelen beavatkozástól. A kritikus fontosságú, vagy bizalmas információkat, információ-feldolgozó eszközöket a biztonságos határzónákon belül kell elhelyezni, továbbá megfelelő biztonsági védelmi eszközökkel kell védeni a megállapított kockázattal arányosan.

Célszerű az irodákban az „üres asztal - tiszta képernyő” szabály alkalmazásával csökkenteni a papírokhoz, az adathordozókhoz és az információ-feldolgozó eszközökhöz való jogosulatlan hozzáférés és sérülés kockázatát.

14.1 Fizikai biztonsági határzóna

Az informatikai infrastruktúra elemeinek és a helyiségeknek a kockázatokkal és a tágabb értelemben vett értékükkel arányos fizikai védelmet kell biztosítani. A helyiségek kockázatarányos védelmének biztosítása érdekében biztonsági zónákat kell kialakítani, továbbá meg kell határozni az egyes zónákba belépésre jogosultak körét.

A szervezetnél három biztonsági zónát kell megkülönböztetni:

- határzóna: az objektum első védelmi rendszere, külső behatolást megakadályozó eszközzel védve (kerítés, sorompó).
- határzóna: épületen belüli részek, melyek csak felügyelet mellett és a belépés ellenőrzésével használható
- határzóna (irodán belül): a szervezet információ-feldolgozó eszközeinek elhelyezését biztosító zárható helységek.

A határzónákra vonatkozó követelményrendszert az alábbi szempontok alapján kell meghatározni:

- hozzáférési követelmény,
- környezeti követelmény,
- biztonsági követelmény,
- ellenőrzési követelmény,
- dokumentálási követelmény.

14.2 IT eszközök és a szerver környezeti biztonsági követelményei

Az informatikai objektumok közüzemi ellátását (áramellátás, fűtés, szellőzés, vízszolgáltatás, stb.) a vonatkozó szabályzatok, és hatósági előírások szerint kell biztosítani. Az főigazgató feladata gondoskodni

arról, hogy a környezeti biztonság megfelelő legyén, ezért figyelembe kell venni a következőket:

- a kiszolgáló-gépek elektromos hálózati áramellátása elkülönítésre kerüljön az egyéb hálózati áramellátástól;
- az elektromos hálózatra veszélyes természeti csapások ellen túlfeszültség védelmi eszköz kerüljön alkalmazásra;
- az rendszerszintű alkalmazások működését befolyásoló számítástechnikai és távközlési eszközök szünetmentes tápegységekkel legyenek ellátva;
- az informatikai hálózat kábelei az egyéb elektromos (erősáramú hálózat, telefonhálózat, stb.) kábelektől elkülönítetten kerüljenek kiépítésre (így informatikai hálózati vezeték nem húzható semmilyen más kábelt vezető kábelcsatornába).
- Balesetvédelmi előírások miatt információt szállító vezetékek, hardver elemek (monitor, nyomtató, számítógép, informatikai hálózati vezeték, stb.) lehetőleg ne kerüljenek az objektumban hálózatba kötött közüzemi berendezések fémvezető képességű elemei (telefonvezeték, radiátorhálózat, klímaberendezés, vízvezeték hálózat stb.) közvetlen közelébe.

A szervezetnél a kiemelten fontos IT eszközök elhelyezésével kapcsolatosan, a költségek figyelembe vételével, kockázatarányosan kell megfontolni az alábbi szempontokat:

14.2.1 Fizikai elhelyezés és védelem kialakításának lehetőségei

- Betörés-riasztó rendszer alkalmazása
- A helyiség határoló falai alkalmasak legyenek a fizikai betörések megakadályozására.
- Ne legyenek a helyiségnek utcára nyíló nyílászárói, vagy ha vannak, akkor azok alkalmasak legyenek a fizikai betörések megakadályozására.
- A szerver elhelyezését úgy kell megválasztani, hogy a felette elhelyezkedő helyiségekben ne legyen vizes blokk (mosdó, wc, konyha, stb.). Ellenkező esetben a födém vízzárásának kialakítása szükséges.
- Amennyiben talajszint alatt helyezkedik el, rendelkezzen elöntés elleni automata védelemmel, előntésjelzővel, amely vonulószolgálathoz van bekötve.

14.2.2 Tűzvédelem kialakításának lehetőségei

- A határoló falak, aljzat, mennyezet, és nyílászárók tűzterjedés gátló hatásának kialakítása (tűzálló festés, tűzálló üvegek, stb.).
- A tűz-, vagy füstriasztó rendszer alkalmazása.
- Kézi tűzoltó-berendezések elhelyezése a bejárat közvetlen közelében

14.2.3 Áramellátás kialakításának lehetőségei

- Az épület villámvédelmének biztosítása
- A független betáplálás biztosítása
- A szerver helyiség betáplálásának redundanciájának biztosítása (generátor, kettős betáplálás)
- A főkapcsolók biztonságos helyen való elhelyezése (lehetőleg a bejárat közelében)
- Az eszközök szünetmentes tápellátása (központi UPS, helyi UPS-ek)

- Az áram betáplálásának terhelés elosztása fázisonként
- Az UPS-ek betáplálásának elosztása fázisonként
- Érintésvédelem kialakítása, rendszeres felülvizsgálata

14.2.4 Klimatizálás kialakításának lehetőségei

- A szerver helységben a megfelelő üzemi hőmérséklet szabályozása
- A klímarendszer független legyen az épület egyéb klíma rendszereitől.
- A klíma berendezések darabszámát, típusát úgy kell tervezni, hogy a kritikus helységekben elhelyezett eszközök hődisszipációs mutatói mellett biztosítani tudják a megfelelő szabályozást.
- A klíma-berendezések automatikus újraindítását biztosítani kell az esetleges áramszünet megszűnése esetén.
- A csapadékos évszakokban megnövekedett pára kártékony hatása ellen páramentesítő alkalmazása célszerű.

14.2.5 Gondoskodás az irodák és az eszközök biztonságáról

Az irodahelyiségekben tárolt informatikai eszközök és papír alapú adathordozók biztonsága érdekében a felhasználóknak:

- a bizalmas (kényes) adatokat tartalmazó nyomtatott adatokat, információkat zárható helyen kell tartaniuk.

A kulcsfontosságú eszközöket úgy kell elhelyezni, hogy a külvilág számára ne legyenek hozzáférhetők. Az épületek ne legyenek feltűnőek és ne mutassák céljukat, ne adják nyilvánvaló jelét – sem belül, sem kívül - annak, hogy abban információ-feldolgozó tevékenység folyik.

Az olyan segédberendezések és eszközök, mint például a fénymásolók, alkalmas módon, a biztonságos körleteken belül legyenek elhelyezve, hogy ezzel is elkerüljük az olyan hozzáférési igényeket, amelyek az információ veszélyeztetésével járna.

Ajtók és ablakok, ha nincs a közelben felügyelő személyzet, zárva legyenek. Az ablakok külső védelméről is gondoskodni kell, különösen a földszinten.

A szervezet által kezelt és menedzselt információ-feldolgozó eszközöket fizikailag is célszerű elválasztani azoktól, amelyekkel külső felek foglalkoznak.

A névtárakat és a belső telefonkönyveket, amelyek bizalmas (kényes) információkat feldolgozó eszközök helyét azonosítják, tilos a nagyközönség számára elérhetővé tenni.

Veszélyes vagy gyúlékony anyagokat biztonságosan kell tárolni a biztonsági körlettől biztos távolságban.

A tartalékberendezést és a tartalékolt adathordozókat olyan biztonságos távolságban kell elhelyezni, amellyel elkerülhető, hogy a központi telephely katasztrófája esetén kárt szenvedjenek.

14.3 Gondoskodás a műszaki berendezések biztonságáról

A berendezéseket úgy kell elhelyezni és védeni, hogy csökkentsük a környezeti fenyegetések és veszélyek kockázatát, valamint a jogosulatlan hozzáférés lehetőségeit, ezért a következő elvek figyelembe vételével kell a műszaki berendezések elhelyezését megoldani:

- A berendezéseket úgy kell elhelyezni, hogy a munkaterületekre történő fölösleges belépések számát minimalizáljuk.

- A bizalmas (kényes) adatokat tároló és feldolgozó eszközöket úgy kell elhelyezni, hogy a használatuk alatt illegális tevékenység ne kerülhesse el a biztonsági felügyeletet ellátók figyelmét.
- A különleges védelmet igénylő tételeket el kell különíteni azért, hogy az általánosan igényelt védelmi szint csökkenjen.
- Ki kell alakítani olyan szabályokat, amelyek az információ-feldolgozó eszközök közvetlen közelében folytatott étkezésre, folyadékfogyasztásra vagy dohányzásra vonatkoznak.
- A környezeti feltételeket állandóan figyelni kell azért, hogy fel lehessen ismerni az olyan helyzeteket, amelyek az információ-feldolgozó eszközök működésére negatív hatással lehetnek.
- Ha az informatikai berendezésekkel folyatott munkavégzés olyan környezetben történik, amely valójában ipari környezetnek megfelelő környezeti hatásokat vált ki a berendezéseken (pl. por, szennyezett levegő, vízpára stb.), ott különleges védelmi módszereket kell alkalmazni, mint pl. a billentyűzetet védő fóliák stb.
- Védelmi intézkedéseket kell tenni vagy előkészíteni olyan esetekre, amelyek a közelben esetleg bekövetkező katasztrófák hatásainak mérséklésére irányulnak, mint pl. a szomszédos épületekben pusztító tűz, a tetőn keresztül vagy a földszint alól betörő víz, vagy valamilyen utcai robbanás.

14.4 Hardver eszközök rendeltetésszerű használata

A munkaállomások rendeltetésszerű használatához az alábbiakat kell figyelembe venni:

- A munkaállomás be-, és kikapcsolásához a hardver eszköz erre a célra kialakított kapcsolóját kell használni. Lehetőség szerint a kikapcsolásra az operációs rendszer kikapcsolás funkcióját kell használni.
- Az adatvesztés elkerülése érdekében a munkaállomás kikapcsolását kerülni kell, amikor az lemezműveletet végez (munkaállomás indítása, fájlhozzáférés, stb.).
- Ha a munkaállomás a művelet végzése közben „lefagy” elsősorban az újraindítással kell próbálkozni (Reset gomb, Ctr+Alt+Del többszöri próbálkozása), kikapcsolást akkor kell kezdeményezni, ha az újraindítás sikertelen volt.
- A munkaállomás adatbeviteli egységeibe csak szabványos, a szervezetnél elfogadott és jóváhagyott adathordozókat szabad behelyezni.

14.5 Fizikai hozzáférések

14.5.1 Munkaállomások fizikai hozzáférése

A felhasználóknak tilos a munkaállomás hardver konfigurációját megváltoztatni, a hardver eszköz belsejébe bármilyen okból belenyúlni.

14.5.2 Nyomtatók fizikai hozzáférése

Az irodai nyomtatókat úgy kell elhelyezni, hogy a kinyomtatott anyagok **illetéktelen kezekbe ne** kerülhessenek, ennek érdekében:

- A megosztott nyomtatókat úgy kell elhelyezni, hogy az állandó felügyelet, vagy a hozzáférés egyedisége biztosított legyen.

- Azokat a nyomtatókat, amelyeken „Bizalmas” anyagok nyomtatása történik, névhez kell kötni, és a munkaállomás közvetlen környezetében kell elhelyezni.
- A nyomtatókból minden, az adatvédelem, adatbiztonság tárgykörébe tartozó adatot tartalmazó iratot a nyomtatást kezdeményező személynek kell eltávolítania.
- El kell kerülni a papíralapú adatokhoz való illetéktelen hozzáférés lehetőségét, a bizalmassági kritérium megsértését harmadik személy által.

14.5.3 Felügyelet nélküli felhasználói berendezés

A felhasználóknak gondoskodniuk kell arról, hogy a felügyelet nélküli berendezések kellő védelemmel rendelkezzenek. A felhasználói körletekben telepített berendezések, mint például a munkaállomások, külön védelmet igényelnek a jogosulatlan hozzáféréssel szemben, amennyiben hosszabb időre felügyelet nélkül maradnak.

Valamennyi felhasználóban és szerződéses partnerben tudatosítani kell a biztonsági követelményeket és eljárásokat, amelyek a felügyelet nélküli berendezéseket védik, valamint saját felelősségeiket ezeknek a védelmeknek a megvalósításában. A felhasználók figyelmét fel kell hívni arra, hogy

- az aktív ember-gép párbeszédeket zárják le akkor, amikor a munka befejeződött, hacsak valamilyen hozzáférést megakadályozó mechanizmussal nem védhetők, például munkaállomás zárolásával;
- amikor a központi kiszolgáló állomásokra történő bejelentkezés révén létrejött ember-gép párbeszédeket befejezték, szabályosan jelentkezzenek ki (nem elegendő ilyenkor a PC, vagy munkaállomás egyszerű kikapcsolása);
- a PC-t, a terminált vagy a munkaállomást, ha nincsen használatban, a jogosulatlan használattal szemben védjék úgy, hogy pl. kulccsal zárják le vagy ezzel egyenértékű védőintézkedést tegyenek, például jelszavas hozzáférést használjanak.

14.5.4 A szállítás alatt álló adathordozók biztonsága

Az információ **sebezhető lehet** jogtalan hozzáférés, visszaélés, vagy sérülés révén akkor, amikor fi**zikai szállítás alatt áll**, például amikor adathordozót postai, vagy futárszolgálat útján továbbítunk. A működési helyek között szállított számítógépes adathordozók megóvásához a következő óvintézkedéseket kell megfontolni:

- Megbízható szállító, vagy futárszolgálatot kell használni.
- A csomagolás a gyártó specifikációs előírásai szerinti legyen, és elegendő ahhoz, hogy megvédje a tartalmat a szállítás alatt bekövetkező bármilyen sérüléstől.
- Szükség esetén külön óvintézkedéseket kell tenni ahhoz, hogy az érzékeny információt a jogosulatlan közzétételtől és módosítástól megóvjuk, ilyenek például:
    - lezárt szállítóeszközök alkalmazása;
    - P2P kézi kézbesítés;
    - megbontásra érzékeny csomagolásmód (amely fel tud mutatni minden hozzáférési kísérletet);
    - kivételes esetekben a küldemény több kézbesítésre bontása és azok különböző útvonalon történő kiszállítása;

- digitális aláírásnak és titkosító kódolásnak a használata
- csak a saját hordozón vehető át az anyagt;
- az adathordozón nincs semmilyen információ, amikor azt átadják a partnernek;
- a visszakapott adathordozót automatikusan vizsgálják a telepített vírusdetektáló programmal;
- az adatokat másolással helyezik át a hálózati meghajtóra;
- az adathordozót ezt követően törlik.
- Amennyiben elengedhetetlen, hogy az adathordozó azonnal ne kerüljön törlésre, úgy azt jelszavas védelemmel látják el, vagy zárt helyen tárolják.

Lehetőség szerint mellőzni kell a fizikai szállítást és különböző elektronikus módszereket kell előnyben részesíteni (e-mail, VPN, cloud)

14.6 Berendezések karbantartása

A berendezéseket korrekt módon kell karbantartani azért, hogy ezzel gondoskodjunk azok folyamatos rendelkezésre állásáról és épségéről. A következő óvintézkedéseket kell kialakítani:

- A berendezéseket a gyártó által ajánlott szervizidőszakok és –specifikációk (műszaki leírások) szerint kell karbantartani.
- A berendezéseken a javításokat és szerviz-tevékenységeket kizárólag az arra feljogosított személyzet végezheti.
- Minden gyanított és tényleges meghibásodásról, valamint valamennyi megelőző és javító karbantartásról feljegyzést kell készíteni.
- Megfelelő óvintézkedéseket kell életbe léptetni akkor, amikor berendezéseket karbantartásra házon kívülre küldenek.
- A szervezet részéről megkötött vagyon, felelősség illetve egyéb biztosítások által megszabott valamennyi követelményt ki kell elégíteni.

14.7 A mobil berendezések irodán kívüli használata

A szervezet vezetőségének **kell engedélyezni** minden olyan berendezésnek a használatát, amelyen a szervezet számára, az irodán kívül végeznek információfeldolgozást. Az így nyújtott biztonságnak egyenértékűnek kell lennie azzal, amelyet az ugyanazon célra házon belül használt berendezéseknél lehet elérni, figyelembe véve azt a kockázat növekedést, amelyet a szervezet számára telephelyen kívül végzett munka jelent. Ezen engedélyhez kötött jogokat a jogosultság nyilvántartásban is vezetni kell.

Információ-feldolgozó berendezés lehet bármilyen formájú adatfeldolgozó eszköz pl.: személyi számítógép, elektronikus határidőnapló, mobiltelefon, papír vagy bármely olyan eszköz, amelyet irodán kívüli munkára használnak, vagy a szokásos munkahelyről elszállítanak.

A következő óvintézkedéseket kell kialakítani:

- A telephelyen kívülre szállított berendezések és adathordozók nem hagyhatók felügyelet nélkül addig, amíg közterületen vannak.
- A hordozható számítógépeket kézi poggyászban, és ahol lehet, utazás közben elrejtett módon kell szállítani.
- A hordozható eszközöket általában tilos kitenni:
  - Erős fizikai behatásnak

- Sugárzó hőnek
- Erős mágneses, vagy elektromágneses térnek
- Fröccsenő víznek
- Poros környezetnek

- A hordozható eszközhöz csak a szervezet által jóváhagyott, és biztosított perifériák használhatók, a perifériákba csak a szervezet által jóváhagyott, és biztosított, szabványos adathordozók használhatók.
- A gyártók berendezés-védelmi utasításait mindenkor be kell tartani, például erős mágneses mezőnek nem szabad kitenni a mágneses, vagy félvezető alapú adathordozókat, számítógépeket.
- Az otthoni munkavégzéshez szükséges óvintézkedéseket kockázatfelméréssel kell megállapítani és a helyzethez illeszkedő óvintézkedéseket kell alkalmazni, például zárható tároló szekrényekben kell elhelyezni a számítógépet.
- Az irodán kívüli berendezések vagyon védelme érdekében illeszkedő vagyonbiztosítási konstrukciót kell alkalmazni.

Az olyan biztonsági kockázatok, mint például a károkozás, az eltulajdonítás, vagy a lehallgatás, helyről helyre jelentősen különbözhetnek, és ezt a helyzethez leginkább illeszkedő óvintézkedések meghatározásakor figyelembe kell venni.

14.8 A berendezések biztonságos leselejtezése, újrahasznosítása

Az adathordozókat - ha már nincs szükség rájuk - informatikai szempontból a biztonságra, valamint a munkahelyi egészségre és biztonságra vonatkozó előírások szerint kell **megsemmisíteni és leselejtezni**. Az adathordozók gondatlan leselejtezése bizalmas (kényes) információk illetéktelen, külső személyekhez való kerülésével fenyeget. Az adathordozók biztonságos leselejtezésére és megsemmisítésére hivatalos eljárását kell kidolgozni annak érdekében, hogy a kockázatot minimalizáljuk. A következő ellenőrzési mechanizmusokat óvintézkedéseket kell kialakítani:

- A bizalmas (kényes) információt tartalmazó adathordozókat biztonságos és védett módon kell tárolni vagy informatikai szempontból a biztonságra, valamint a munkahelyi egészségre és biztonságra vonatkozó előírások szerint kell megsemmisíteni, például elégetéssel vagy iratmegsemmisítővel, esetleg úgy, hogy adatait az előírások szerint megsemmisítik azért, hogy a szervezeten belül másik alkalmazásban felhasználják.
- A következő lista olyan tételeket sorol fel, amelyek esetében szükség lehet biztonságos megsemmisítési eljárásra:
  - papíralapú dokumentumok;
  - hang-, video- vagy más felvételek;
  - kinyomtatott anyagok, dokumentumok, jelentések;
  - hordozható merevlemez egységek;
  - optikai adattárolók (mindenféle formátumúak, beleértve a gyártott szoftverek leszállított adathordozóit is);
  - program nyelveken írt program kódok kinyomtatott formái;
  - tesztelés, bevizsgálás adatai;
  - rendszerdokumentáció.

- Általában egyszerűbb úgy megszervezni a begyűjtendő és biztonságosan megsemmisítendő adathordozókra az eljárást, hogy nem válogatják szét a titkos, bizalmas és kényes információkat hordozó anyagokat, hanem egységesen és egyformán semmisítik meg az összes anyagot.
- Sok vállalkozás ajánl szolgáltatást papír dokumentumok, informatikai berendezések s adathordozók begyűjtésére és megsemmisítésére. Gondosan kell kiválasztani azt az alkalmas szerződő felet, aki a kellő ellenőrzési mechanizmussal, óvintézkedéssel, eljárásrenddel és gyakorlattal rendelkezik.
- Az bizalmas (kényes) tételek megsemmisítéséről, jegyzőkönyvet kell felvenni, annak érdekében, hogy az ellenőrizhetőségi és nyomon követhetőségi naplót (lefűzött jegyzőkönyvek) napra készen lehessen tartani.
- Amikor az adathordozókat megsemmisítés céljából összegyűjtik, figyelembe kell venni azt is, hogy a felhalmozott adatkészlet egy olyan szinergikus hatással járhat - az egész több mint részeinek összege -, amelynek következménye az lehet, hogy nem minősített információk összessége magasabb titkosítási minősítést igényelne, mint egyes kis mennyiségű minősített információ.

Az adathordozókat selejtezésre kell kijelölni, ha

- az életciklusa lejárt,
- a tárolt adatok nem olvashatók el és nem állíthatók helyre,
- további felhasználás alól kivonásra kerül,
- technológiaváltáskor, mentés, átmásolás után.

A berendezések valamennyi elektronikus adattároló részegységét, pl. a lemezegységeket, ellenőrizni kell annak érdekében, hogy meggyőződjünk arról, hogy a bizalmas (kényes) információt és a vásárolt szoftvereket arról eltávolították és felülírták, mielőtt leselejtezték volna.

A bizalmas (kényes) információt tartalmazó, de sérült adattároló-eszközök kockázatfelmérést igényelhetnek annak meghatározására, hogy mi a jobb, az adott eszközt megsemmisíteni, megjavítani, vagy elektronikus szemétként elszállíttatni.

14.9 Külső helyről érkező adathordozók kezelése

Külső helyről érkező adathordozókat használatba venni csak **ellenőrzés után szabad**. Az ellenőrzés során ki kell térni a küldő azonosítására, a vírusmentesség ellenőrzésére, az adattartalom beolvashatóságára. Az adathordozókat használatba venni csak az előírt ellenőrző eljárások után szabad.

14.10 „Üres asztal – tiszta képernyő szabály”

Be kell vezetni, és be kell tartatni az „üres asztal” szabály elfogadását, mind a papíralapú anyagokra, mind a hordozható adattároló-eszközökre, valamint a „tiszta képernyő” szabályt az információ-feldolgozó eszközökre vonatkozóan, hogy ezáltal lecsökkenjen a jogosulatlan hozzáférés, az információvesztés és információkárosodásának kockázata, mind a rendes munkaidőben, mind azon kívül.

A következő óvintézkedéseket kell megtenni:

- A papíranyagokat és a számítógépek nem beépített adathordozóit megfelelő, zárható szekrényben vagy más, hasonlóan biztonságos

szekrényben kell tárolni, amikor éppen nincsenek használatban, különösen a munkaidőn túli időszakokban.

- A bizalmas (kényes) és kritikus fontosságú információt használaton kívül el kell zárni (ideális esetben tűznek ellenálló biztonsági széfben vagy szekrényben), különösen akkor, amikor az iroda üres.
- Személyi számítógépeket, munkaállomásokat és nyomtatókat nem szabad „bejelentkezve" hagyni akkor, amikor felügyelet nélkül maradnak, és a használaton kívüli számítógépekhez való biztonsági zárakkal, jelszavakkal, vagy más intézkedésekkel kell védeni az eszközöket.
- Az elektronikus levelezés fogadó és küldő logikai és fizikai pontjait védein kell.
- A bizalmas (kényes), vagy minősített információt kinyomtatás után azonnal el kell távolítani a nyomtatóról.

15. IT üzletmenet-folytonosság és katasztrófakezelés

Ezt a területet IT üzletmenet-folytonosság és katasztrófakezelési szabályzat kezeli.

16. Információcsere

16.1 Internet

A szervezet felhasználói egy ponton lépnek ki a világhálóra. Az Internet felől érkező támadások megelőzésére szabad portokat ellenőrzés nélkül hagyni nem szabad.

Az IT üzemeletető rendszergazda a **jogosultsági rendszerben meghatározott elrendelő** által, a meghatározott munkatársaknak távoli elérést engedélyezhet (VPN).

Az Internet felől érkező, számítógépes vírust, férget tartalmazó küldemények, csatolt fájlok, egyéb kárt okozó, ártó szándékkal küldött levelek szűrésére korszerű és menedzselt tartalomszűrő és vírusirtó szoftvernek kell üzemelnie.

A külső kommunikáció során a törvényes adatkezelésből származó védett adatot jogellenesen továbbítani tilos!

Sem munkaidőben, sem azon kívül nem szabad az Interneten felkeresni a munkaállomásokról nem informálódásra szolgáló, kétes tartalmakat szolgáltató szervereket, zenei vagy film fájlcserélőket.

Az internetes kommunikáció során meggondolt, felelős magatartással kell a veszélyforrásokat és valós kockázatokat elkerülni, a védett adatok megszerzésének lehetőségét kizárni.

16.2 E-mail

Az elektronikus levelezést a szervezetek és személyek közötti kapcsolatokban alkalmazzák. Azonban az emberek közötti kommunikáció hagyományos formáitól az elektronikus levél lényegesen különbözik, például sebességben, üzenet-szerkezetben, az informálisság mértékében, valamint a jogtalan tevékenységekkel szembeni sérülékenységében, hiszen egy elektronikusan nem aláírt és kriptográfiailag nem védett elektronikus levél

egy közönséges postai levelezőlapnak felel meg adatbiztonság és adatvédelem tekintetében.

Az elektronikus levelezés használatából származó biztonsági kockázatok csökkentése végett ellenőrzési mechanizmusokat és egyéb óvintézkedéseket kell kialakítani. Ezek a biztonsági kockázatok a következőket foglalják magukban:

- az üzenetek sebezhetőségét, nevezetesen az üzenethez történő jogtalan hozzáférés, módosítás tekintetében vagy a túlterheléses támadással szemben;
- az olyan sebezhetőséget, amely bizonyos hibák következményeként áll elő, mint például a helytelen címzés, a téves címre történő irányítás, illetve a sebezhetőség az informatikai szolgáltatás általános megbízhatósági szintjéből és rendelkezésre állási paramétereiből adódik;
- a hírközlési, távközlési és informatikai hálózat sajátosságainak változásából származó hatásokat, amelyek a szervezeti („ügyviteli") folyamatokra hatnak, például az adattovábbítás megnövekedett sebességének a hatása, vagy annak a hatása, hogy hivatalos levelet lehet küldeni, de nemcsak szervezet a szervezetnek, hanem például személy a személynek;
- jogkövetkezmények kezelését, mint például az olyan követelmények kielégítése, hogy jogilag megalapozottan bizonyíthassuk az elektronikus levél eredetét, továbbítását, a kézbesítését, és az átvételét;
- annak következményeit, hogy a szervezet munkatársa elektronikus elérhetőségének listáját a külvilág számára közzé tesszük;
- a távoli felhasználók hozzáféréseinek nyomon követését és ellenőrzését akkor, amikor elektronikus leveleikért távolról bejelentkeznek a levelező rendszerünkbe.

A fentiek érdekében az elektronikus levelezés kialakításával kapcsolatban a következő irányelveket érdemes figyelembe venni:

- az elektronikus levelezéssel szembeni támadások, például a vírusok, a levelek elfogására;
- az elektronikus levelekhez csatolt mellékletek védelmére;
- iránymutatást arra, hogy mikor nem célszerű elektronikus levelezést használni;
- az alkalmazottak felelősségét abban, hogy ne veszélyeztessék a szervezetet, például azzal, hogy elektronikus rágalmazó levelet küldenek, amit zaklatásra használnak, vagy jogosulatlan megrendelést adjanak fel;
- az elektronikus levél bizalmassága, épsége és sértetlensége védelmében kriptográfiai technikák alkalmazására.

16.3 A nyilvánosság számára hozzáférhető rendszerek

Az elektronikusan közzétett információ sértetlenségét, épségét meg kell őrizni úgy, hogy megakadályozzuk az olyan jogtalan módosításokat, amely a közzétevő szervezet hírnevét ronthatják.

A nyilvánosan elérhető rendszerekben elhelyezett információknak, mint például egy WEB szerveren elhelyezetteknek, amely az Internetről elérhető, meg kell felelnie a hatályos magyar törvényeknek, jogszabályoknak és a szabályozásnak.

Ha a nyilvánosan elérhető rendszereken olyan szoftvereket, adatokat és más információt teszünk hozzáférhetővé, amelyek épsége és sértetlensége magas fokú védelmet igényel, akkor azt erre alkalmas mechanizmussal kell védeni.

Az olyan elektronikus publikációs rendszert, amely - különösen, ha visszacsatolást is megenged a külvilág oldaláról - megengedi a közvetlen információ bejuttatását is, finoman kidolgozott ellenőrzési mechanizmusokkal kell védeni:

- az információt csak a hatályos adatvédelmi jogszabálynak megfelelő módon lehet gyűjteni és tárolni;
- a bizalmas, kényes információt a begyűjtés és a tárolás során gondosan védeni kell;
- a hozzáférés a közzétevő rendszerhez nem engedheti meg azt, hogy a hozzá kapcsolódó, a háttérben meghúzódó kiszolgáló más hálózatokhoz jogtalanul, a külvilághoz pedig engedély nélkül hozzáférhessen.

16.4 Az információcsere egyéb formái

Az információ károsodhat, ha hiányzik a biztonsági tudatosság, nincsenek irányelvek, szabályzatok, vagy eljárások. Erre példa az a közterületen, mobil készüléken folytatott beszélgetés, amelyet bárki hallhat, vagy amikor az üzenetrögzítő készülék hangja bárki által hallható lejátszáskor, vagy amikor jogosulatlanul férnek hozzá a tárcsázással hívható hangposta-rendszerhez.

A szervezet folyamatos működésében zavarok állhatnak be és információ kerülhet nyilvánosságra, ha a kommunikációs eszközök meghibásodnak, túlterhelődnek, vagy üzemszünet következik be. Az információ akkor is nyilvánosságra kerülhet, ha ezekhez illetéktelen felhasználók férnek hozzá.

Egyértelmű irányelveket kell meghatározni a munkatársaknak e tekintetben:

- a munkatársak figyelmét fel kell hívni arra, hogy legyenek elővigyázatosak, például ne tárjanak fel bizalmas, kényes információt, lehetőleg kerüljék el, hogy telefonálás közben mások kihallgathassák beszélgetésüket, ezért figyelni kell a közvetlen körülötte álló személyekre, különösen mobil telefonáláskor, illetve tudni kell, hogy vannak-e jelen mások is a telefonvonal másik végén.
- fel kell hívni az alkalmazottak figyelmét arra, hogy tilos nyilvános helyen, vagy nyílt irodákban és vékony fallal elkerített tárgyalókban folytatni bizalmas beszélgetéseket;
- fel kell hívni az alkalmazottak figyelmét arra, hogy bizalmas információt tartalmazó üzeneteket nem szabad az üzenetrögzítőre mondani, mivel ezt bármely, jogosulatlan személy is lejátszhatja, hiszen ezek az üzenetek gyakran távközlési hálózatok szolgáltatásaiban tárolódnak (ld. mobil szolgáltatók), vagy téves tárcsázás következtében nem a helyes címzett számára kerülnek rögzítésre;

16.5 Információcsere egyezmény

A szervezetek közötti információ - akár elektronikus, akár manuális – lebonyolítására megállapodást kell kötni. Egyes ilyen megállapodásokat hivatalos formában, mint egy szerződést kell megkötni.

Egy ilyen megállapodás biztonsági tartalma tükrözze az érintett szervezeti („ügyviteli”) információ bizalmasságának, kényességének fokát. A biztonsági

feltételekről szóló megállapodásban a következő ellenőrzési mechanizmusokat és óvintézkedéseket kell kidolgozni:

- a vezetőség feladat-, hatás- és felelősségi körét az információ továbbítás ellenőrzésében, az értesítések kiküldésében, a továbbítás kezdeményezésében és elindításában, valamint a fogadásában, nyugtázásában.
- az információküldő értesítéséről szóló eljárásokat, az információtovábbításról, az átvitel megkezdéséről és az információ megérkezéséről, nyugtázásáról;
- információ-, vagy adatcsomagok készítésének és továbbításának minimális műszaki szabványait;
- a futárokat azonosító szabályokat;
- adat-, információ elvesztése esetén viselendő anyagi és erkölcsi felelősséget és kártérítési kötelezettségeket;
- a bizalmas (kényes) és a kritikus fontosságú információ egyezményes címkézési rendszerét, amellyel gondoskodnak arról, hogy a címkék azonnal érthetők legyenek, és hogy az információ kellőképpen védve legyen;
- feladat-, hatás- és felelősségi köröket az információ és a szoftver tulajdonjog, az adatvédelem, a szoftver szerzői és szomszédos jogok védelme és hasonló területek tekintetében;
- az információ és a szoftver elektronikus rögzítésére és visszaolvasására vonatkozó műszaki szabványokat;
- bármely olyan sajátos óvintézkedést, amelyet olyan bizalmas (kényes) információ, adat, vagy szoftver tételek védelme tesz szükségessé, mint amilyenek a kriptográfiai kulcsoké.

17. Rendszerkezelés

17.1 Általános rendszertervezés

Az informatikai rendszerek, vagy az egyes rendszerelemek tervezéskor a funkcionalitáson, a gazdaságosságon túl a biztonsági szempontokat is figyelembe kell venni. A rendszergazdának ügyelnie kell arra, hogy tervezéskor a biztonsági megoldások is hangsúlyt kapjanak.

A tervezés során általában az alábbi biztonsági szempontokat kell figyelembe venni:

- A rendszer együttműködése a meglévő rendszerelemekkel
- Beépített biztonsági megoldások
- Az informatikai rendszer hozzáférési megoldásai (jogosultság kezelés, titkosírás, stb.)
- Az informatikai rendszer rendelkezésre-állást támogató megoldásai (karbantarthatóság, javíthatóság, van-e támogatás, mentések végrehajthatósága, stb.)
- Az informatikai rendszer menedzselhetősége (központilag menedzselhető, vagy helyileg)
- Az informatikai rendszer ellenőrizhetősége (naplózhatók-e a kritikus folyamatok, távoli elérés biztosított-e, stb.)

17.2 Kapacitástervezés

Nyomon kell követni a kapacitásigényt és el kell készíteni a jövőre vonatkozó kapacitáskövetelményekre vonatkozó előrejelzéseket annak érdekében, hogy megfelelő hardver kapacitás álljon rendelkezésre.

Ezeknek az előrejelzéseknek a szervezeti (ügyviteli) és az új rendszerkövetelményeket kell figyelembe venniük, valamint a szervezet információfeldolgozásának jelenlegi és előre jelzett tendenciáit.

Különös figyelmet érdemelnek a kulcsfontosságú erőforrások, mivel esetenként lényegesen költségesebbek, és sokkal több időt igényel az új kapacitások beszerzése. A rendszergazdának nyomon kell követnie a kulcsfontosságú erőforrások kihasználtságát, beleértve a központi egységek processzorait, központi memóriájukat, háttértárolóikat, nyomtatóikat és egyéb adatkimeneti eszközeit, valamint távközlési, kommunikációs rendszereit.

A rendszergazdának fel kell ismernie a felhasználási szokások változásainak tendenciáit, különösen azokat, amelyek kapcsolódnak a szervezeti (ügyviteli) alkalmazásokhoz, vagy a vezetői információrendszerek eszközeihez.

Ezen információk felhasználásával fel kell ismerni a potenciális szűk keresztmetszeteket, amelyek fenyegetést jelenthetnek a rendszerbiztonságra és a végfelhasználói szolgáltatásokra, és ajánlatos ennek megfelelő kiküszöbölési tevékenység tervezése.

17.3 A rendszer átadás-átvétele

Az új információrendszerek, a rendszerfrissítések, aktualizálások és az új verziók átadás-átvételi követelményeit meg kell határozni, és az átadás-átvétel előtt el kell végezni a vonatkozó rendszerbevizsgálásokat, teszteléseket.

A hardver eszközök beszerzéséhez az alábbi tényezők figyelembevétele szükséges:

- A hardver funkcionalitása, erőforrásai
- A hardver várható rendelkezésre állása (megbízhatóság)
- A hardver garanciális támogatása (garancia idő, tartalom)
- A hardver support támogatása (tanácsadás, alkatrész biztosítás)

A szoftver megoldásoknál az alábbi tényezők figyelembevétele szükséges:

- A szoftver funkcionalitása
- A szoftver platformfüggősége
- Támogatja-e a szoftver a homogenitási törekvéseket
- A szoftver biztonsági megoldásai (jogosultság kezelés, titkosítás, stb.)
- A szoftver menedzselhetősége
- A szoftverhez biztosított support

A vezetőknek gondoskodniuk kell arról, hogy az új rendszerek átadás-átvételi követelményei és kritériumai egyértelműen meg legyenek határozva, az illetékes vezetők részéről jóváhagyva, dokumentálva és leellenőrizve. Ki kell alakítani ellenőrzési mechanizmusokat, óvintézkedéseket a következő területekre:

- a számítógépek teljesítményével és a számítógép kapacitásával szemben szabott követelmények;

- a hibák utáni visszaállítás és az újraindítási eljárásai, a katasztrófa utáni helyreállítási tervek;
- a belső szabványok, szabályzatok által előírt rutin üzemeltetési eljárások előkészítése és bevizsgálása;
- az illetékes vezetők jóváhagyása szerinti biztonsági ellenőrzési mechanizmusok és óvintézkedések kialakítása;
- eredményes és hatékony manuális eljárások;
- annak bizonyítékai, hogy az új rendszer üzembe helyezése előtt megvizsgálták azt, hogy az új rendszer nem gyakorol kedvezőtlen hatásokat a meglévő rendszerekre.
- annak bizonyítékai, hogy igenis figyelmet fordítottak arra a hatásra, amit az új rendszer üzembe helyezése okoz a szervezet általános biztonságára;
- az új rendszerek üzemeltetésének, illetőleg használatának a betanítása.

Lényegesebb új fejlesztések esetében konzultálni kell mind az üzemeltetőkkel, mind a felhasználókkal a fejlesztési folyamat minden lépéséről annak érdekében, hogy gondoskodjunk a javasolt rendszer tervének üzemi hatékonyságáról. Megfelelő bevizsgálásokat kell elvégezni annak igazolására, hogy az átvételi kritériumok teljes mértékben teljesülnek.

17.4 Szoftverek

A standard szoftverek (operációs rendszerek, alkalmazói szoftverek, office programcsomagok, rendszer-felügyeleti programcsomagok, stb.) beszerzését, nyilvántartását az **IT üzemeltetésért felelős személy** végzi.

A programok jogszerű használatáért a felhasználók felelősséggel tartoznak. Az **IT üzemeltetésért felelős személy**, valamint a felhasználók a jogszabályi előírások megszegése esetén a munkáltatónak okozott kárért a vonatkozó törvényben leírtak szerint, harmadik személyeknek okozott kárért pedig a polgári jog általános szabályai szerint felelnek.

A szoftver- és hardver-licensz megállapodások előírásainak betartását rendszeresen ellenőrizni kell, ezért a rendszergazdának bizonyos időközönként ellenőriznie kell a felhasználói gépeket. Az ellenőrzés során talált, meg nem engedett szoftverek használatának megszüntetésére, az illegális szoftver törlésére a felhasználót fel kell szólítania, illetve el kell végezni a törlést, valamint a vonatkozó biztonsági intézkedéseket.

A használt szoftverek licenceire (ahol ez lehetséges) nyilvántartást kell készíteni, amelyért a rendszergazda a felelős. A nyilvántartás tartalmazza:

- A szoftver megnevezését
- A szoftver verziószámát
- A szoftver regisztrációs kódját
- A szoftverhez tartozó licence szerződés számát
- A szoftver licence hány telepítésre ad lehetőséget

17.5 A szoftvercsomagok változtatására vonatkozó korlátozások

A szoftvercsomagok módosítási szándékától lehetőleg el kell tántorítani a kezdeményezőket. Amennyire az csak lehetséges, és a gyakorlatban az kivihető, a szállító által gyártott szoftvercsomagot módosítás nélkül kell

használni. Ahol mégis lényegesnek tartják egy szoftvercsomag módosítását, a következő pontokat kell megfontolni:

- annak lehetőségét, hogy a kívánt változtatást a szállítótól is meg lehet kapni a program szabályos aktualizálásaként, frissítéseként;
- annak kockázatát, hogy a beépített ellenőrzési mechanizmusokat és óvintézkedéseket és az integritást fenntartó folyamatokban kárt okoznak;
- kell-e kérnünk a szállító hozzájárulását és egyetértését;
- annak következményeit, hogy a szervezet a szoftver további karbantartásáért - épp a végrehajtott változások eredményeként - maga válik felelőssé.

Amennyiben a változtatást lényegesnek tartjuk, az eredeti szoftvert meg kell őrizni és a változtatást egy egyértelműen azonosított másolaton kell végrehajtani. Minden egyes változtatást teljes egészében tesztelni és dokumentálni kell azért, hogy szükség esetén ismét alkalmazni lehessen a szoftver jövőbeli, javított kiadásaihoz.

18. Védelem a rosszindulatú szoftver ellen

18.1 A vírusvédelmi feladatok, felelősségek

A szervezetnél a vírusvédelmet egységesen kell kezelni. A vírusvédelmi feladatok ellátásáért egy személyben az **IT üzemeltetést végző személy** a felelős. Feladatai:

- Részt vesz a vírusvédelmi eszközök kiválasztásában, felügyeli azok rendszeresítését, és telepítését.
- Részt vesz a vírusvédelemmel kapcsolatos oktatási és tudatosítási feladatok szervezésében és lebonyolításában.
- Rendszeresen értékeli a vírusvédelmi események emlékeztetőit, szükség esetén javaslatot tesz fegyelmi vizsgálat lefolytatására.
- Felügyeli a vírusvédelmi eszközök működőképességét.
- Vírusfertőzés esetén:
    - Információkat gyűjt a vírusfertőzés főbb jellemzőiről (fertőzés módja, mértéke, stb.).
    - Meghatározza a vírusmentesítéshez szükséges mentesítési eljárásokat, megbecsüli azok erőforrás igényét, idejét.
    - Felügyeli a vírusmentesítés folyamatát, szükség esetén kapcsolatot tart fenn a vírusvédelmi cégek tanácsadóival.
    - Folyamatosan tájékoztatja a szervezeti egységek vezetőit.
    - Felügyeli a visszaállítás folyamatát. Amennyiben minden rendszert sikerült visszaállítani normál működésre, javaslatot tesz a katasztrófa-menedzser részére vírusriadó visszavonásáról.
    - Kivizsgálja a fertőzés okait, szükség esetén javaslatokat tesz a vírusvédelmi rendszer módosításaira, illetve a fegyelmi eljárások végrehajtására.
- Folyamatosan tájékozódik az újabb vírusfenyegetettségekről, és vírusvédelmi eszközökről.
- Rendszeresen felülvizsgálja a vírusvédelmi eszközök beállításait, szükség esetén javaslatokat tesz azok módosítására.

- Végrehajtja a vírusvédelmi eszközök telepítését, végrehajtja a jóváhagyott beállításokat.
- Tájékoztatást vagy oktatást tart a felhasználóknak a vírusvédelemről.
- Tervezi és nyomon követi a vírusvédelmi eszközök optimális életciklusát, szükség esetén javaslatokat tesz az eszközök fejlesztésére
- Megoldja a vírusvédelemben előforduló váratlan vagy tisztázatlan technikai problémákat.

18.2 Általános előírás

Elővigyázatossági intézkedésekre van szükség ahhoz, hogy rosszindulatú szoftver betelepülését megelőzzük és észleljük. A szoftver és az információ-feldolgozó eszközök igencsak sérülékenyek az olyan rosszindulatú szoftverek betelepülésével szemben, mint a számítógépvírusok, a hálózati férgek, a trójai falovak és a logikai bombák.

A felhasználóknak tilos a munkaállomásukon, hordozható számítógépükön alkalmazott vírusvédelmi szoftver aktív védelmének kikapcsolás, vagy a védelmi beállításának megváltoztatása.

A szervezetnél a védendő információ-feldolgozó eszközök hatékony védelmének érdekében valósidejű védelmet kell kialakítani.

A szervereken és munkaállomásokon a valósidejű védelemnek folyamatosan bekapcsolva kell lennie, hogy biztosítsa a felhasználói munka során igénybe vett állományok (adatok, programok) használat előtti vírusellenőrzését.

Biztosítani kell, hogy a munkaállomásokon a valósidejű védelmet a felhasználók ne tudják kikapcsolni. Amennyiben a valósidejű védelem a detektált vírus eltávolítására nem képes, a vírusvédelmi rendszer automatikus értesítést küld a felhasználó számára, és a fertőzés gyanús állományt a rendszer automatikusan karanténba helyezi.

A felhasználóknak tudatában kell lenniük, hogy a jogosulatlan és a rosszindulatú szoftverek milyen veszélyesek, a vezetőknek, ahol csak lehet, különleges óvintézkedéseket és ellenőrzési mechanizmusokat kell bevezetniük azért, hogy észleljék azokat a szoftvereket és megakadályozzák betelepülésüket.

Különösen az a lényeges, hogy a személyi számítógépek esetében óvintézkedéseket tegyünk a számítógépvírusok észlelésére és betelepülésüknek megelőzésére.

A következő ellenőrzési mechanizmusokat, óvintézkedéseket kell megfontolni:

- egy hivatalos szabályzat létrehozását, amely megköveteli a szoftver licencekben rögzített szabályoknak történő megfelelést és megtiltja a jogtalan szoftver használatot; (**Munkavállalói Nyilatkozat és Informatikai és Információbiztonsági Szabályzat Felhasználóknak** dokumentum)
- egy olyan óvintézkedés létrehozását, amely véd az olyan kockázatok ellen, amelyek adatállományoknak és szoftvereknek külső hálózatokból történő letöltésével, vagy bármely más adathordozó segítségével történő megszerzésével kapcsolatosak, és amely szabályzat azt is meghatározza, hogy milyen védelmi intézkedéseket kell hozni;
- a vírusokat észlelő (detektáló) és hatásait kijavító szoftver telepítését és szabályos időközönkénti frissítését, valamint a

számítógépek és az adathordozók rendszeres átvizsgálását, akár elővigyázatossági óvintézkedésként, akár rutin feladatként;

- a bizonytalan eredetű, vagy nem engedélyezett forrásból származó elektronikus adathordozón kapott, vagy a nem megbízható hálózaton keresztül kapott állományok használat előtti vírusfertőzöttség ellenőrzését;
- minden elektronikusan kapott levélmelléklet és adatállomány-letöltések rosszindulatú szoftverrel való fertőzöttségének használat előtti ellenőrzését. Ez az ellenőrzés különböző helyeken történhet, például az elektronikus levelezőrendszer szerverén, asztali számítógépeken, vagy akkor, amikor a szervezet hálózatába belépnek;
- a rendszerek vírusvédelmével foglalkozó, ezek használatát betanító, a vírustámadásról jelentést készítő és azokból helyreállítást végző szervezeti eljárásokat, folyamatokat, feladat-, hatás és felelősségi köröket meg kell határozni;
- helyes IT Akciótervet, amelyek a vírustámadás utáni helyreállításra vonatkoznak, beleértve valamennyi szükséges adatmentési, szoftverrendszer mentési és visszaállítási eljárásokat;
- azokat az eljárásokat, amelyek a rosszindulatú szoftverrel kapcsolatos információk helyességét hivatottak igazolni és gondoskodnak arról, hogy a vírusfigyelmeztető kiadványok pontosak és információban gazdagok legyenek. A rendszergazdának kell gondoskodnia arról, hogy a megtévesztés és a valódi vírus közötti megkülönböztetésre megbízható forrásokból származó anyagokat használjanak fel, tekintélyes szaklapokat, megbízható Internet helyekről, vagy vírusvédő szoftverek szállítóitól.
- A vírusfertőzés veszélyének csökkentése érdekében ki kell használni azokat a rendelkezésre álló technikai eszközöket, amelyek nem vírusvédelmi feladatokat látnak el, de egyes funkcióik alkalmas a vírusok elleni védekezésre, mint például:
    - a hálózati aktív eszközök (nem használt portok letiltása);
    - tartalomszűrő eszközök (vírusok jellemző karakter sorozatainak kiszűrése);
    - betörés detektáló (IDS) eszközök.

18.2.1 Vírusvédelmi események

A fertőzés nagyságától függően az alábbi területeket különböztetjük meg:

- **elszigetelt:** ha az irodán belül, 24 órán belül legfeljebb 2 fertőzés fordul elő, és egy védendő eszközön sem ismétlődött a fertőzés,
- **ismétlődő:** ha egy bizonyos eszköz egy nap többször, vagy több egymás utáni napon megfertőződik;
- **sorozatos:** ha az irodán belül, 24 órán belül 8-10 fertőzés történt;
- **tömeges:** fentieknél nagyobb 24 órán belüli fertőzésszám.

Fertőzés az is, amit nem a vírusvédelmi eszközök jeleznek, hanem ami a felhasználók és rendszergazdák jelzései alapján valószínűsíthető.

18.2.2 Események szintjei

1. szintű („C" típusú kategória) vírusvédelmi eseménynek minősül, ha a víruskereső elszigetelt fertőzést észlelt, és az előírt vírusmentesítést elvégezte.

2. szintű („B" típusú kategória) vírusvédelmi eseménynek minősülnek a következők:

- A vírusvédelem elszigetelt fertőzést észlel, de nem tudja a vírusmentesítést elvégezni.
- A vírusvédelem sorozatos vagy ismétlődő vírust észlelt, és a vírusmentesítést elvégezte.
- A vírusvédelmi menedzsment munkaállomás azt észleli, hogy valamelyik kiemelt eszközön nem fut a vírusvédelem.
- Az adatvédelmi munkaállomás azt észleli, hogy valamelyik munkaállomáson 3 napja nem fut a vírusvédelem.
- A vírusvédelmi eszköz jelzi, hogy egy számítógépen 7 napnál régebbi a szignatúra.
- Kivételt képez az az eset, amikor a menedzsment felület a saját adatbázisa alapján azért mutat régi szignatúrákat, mert az adott számítógép több napja nincs bekapcsolva vagy már nem a hálózat része.
- A központi vírusvédelmi eszközök valamelyikének 1 napnál hosszabb üzemképtelensége.
- Itt fel nem sorolt egyéb esetek, amikor a vírusvédelmi rendszerbe bármi okból illetéktelenül beavatkoznak.

3. szintű („A" típusú kategória) vírusvédelmi eseménynek (**IT akcióterv**) minősül:

- Tömeges vírusfertőzés.
- Sikertelen vírusmentesítés sorozatos, vagy ismétlődő fertőzés esetén.

18.3 Vírusfertőzések kockázatának csökkentési lehetőségei

18.3.1 Korlátozások operációs rendszer szinten

A vírusvédelmi kockázatok csökkentése érdekében lehetőség szerint az operációs rendszerek szintjén korlátozásokat kell bevezetni. A korlátozások terjedjenek ki az alábbiakra:

- A munkaállomásokon és szervereken meg kell akadályozni a **nem használt** távdiagnosztikai portok, távoli hozzáférést biztosító szolgáltatások elérését.
- A munkaállomásokon és szervereken meg kell akadályozni a nem használt szervizek, beépített alkalmazások hozzáférését.
- A korlátozásokat a telepítő image-ben, illetve a csoportos és helyi házirendben is alkalmazni kell.

18.3.2 Szoftverek biztonsági frissítése

A vírusfertőzések kockázatainak csökkentése érdekében a szervezetnél meg kell oldani az alkalmazott szoftverek folyamatos biztonsági frissítését. A frissítéseket úgy kell ütemezni, hogy egy sérülékenység nyilvánosságra hozatala és a biztonsági frissítése között a legkevesebb idő teljen el.

Fejlesztések alkalmával kötött szerződésekben meg kell fontolni a fejlesztésre kerülő szoftver biztonsági frissítéseiről szóló utógondozási feladatokat.

19. Tűzfalak

A nyilvános hálózatokhoz történő kapcsolódás vonatkozásában megfelelő tűzfalakat kell kialakítani a szolgáltatás megtagadása, illetve a belső erőforrásokhoz történő jogtalan hozzáférések megakadályozása érdekében. Minden alkalmazással, illetve infrastruktúrával kapcsolatos tevékenységhez kötődő információáramlást ellenőrzés alatt kell tartani mindkét irányban, és meg kell védeni a túlterheléses támadással szemben.

A tűzfalaknak aktív védelmet kell nyújtaniuk, megakadályozva az illetéktelen hozzáférést a tűzfal által védett adatokhoz, adatbázisokhoz.

Tűzfallal kell védeni a központi rendszereket, és el kell választani egymástól a produktív, a tesztelői és a fejlesztői környezetet annak érdekében, hogy egyrészt az adatokhoz csak dedikált, ellenőrzött utakon juthassanak el a felhasználók, másrészt kizárólag az arra jogosult felhasználók férhessenek a számukra engedélyezett adatállományokhoz.

A központi rendszerek tűzfalai által biztosított védelem tervezése, a tűzfalak karbantartása a rendszergazda feladata.

20. Távmunka

A távmunka során távközlési technológiákat alkalmazunk arra, hogy a munkatársak a szervezet állandó telep-helyétől távol végzett munkáját lehetővé tegyük. A távmunka munkahelyének megfelelő védelmét a szóban forgó helyszínen kell létrehozni azért, hogy a berendezés és az információ ellopása, az információ felfedése és nyilvánosságra hozatala, a szervezet belső rendszereihez az illetéktelen hozzáférés vagy az informatikai szolgáltatásokkal való visszaélés ellen megvédjük.

Fontos, hogy a távmunkára a vezetőség adja meg az engedélyt és végezze annak ellenőrzését, ugyanakkor az effajta munkavégzéshez alkalmas intézkedéseket kell kialakítani.

A szervezeteknek a távmunka-végzési tevékenységek ellenőrzéséhez ki kell fejleszteniük a szabályozást, az eljárásokat és a szabványokat. A szervezeteknek csak akkor szabad a távmunka- végzési tevékenységekre felhatalmazást megadniuk, ha meg vannak elégedve azzal, ahogyan a biztonsági óvintézkedéseket és ellenőrzési mechanizmusokat kialakították, és hogy ezek megfelelnek a szervezet biztonsági szabályozásának. A következőket kell kialakítani:

- a távmunka-végzési telephely meglévő fizikai biztonságát, figyelembe véve mind az épület, mind a környezet fizikai biztonságát;
- a tervezett távmunka-végzési környezetet;
- a hálózat, a távközlés biztonsági követelményeit, figyelembe véve azt az igényt, hogy a szervezet belső rendszereihez távolról fognak hozzáférni, a távolról elért és a hálózati vonalakon továbbított információ bizalmasságának, titkosságának fokától függően, valamint a szervezet belső informatikai rendszerei bizalmasságának, titkosságának fokától függően;
- az információhoz és erőforrásokhoz történő bármely illetéktelen hozzáférés fenyegetését, amelyet más személyek okozhatnak, akik ugyancsak használják a „távmunka telephely” helyiségeit, például a család vagy a barátok.

21. Home Office szabályzat

Az otthoni munkavégzés alapvetően kizárólag a munkavégzés helyszínében különbözik az irodai munkavégzéstől. Ennek értelmében ugyanolyan elvárások és kötelezettségek tekintendők érvényesnek az elvégzett munka mennyisége, minősége, hatékonysága és adminisztrálása szempontjából, mint az irodai munkavégzés esetében.

A szabályzat hatálya a Munkáltatónál munkaviszonyban álló **HOME OFFICE** munkavégzés igénylésének lehetőségével foglalkoztatott valamennyi munkavállalóra kiterjed, valamint a **HOME OFFICE** igénylésének lehetőségével foglalkoztatott munkavállalók munkáltatói jogkörgyakorlóira és/vagy munkaidő beosztással megbízott másodlagos munkáltatói jogkörgyakorlókra is kiterjed.

21.1 Jogi keretrendszer

A **HOME OFFICE** a munkáltató telephelyétől elkülönült helyen, egyedi engedély alapján, külön jóváhagyással, alkalmi jelleggel folytatott olyan tevékenység, amelyet információtechnológiai vagy számítástechnikai eszközzel végeznek és eredményét elektronikusan továbbítják. Az engedélyezett otthoni, **HOME OFFICE** munkavégzésre, illetve távmunkára speciális munkavédelmi szabályok vonatkoznak (1993. évi XCIII. tv. a Munkavédelemről), így csak a munkáltató által munkavédelmi szempontból előzetesen megfelelőnek minősített munkahelyen folytatható.

A Munkáltató által előre engedélyezett **HOME OFFICE** munkavégzés megkezdése előtt a munkavállalónak meg kell adnia a **HOME OFFICE** munkavégzés pontos helyszínét, amelyet a Munkáltató előzetesen és később szúrópróba módszerével, előzetes bejelentést követően ellenőrizhet.

HOME OFFICE-ban értelemszerűen csak olyan feladatok végezhetők el, melyek jellegüknél fogva erre alkalmasak.

Hivatkozások

- 2012. évi 1. tv. a Munka Törvénykönyvéről
- 1993. évi XCIII. tv. a Munkavédelemről
- 50/1999 . (Xl.3.) EüM rendelet a képernyő előtti munkavégzés minimális egészségügyi és biztonsági követelményeiről

21.2 Munkakörnyezet kötelező jellemzői

A **HOME OFFICE** keretében történő munkavégzés helyéről és berendezésről (ide nem értve a munkáltató által biztosított notebookot vagy laptopot és mobiltelefont), a munkavégzés feltételeinek biztosításáról (zavartalan munkakörnyezet a teljes munkaidő - alapesetben 8 óra - alatt) a munkavállalónak kell gondoskodnia, vállalva az ezzel kapcsolatos minden költséget.

HOME OFFICE munkavégzés esetén nem az egész lakás/ház minősül munkahelynek, hanem a szoros értelemben vett azon helyiség vagy helyszín, ahol a munkavállaló munkát végez.

21.3 Home office munkavégzés céljára szolgáló helyiség, helyiségrész követelményei

HOME OFFICE munkahely olyan lakóingatlanban alakítható ki, mely alkalmas a feladatok ellátására a munkahellyel kapcsolatos általában vett elvárások tekintetében. A lakóingatlanban biztosítottnak kell lenni a munkavédelmi törvényben meghatározott egészséges és biztonságos munkavégzés feltételeinek. A munkahely kialakítását megelőzően és annak fenntartása alatt a munkáltató és megbízottai a munkavállalóval való előzetes (1 munkanap) időpont egyeztetést követően jogosultak ellenőrizni a feltételek meglétét.

HOME OFFICE munkahelyet is magában foglaló helyiséget/helyiség részt a munkavállaló biztosítja, figyelemmel arra, hogy a munkahely csak huzamos emberi tartózkodásra szolgáló helyiségben alakítható ki. Nem hozható létre **HOME OFFICE** munkahely pince szinten, garázsban.

Huzamos tartózkodásra szolgáló helyiség minimális méretei:

- belmagasság: 2,5 m
- alapterület: minimum 6 m2
- légtérfogat: minimum 15 m3

Egyéb követelmények:

- A **HOME OFFICE** munkahelynek fényvédelemmel (függöny, redőny stb.) ellátott ablakkal kell rendelkeznie.
- A **HOME OFFICE** munkahelyet úgy kell megtervezni, hogy a munkavállalónak elegendő tere legyen a testhelyzete változtatásához és a mozgáshoz. A munkahely megközelítéséhez 80 cm széles hely szükséges a biztonságos közlekedés érdekében.
- Hideg évszakban 20-22 °C léghőmérsékletet kell biztosítani.
- Korlátlan ivóvíz hozzáférést szükséges biztosítani.

Minimálisan szükséges eszközök és berendezések:

- Munkavégzésre alkalmas munkaasztal
- Ergonomikus kialakítású munkaszék
- Számítástechnikai eszközök

21.4 Informatikai követelmények és eszközhasználat

A legfontosabb lényegi vonása a **HOME OFFICE**-ban végezhető feladatoknak, hogy infokommunikációs eszközök segítségével számítástechnikai eszközön végezhetők és továbbíthatók a munkáltató és/vagy ügyfél részére.

A Munkáltató által biztosított eszközöket kizárólag a Home Office keretében foglalkoztatott munkavállaló használhatja, kizárólag munkavégzés céljából.

A Munkáltató akár közvetlenül, akár távoli eléréssel jogosult betekinteni a munkavállaló által használt számítástechnikai eszközökbe.

A **HOME OFFICE** munkavégzés során a munkavállalónak biztosítani kell a munka eredményének továbbításához szükséges stabil széles sávú internet kapcsolatot, valamint a vállalati internetes (pl. Skype) megbeszéléseken a többi résztvevő számára is a megfelelő hangminőséget és a zavaró környezeti zajok kizárását (pl. porszívó hangja, gyereksírás, kutyaugatás és egyéb zörejek).

21.5 Munkaidő beosztása

A **HOME OFFICE**-ban munkát végző munkavállaló munkaidejét a Munkáltató osztja be, tehát az is az irodai ill. telephelyi munkavégzésre vonatkozó munkaidőbeosztási szabályok alá tartozik, és a Munkáltató ezeknek az időtartamoknak a betartását is ellenőrizheti és nyilvántarthatja.

21.6 Home office munkavégzésre vonatkozó előzetes általános engedélyezés

- Munkavállaló feladatai munkaköre jellege alapján részben **HOME OFFICE** keretében is elláthatóak.
- Munkavállaló biztosítja a **HOME OFFICE** munkavégzéshez megfelelő munkakörnyezetet.

21.7 Eljárásrend

- A **HOME OFFICE**-ban dolgozó munkavállalóknak a munkaidő megkezdésekor munkavégzésrealkalmas állapotban kell lenniük. (Pl.: elérhetőnek kell lenniük, telefonhívásra tudni kell reagálniuk, az előírt vagy szokványos határidőn, de legalább 15 percen belül.)
- A **HOME OFFICE**-ban dolgozó munkavállalókkal közvetlen felettesük napi szinten egyeztet (előre meghatározott időben és formában) az elvégzendő feladatokról, a folyamatban lévő vagy újonnan beérkezett igényekről, hibajegyekről.
- A **HOME OFFICE**-ban dolgozó munkavállalóknak felettesük határozza meg a feladatok elosztását, prioritását, az érintett kollégával egyeztetve a feladatok erőforrás- és időigényét.
- A **HOME OFFICE**-ban dolgozó munkavállaló szükség esetén eszkalálja az esetet, felettesétől további erőforrásokat, illetve külső támogatást igényel.
- A **HOME OFFICE**-ban dolgozó munkavállaló munkaszerződésében meghatározott munkarend szerint dolgozik felettesével egyeztetett, részére kiadott feladatok megoldásán.
- A **HOME OFFICE**-ban dolgozó munkavállaló, amennyiben szükséges, előzőleg egyeztetett időpontban és formában egyeztet ügyfelekkel.

- A **HOME OFFICE**-ban dolgozó munkavállaló a munkanap végén előre egyeztetett időben és formában áttekinti és értékeli felettesével a napközben végrehajtott feladatok státuszát.

22. Kriptográfia

Meg kell védeni az információ titkosságát, bizalmasságát, hitelességét, épségét és sértetlenségét. Kriptográfiai rendszereket és technikákat kell alkalmazni mindazon információ védelmére, amelyeket biztonsági szempontból kockázatosnak tekintünk, és amelyet más ellenőrzési mechanizmusok és óvintézkedések nem látnak el kellő védelemmel.

A szervezetnek ki kell dolgoznia az irányelveit arról, hogy információja megvédése érdekében hogyan fogja használni a kriptográfiai eljárásokat, ellenőrzési mechanizmusokat. Erre a szabályozásra azért is szükség van, hogy maximálisan ki lehessen használni a kriptográfiai módszerek alkalmazásának előnyeit, hogy a lehető legkisebbre lehessen lecsökkenteni alkalmazásuk kockázatait, ugyanakkor elkerülhető legyen a helytelen és pontatlan használat. Bevezetése esetén következőket kell figyelembe venni:

- a szervezet vezetésének álláspontját abban a tekintetben, hogy az egész szervezetben kriptográfiai ellenőrzési mechanizmusokat és óvintézkedéseket használjanak, beleértve azokat az általános irányelveket és szabályokat, amelyek a szervezet információinak védelmére vonatkoznak;
- a kriptográfiai kulcskezelés megközelítését, beleértve mindazokat a módszereket, amelyekkel a titkosított információt vissza lehet nyerni, ha a kulcs elveszett, nyilvánosságra került vagy megsérült;
- szerepeket és felelősségeket, például, hogy ki a felelős a szabályozás és az irányelvek megvalósításáért, a kulcskezelésért;
- azt, hogy mely szabványokat alkalmazzunk ahhoz, hogy az egész szervezetben eredményes legyen a megvalósítás (mármint, hogy melyik szervezeti folyamatban melyik megoldást alkalmazzuk).

23. Digitális aláírás

A digitális aláírás egy olyan informatikai eszköz, amivel védhetők az elektronikus okmányok, okiratok, dokumentumok hitelessége, épsége és sértetlensége. Az elektronikus kereskedelemben például arra is használhatóak, hogy szükség esetén ellenőrizzük az aláíró személy személyazonosságát, és az ellenőrizhető, hogy vajon a már aláírt okmány tartalmán változtattak-e.

A digitális aláírások bármilyen elektronikus dokumentumformára alkalmazhatók, hiszen ezeket mind elektronikusan fogják feldolgozni, így például alkalmazhatjuk a következő tranzakciók aláírására: elektronikus fizetésre, pénz átutalására, szerződésekre és megállapodásokra.

A digitális aláírások olyan kriptográfiai technikákkal valósíthatók meg, amelyek egyértelműen összetartozó kulcspárokra támaszkodnak, ahol az egyik kulccsal készül az aláírás (a magánkulccsal), míg egy másik kulccsal ellenőrzik az aláírás helyességét, hitelességét (a nyilvános kulccsal).

Különös gondot kell fordítani a magánkulcs titokban tartására. Azért kell ezt a kulcsot titokban tartani, mert bárki, aki hozzáfér ehhez a kulcshoz, úgy tud vele dokumentumot, okmányt aláírni, például fizetést, szerződést, hogy a tulajdonképpen kulcs igazi tulajdonosának az aláírását hamisítja rá. Továbbá fontos a nyilvános kulcs sértetlenségét, épségét is megóvni.

A szervezetnek elemeznie kell és döntenie kell, hogy milyen aláíró algoritmust és milyen hosszú kulcsot alkalmazzon. A digitális aláíráshoz alkalmazott kriptográfiai kulcsoknak különbözniük kell a titkosírásra alkalmazott kulcsoktól.

A digitális aláírások alkalmazásakor figyelembe kell venni minden hatályos jogszabályt, amely azokat a feltételeket írja elő, amelyek mellett a digitális aláírás jogilag hatályos kötelezettséget hoz létre. Szükség lehet arra is, hogy a digitális aláírás jogi következményeinek meghatározására két fél között előíró szerződést vagy egyéb megállapodást kössünk ahhoz, hogy a digitális aláírások használatát támogassuk, mert esetleg a jogi keretek e téren jogilag nem pontosan szabályozottak.

24. Az IBSZ-hez kapcsolódó szabályzatok

- Informatikai és Információbiztonsági Szabályzat és Irányelvek Felhasználóknak
- Jogosultági és hozzáférési szabályzat
- IT üzletmenet-folytonosság és katasztrófakezelési szabályzat
- Információbiztonsági Incidenskezelési Szabályzat

24.1 A szabályzatok által meghivatkozott dokumentumok

- Munkavállalói Nyilatkozat
- IT-Akciótervek

24.2 A szabályzatok által meghivatkozott nyilvánartások

- Kockázati mátrix
- Adatvagyon leltár
- HW és SW leltár
- Jogosultság nyilvántartó

24.3 A szabályzatok által meghivatkozott formanyomtatványok

- IBIR oktatási jegyzőkönyv
- Fontos információk és elérhetőségek
- IBIR Incidens jegyzőkönyv
- Adathordozó megsemmisítési jegyzőkönyv
- Eszköz átadás-átvételi jegyzőköny