Végrehajtását elrendelem:

Tóka István bv. ezredes
bv. tanácsos
ügyvezető

Az Ipoly Cipőgyár Kft.

Informatikai Biztonsági Szabályzata

Hatályba lépés időpontja: 2021. szeptember 30.

I. A szabályzat célja

Az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) célja az Ipoly Cipőgyár Kft.-nél (a továbbiakban: Kft.) működő informatikai rendszerek biztonságos használatának szabályozása, a veszélyeztető és fenyegető tényezők felmérésének, valamint a velük szembeni védekezésnek a szabályozása.

II. A szabályzat hatálya

A szabályzat **személyi hatálya** kiterjed a Kft. informatikai rendszerével kapcsolatba kerülő teljes személyi állományra.
Az IBSZ rendelkezéseit a Kft.-vel szerződéses jogviszonyban álló magánszemélyek, jogi személyek, egyéb szervezetek: külső támogatók és partnerek vonatkozásában is érvényesíteni kell.

A szabályzat **tárgyi hatálya** kiterjed:

- a védelmet élvező adatok teljes körére, függetlenül a felmerülési és feldolgozási helyüktől, idejüktől, az adatok fizikai megjelenési formájától,
- a Kft. tulajdonában és használatában lévő, illetve a személyi állomány által használt valamennyi információs rendszerre (számítógépek, nyomtatók, külső háttértárolók), számítástechnikai eszközre (aktív hálózati elemek, adathordozók), azok műszaki dokumentációira,
- a Kft. teljes informatikai infrastruktúrájára (szerverek, kliensek, számítógépes vezetékes, illetve vezeték nélküli hálózatok, hálózati aktív eszközök, szünetmentes áramforrások),
- a Kft. szervezeti egységei által használt szoftverekre (rendszerprogramok, segédprogramok, alkalmazások, operációs rendszerek),
- az informatikai folyamatban szereplő összes dokumentációra,
- az adatok felhasználására vonatkozó utasításokra,
- az adathordozók felhasználására és tárolására.

A szabályzat **területi hatálya** kiterjed a Kft. valamennyi szervezeti egységére, a Kft. székhelyére, telephelyére és fióktelepeire egyaránt, az ott található irodahelyiségekre. Irodán kívüli használatra kiadott eszközök esetében azok használatának helyére.

III. Általános rendelkezések

1. A társaság informatikai biztonsági stratégiája

A Kft. célja olyan megbízható - megfelelő információvédelemmel ellátott, megfelelő működésű - információs rendszer felállítása, fejlesztése, használata, amely a Kft. működését biztonságosan támogatja, rugalmasan követve a vele szemben a Kft. fejlődéséből és a gazdasági, valamint a jogszabályi környezetből keletkező igényeket.

Továbbá cél a biztonság olyan szintjének előírása, amely megfelel a Kft. speciális helyzetéből adódó követelményeknek (mind fizikai, mind a foglalkoztatás jellegéből adódóan), ugyanakkor gazdaságosság szempontjából optimális előírásokkal dolgozik.

A Kft. célja a jelen szabályzat személyi hatálya alá tartozók folyamatos tájékoztatása a Kft. informatikai rendszerének hasznosságáról, az ezzel kapcsolatos saját felelősségükről, ezáltal érdekeltté téve őket a rendszer működtetésében és a védelmi előírások betartásában.

2. Feladatok, hatáskörök, felelősség

Ügyvezető:

- felel az elektronikus információs rendszerek védelméért,
- biztosítja a biztonságos munkavégzéshez és adatkezeléshez szükséges feltételeket,
- gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, a személyi állomány információbiztonsági ismereteinek szinten tartásáról,
- rendszeres biztonsági ellenőrzések útján meggyőződik arról, hogy a Kft. elektronikus információs rendszereinek biztonsága megfelel a jogszabályoknak, valamint a jelen szabályzatban előírt követelményeknek,
- biztonsági esemény bekövetkezésekor gondoskodik a gyors és hatékony reagálásról,
- kijelöli az adatvédelmi tisztviselőt, ellenőrzi az általa végzett munkát, és az informatikus-rendszergazda munkáját,
- biztosítja az informatikai biztonság feltételeit,
- felelős a jelen szabályzatban foglaltak betartatásáért.

Informatikus-rendszergazda:

- biztosítja az informatikai rendszer üzemképességét és megszervezi a műszaki ellátását,
- felügyeli és előkészíti a rendszer módosítását, fejlesztését,
- irányítja és ellenőrzi a felhasználók informatikai rendszerrel kapcsolatos munkáját, a felhasználói jogosultságokat,
- gondoskodik a jelen szabályzatban foglaltak következetes és szakszerű végrehajtásáról,
- ellátja az adatfeldolgozás felügyeletét,
- ellenőrzi a biztonsági előírások betartását,
- folyamatosan figyelemmel kíséri a veszélyforrások körében bekövetkező változásokat, kockázatelemzést végez és kezdeményezi a szükséges intézkedések megtételét,
- folyamatosan ellenőrzi és koordinálja a szervízellátást,
- bármely szervezeti egységnél ellenőrizheti jelen szabályzat előírásainak betartását,
- a jelen szabályzat rendelkezéseit be nem tartó személyekkel szemben felelősségre vonást kezdeményezhet az adott szervezeti egység vezetőjénél,
- betekinthet az informatikai feldolgozásokkal kapcsolatos valamennyi iratba,
- javaslatot tesz az ügyvezető felé új, vagy kiegészítő berendezések, alkalmazások telepítésére, szerződésmódosításokra az általa felügyelt területen.

Adatvédelmi tisztviselő:

- a Kft. adatvédelmi tevékenységét szervezi és felügyeli,
- a jelen szabályzatban foglalt adatvédelmi feladatokat ellátja,
- részt vesz a feladatkörét érintő szabályozások elkészítésében és módosításában,
- figyelemmel kíséri az alkalmazott, módosított, új jogszabályokat, egyéb adatvédelmi előírásokat,
- betekintési joga van az adatvédelemmel kapcsolatos iratokba, dokumentációkba,

- a felhasználóknál ellenőrzi az előírt biztonsági követelmények betartását.

Felhasználók, a személyi állomány:

- kötelesek megismerni a jelen szabályzatban foglaltakat, és munkájuk során alkalmazniuk kell a rájuk nézve kötelezően előírtakat,
- a Kft. által kezelt információkat kötelesek biztonságosan kezelni,
- kötelesek a hatályos biztonsági szabályokat megismerni, betartani,
- személyes felelősséggel tartoznak a munkaeszközeikért, a felhasználói munkaállomásokért, az azokon tárolt vagy rajtuk keresztül elérhető adatok, felhasznált információk védelméért,
- kötelesek közvetlen vezetőjüknek jelenteni, ha olyan jelenséget vagy tevékenységet észlelnek, mely a hatályos biztonsági szabályokat sérti,
- a jelszavak megválasztása és használata során a helyes biztonsági gyakorlatnak megfelelően kell eljárniuk,
- gondoskodniuk kell a felügyelet nélkül hagyott informatikai eszközök megfelelő védelméről.

3. A felhasználók kötelmei

Felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre.

A felhasználó jogosult a munkavégzéshez szükséges infokommunikációs eszközöket használni, a használathoz szükséges ismereteket dokumentáció vagy képzés formájában megkapni.
A felhasználó a rendelkezésére bocsátott infokommunikációs eszközöket csak a Kft. céljaival, feladataival kapcsolatos, a munkaköri feladatai ellátásához szükséges tevékenység céljára, rendeltetésszerűen, a számára megállapított jogosultságok keretén belül, a jogszabályokkal és szabályozókkal összhangban használhatja.
A felhasználó köteles a használatra átvett informatikai eszközöket az elvárható gondossággal kezelni és a károsodástól védeni.
A felhasználó személyes anyagi felelősséggel tartozik az általa szándékosan vagy gondatlansággal az infokommunikációs eszközökben okozott, bizonyított károkért.
A munkaállomás illetéktelen hozzáférés elleni védettségéért, a munkaállomáson végzett minden tevékenységért a bejelentkezéstől a kijelentkezésig a felhasználó a felelős.
A munkaállomás illetéktelen hozzáférés elleni védelme érdekében a felhasználó köteles a munkaállomást zárolni, ha ez nem lehetséges, köteles a munkaállomásból kijelentkezni vagy azt kikapcsolni, amennyiben azt felügyelet nélkül hagyja. A munkaállomást a munkaidő végén vagy a munkavégzés befejezésekor ki kell kapcsolni.
Közös használatú hálózati nyomtató esetében a felhasználó a kinyomtatott dokumentumokat köteles a nyomtatóból eltávolítani.
A felhasználó a rendelkezésére bocsátott mobil infokommunikációs eszközöket és adathordozókat köteles megőrizni, az illetéktelen hozzáféréstől személyes felügyelettel vagy az eszköz, adathordozó elzárásával megvédeni.
A felhasználó köteles az általa észlelt informatikai biztonsági eseményről értesíteni közvetlen vezetőjét, aki gondoskodik a szükséges intézkedések megtételéről.
A felhasználó köteles a rendszer általa észlelt rendeltetésellenes működését a közvetlen vezetője részére haladéktalanul bejelenteni.

4. Információbiztonság-tudatosság, oktatás

Minden a Kft. által kezelt információhoz hozzáférő személyi állományi tagot megfelelő biztonság-tudatossági oktatásban kell részesíteni.
A személyi állományt a Kft.-nél végzendő tevékenység megkezdése előtt jelen szabályzat tartalmára épülő információbiztonsági képzésben kell részesíteni.

5. Eljárás a szabályzat rendelkezéseinek megsértése esetén

A biztonsági szabályok betartása minden személyi állományi tagra, a Kft.-vel szerződéses jogviszonyban álló személyre nézve kötelező.
Azon személyi állományi tag esetén, aki a biztonsági szabályokat súlyosan megsértette, fegyelmi eljárás lefolytatásának van helye.
A biztonsági szabályok be nem tartásával okozott kárért a személyi állomány tagja helytállni köteles.

6. Az informatikai rendszerek biztonsági osztályba sorolása

A Kft.-nél működő informatikai rendszerek mind az információvédelem, mind a megbízható működés szempontjából alapbiztonsági osztályba tartoznak.

IV. A hozzáférés szabályozása

Az adatok és információk védelmét a Kft. belépési azonosítók használatával támogatja. A Kft. információs rendszerében alapbiztonsági fokozatnak megfelelően kell az egyéni és/vagy csoportos szerepeket és jogosultságokat kiosztani, illetve karbantartani.

A hozzáférések kiosztásánál biztosítani kell, hogy egy azonosító csak egy felhasználóhoz kerüljön, illetve egy felhasználóhoz csak egy azonosító tartozzon. Törekedni kell arra, hogy az azonosítókhoz tartozó jelszavak ne legyenek könnyen kitalálhatóak, legalább 6 karakter hosszúak legyenek, tartalmazzanak kis- és nagybetűket, valamint számokat is.

Az informatikus - rendszergazda e körben:

- megtervezi a hálózati hozzáférési jogosultságokat,
- a jogokat kiosztja, változtatja, törli, a jelszavakat nyilvántartja,
- ellenőrzi az azonosítók használatát, az illetéktelen hozzáférési próbálkozásokat,
- nyilvántartja a hozzáférési jogosultságokat, biztosítja azokat az arra illetékes vezetőknek.

Jogosultságok:

Az informatikus - rendszergazda meghatározza a hozzáférési jogokat, privilégiumokat.

A szoftver készítő - fejlesztő programokat módosíthat.

Felhasználó I. adatokat vihet be.

Felhasználó II. az adatokat ellenőrzi, módosíthatja és felhasználhatja.

Felhasználó III., külső ellenőrző szervek (BVOP, Bv. Holding Kft., NAV, ÁSZ, könyvvizsgáló, stb.) az adatokat csak felhasználhatják/lekérdezhetik.
Egyéb személy nem férhet hozzá az adatokhoz.

A karbantartást végző külső szakemberek részére az adat - és titokvédelmi előírások betartását is biztosító hozzáférést kell elérhetővé tenni.

A hálózatokban a fontosabb rendszeresemények minimum 30 napon át rögzítésre kerülnek, a rögzített adatok lekérdezhetők és kinyomtathatók, így a:

- rendszerindítások, leállások, leállítások,
- rendszeróra állítások,
- be - és kijelentkezések,
- programleállások.

V. A számítógépes rendszerek biztonsági ellenőrzése

A Kft. informatikai rendszerének ellenőrzésére az ügyvezető vagy az általa megbízott, a nevében eljáró szakember és az informatikus - rendszergazda jogosult.

VI. A fejlesztés informatikai biztonsági feladatai

A Kft. informatikai fejlesztései során alkalmazni kell a Beszerzési Eljárásrend, valamint a számviteli előírások vonatkozó rendelkezéseit. Alapbiztonsági osztályra nézve a fejlesztés fázisai a következők:

- követelményrendszer megfogalmazása,
- globális rendszerterv készítése,
- részletes megvalósítási terv,
- megvalósítás,
- tesztelés,
- átadás.

Követelményrendszer felállítása:

- az igények körültekintő felmérése a jelenlegi és a várható jövőbeli feladatokat figyelembe véve,
- az igények megfogalmazása és egyeztetése az informatikus - rendszergazdával és az érintett szakterületek vezetőivel.

Globális rendszerterv:

- a fejlesztés adatbázisának megtervezése,
- a logikai, fizikai és kommunikációs rendszerkapcsolatok megtervezése,
- a szoftver és hardverigény megtervezése,
- az igényelt kezelőszemélyzet meghatározása,
- ajánlatkérő dokumentáció összeállítása, melynek elkészítése és megőrzése az informatikus - rendszergazda feladatkörébe tartozik.

A beszerzésnél törekedni kell független minősítő cég által kiállított minőségi bizonyítvánnyal és ellenőrzött referenciákkal rendelkező termékek vásárlására. Szoftverek esetén csak jogtiszta, megfelelő dokumentációval ellátott terméket szabad beszerezni és használatba venni.

Biztosítani kell a rendszer felfelé való kompatibilitását mind hardver, mind szoftver szempontból a rendszer bővíthetősége és az alkalmazói rendszerek hosszútávú működtethetősége miatt, az eladónak biztosítania kell a szavatosságot, jótállást és a támogatást.

Részletes megvalósítási terv:

A kiválasztott ajánlat ismeretében a fejlesztés környezetének, a telepítés, a tesztelés, az átadás - átvétel feltételeinek, módjának, a használatba vételnek, a jogosultságoknak, a későbbi üzemeltetésnek, valamint a biztonsági előírásoknak a megtervezése a létesítés ütemezésével és a felelősök megnevezésével.

Telepítés:

Hardver eszközök telepítését csak az informatikus - rendszergazda vagy az informatikus-rendszergazda az eladó szakembereivel együtt végezheti.
Szoftverek esetén a telepítés a programoktól függően történhet az informatikus-rendszergazda, vagy egyedi program esetén a program készítője és az informatikus-rendszergazda által közösen, a részletes programleírások és telepítési utasítások szerint.

A szoftverek üzembe helyezése:

A teljes rendszer működését szervezői tesztanyag összeállításával és futtatás utáni eredmény-helyesség vizsgálattal kell megállapítani. A programozói és szervező teszt alapján helyesnek bizonyult programrendszer működését a szervezési dokumentációban rögzített formájú "felhasználói" tesztelésnek lehet (bonyolultabb rendszernél kötelező) alávetni.
Ilyen lehet például a párhuzamos adatfeldolgozás, a felhasználó által összeállított minta adatsor feldolgozás, stb. A felhasználói teszt eredményét a felhasználó és a szervező közösen értékeli ki.

Külső - vásárolt vagy megrendelt egyedi - programok esetén a programok készítőjének feladata a tesztelés.

A rendszer hibátlan működését a felhasználó a kimeneti adatok logikai összefüggéseinek ellenőrzése útján folyamatosan köteles figyelni és hiba észlelése esetén az informatikus-rendszergazdát értesíteni.

Az üzemszerű feldolgozást csak a tesztanyagok futtatása által hibátlannak talált programrendszer esetén, a hozzáférési jogosultságok és azonosítók beállítását követően lehet megkezdeni.

Az átadás-átvétel a fejlesztés lezárásával és a teljes rendszerdokumentáció átvételét követően történhet meg.

A teljes rendszerdokumentációnak a következő főbb részeket kell tartalmaznia:

- szervezési dokumentáció: tartalmazza az alapadatok körét és ellenőrzésük módját, a feldolgozás logikai folyamatát, a közben létrejövő adatállományokat, a feldolgozás során keletkező eredmény adatokat, valamint ezek helyességének ellenőrzési módját.

- program dokumentáció: tartalmazza a rendszer programszintű működési leírását, az adatállományok és programok kapcsolatát.
- üzemeltetési dokumentáció: tartalmazza a rendszer üzemeltetéséhez szükséges hardver-szoftver feltételeket és az operátori teendők részletes leírását.
- felhasználói dokumentáció: részletesen tartalmazza a számítógéppel közvetlen kapcsolatba kerülő felhasználók rendszeres üzemeltetésre (használatra) vonatkozó teendőinek részletes leírását. Az üzemeltetési dokumentációnak mind a felhasználó, mind az üzemeltetés számára egyértelmű és naprakész információkat kell tartalmaznia a rendszer működtetéséhez.

A teljes rendszerdokumentáció nyilvántartását és tárolását jelen szabályzat iratok kezelésére vonatkozó rendelkezései szerint kell végezni és változásmenedzsment keretében kell karbantartani.

Kötelező nyilvántartások a telepített rendszerekről:

- a hardver eszközök telepítésekor az eszközök pontos konfigurációját, a tartozékokat és a licence jogosultsággal telepített szoftvereket nyilvántartásba kell venni gépenként, melynek tartalmaznia kell a leltári számot, a gyártót, a telepítés idejét, a használó helyét, nevét,
- a nyilvántartásban az eszköz életciklusában bekövetkező változást pontosan követni kell,
- a szoftverek telepítésekor nyilvántartásba kell venni a telepített operációs rendszert, vírusirtót és a licence jogosultsággal rendelkező egyéb programokat (gépenként is), melyen fel kell tüntetni a telepítés idejét, a program készítőjét, verziószámot, a licence tulajdonosát, a jogos használó azonosítóját, a lehetséges másolatok számát és az engedélyezett felhasználók számát,
- a nyilvántartások mellett meg kell őrizni a számlamásolatokat és a szerződésmásolatokat is.

A gépenkénti nyilvántartást az informatikus-rendszergazda vezeti és felel az aktuális állapothoz szükséges adatok helyességéért.

VII. Az üzemeltetés informatikai biztonsági feladatai és az üzemeltetett információs rendszerek biztonsági előírásai rendszerelemenként

1.Az informatikai eszközök üzemeltetése

Az informatikai eszközök üzemeltetéséért felelős személyeket az ügyvezető bízza meg az üzemeltetési feladatok ellátásával.

2.Központi gépek, hálózatok, egyedi pc-k

A központi gépek (szerverek) hálózati áramellátását a szünetmentes tápegységek alkalmazásával kell biztosítani, lehetővé téve a folyamatos üzemeltetést. Ezekre a berendezésekre csak a névleges teljesítményüknek megfelelő fogyasztót szabad csatlakoztatni. Tehát a szervere(ke)n és egy vagy két munkaállomáson kívül mást rákapcsolni nem szabad.

A hálózati kábelek, csatlakozóik megbontását csak az ezzel a feladattal megbízott szakember végezheti. A gépek felhasználók által történő megbontása, átalakítása szigorúan tilos.

A gépeket és tartozékaikat a helyükről elvinni az üzemeltetési feladatok ellátásáért felelős vezető engedélye nélkül nem szabad. Gondoskodni kell a printerek, monitorok csatlakozásainak csavaros rögzítéséről, a kicsúszás megakadályozásáról.

Rendellenes működés esetén a munkát azonnal fel kell függeszteni és értesíteni kell az informatikus-rendszergazdát. Az eszközök szakszerű javításáról, karbantartásáról az üzemeltetésért felelős személy gondoskodik, felé kell jelezni az erre vonatkozó igényeket. Az erőforrásokat úgy kell kialakítani, illetve hiba esetén átcsoportosítani, hogy a kiesés a legkevesebb időt vegye igénybe. A gyors hibaelhárítás és az alkatrész utánpótlás biztosítása érdekében szervíz hátteret kell biztosítani úgy, hogy a hiba kijavítását a bejelentéstől számított 12 órán belül meg kell kezdeni. Ha a meghibásodott eszköz helyben nem javítható, a szervíznek cserekészüléket kell biztosítania. Ez alól a speciális cipőtervező program (Footwear CAD®) és az azt kiszolgáló gépi háttér a kivétel, ahol a kiszállási idő 48 órán belüli.

Az informatikus-rendszergazda gondoskodik a lokális hálózatok naprakész dokumentálásáról. Új hálózati kapcsolatokat, bővítéseket csak az informatikus-rendszergazda vagy megrendelés alapján az erre megbízott külső szakember végezhet.

Az egyes hálózatokon el kell érni, hogy az adott munkahelyen bejelentkezett dolgozó csak a munkájához szükséges adattárakat érhesse el. A munkahelyi hozzáférési jogosultságokat - melyeket az informatikus-rendszergazda rögzít - ennek megfelelően szükséges kialakítani.

Az üzemelő rendszerek környezetének módosítását kizárólag a telepítést végző munkatársak kivitelezhetik. Az üzemeltetési környezetet meghatározó paramétereket, kezdeti beállításokat a felhasználók nem módosíthatják.

Fenti beállítások géptípusonkénti másolatát az informatikus-rendszergazda őrzi.

Gondoskodni kell a szervereken és munkahelyeken kialakított könyvtárstruktúrák rendszeres karbantartásáról, az elavult, nem használt állományok törléséről.

Idegen szoftvert az üzemelő rendszert tartalmazó hálózatra telepíteni tilos.

Áramszünet vagy rendellenes gépkikapcsolás okozta adathibákból eredő leállásokat az "üzemeltetési napló"-ban kell rögzíteni, és az informatikus-rendszergazdát haladéktalanul értesíteni kell.

3.Az informatikai rendszerek karbantartása

Az informatikai eszközök folyamatos rendelkezésre állásának és használhatóságának érdekében gondoskodni kell azok megfelelő karbantartásáról.
Az informatikai eszközök karbantartása, javítása során biztosítani kell a rajtuk tárolt információ jogosulatlan megismerés elleni védelmét.
A számítástechnikai gépek, berendezések javítását kizárólag az erre a célra kiképzett személy vagy külső szolgáltató végezheti.
A számítógépek meghibásodása esetén bárminemű javítás, hibaelhárítás a felhasználó által tilos, ideértve a számítógépek szétszedését, hardveregységek behelyezését, kivételét, a saját hatáskörben történő szervizeltetést.

A karbantartás mechanikus és elektromos karbantartásból áll.

Általános szabályok:

- a hardver elemeknél a megelőző karbantartást az adott elemre vonatkozó karbantartási előírásoknak megfelelően kell elvégezni,
- a berendezésekben karbantartást, javítást csak az arra kiképzett személyek végezhetnek,
- a berendezések burkolatát csak a műszaki személyek nyithatják ki,
- bekapcsolt állapotban a mechanikus szerelvényekbe nyúlni tilos,
- elektromos mérést, vizsgálatot - a gép bekapcsolt állapota mellett - csak megfelelő képzettséggel rendelkező személy végezhet.

Mechanikus karbantartás:

A nyomtatók rendszeres mechanikus karbantartást igényelnek. A forgó, csúszó alkatrészek folyamatos karbantartását kell biztosítani, mivel a papír adathordozókból, valamint a kívülről lerakódó por helytelen működést, majd meghibásodást okoz. Ennek megelőzésére a port rendszeresen el kell távolítani.
A monitorok képernyőjére lerakodó por a szövegek olvashatóságát rontja, a munkahely előtt ülő dolgozó szemét fárasztja. Ezért a monitorok és szűrők rendszeres portalanításáról a gép kezelőjének gondoskodnia kell.

A tisztításnak három fajtáját különböztetjük meg:

- portalanítás sűrített levegővel,
- alkoholos lemosás,
- mosószeres lemosás.

Ha egy berendezésnél mindhárom tisztítási műveletet el kell végezni, akkor azokat a fenti sorrendben kell végrehajtani.

A sűrített levegőt megfelelő nyomással, elsősorban kültéri helységekben szabad használni. Az olajos, zsíros szennyeződések eltávolítása alkohollal vagy megfelelő oldószerrel történik, nem foszló vászon használatával.

A mechanikus karbantartás idejére a gépet áramtalanítani kell oly módon, hogy véletlen bekapcsolás ne történhessen.

Elektromos karbantartás:

Az elektromos ellenőrzéseket és karbantartásokat csak megfelelő szakképzettséggel és munkavédelmi ismeretekkel rendelkező szakemberek végezhetik. A villamos berendezéseket, illetve hálózatot tűzvédelmi szempontból 3 évenként felül kell vizsgáltatni.

A hibás eszköz szállításakor az eszközt szállító tömbben kell vezetni.

4.Rendészeti védelem

A belépés ellenőrzése: a Kft. székhelyén a bv. intézet által működtetett biztonsági rendszer üzemel, mely regisztrálja a Kft. székhelyére történő be- és kilépés idejét. A Kft. telephelyén portaszolgálat működik, ahol részben informatikailag, részben manuálisan történik a be- és kilépés regisztrációja.

Az egri fióktelepen a bv. intézet által működtetett biztonsági rendszer üzemel, mely regisztrálja a Kft. fióktelepére történő be- és kilépés idejét.
Az almáskamarási fióktelepen videó és riasztó rendszer üzemel.

5.Tűzvédelem: a Kft. székhelyén az alsó és felső szinten lévő üzemrészekben a tűzjelző rendszer ki van építve. A Kft. telephelyén az alapanyag raktárakban és a polgári tűzödében van kiépített tűzjelző rendszer. A raktárházban intelligens tűzjelző rendszer működik. Az egri fióktelepen egy kiépített és rendszeresen karbantartott tűzjelző rendszer van a tűzöde II. üzemrészben. A tűzjelző rendszer karbantartását szerződés alapján vállalkozó végzi.

6.Vízvédelem: ide tartozik minden olyan intézkedés, amely az informatikai rendszer működését veszélyeztető alábbi események megelőzésére, elhárítására történik:

- árvíz,
- eső: a nyitva hagyott ablakon befolyva, vagy a külső falakon végigfolyva a falba épített dobozokban lévő vezetékek és csatlakozások beázása következtében elektromos zárlatot okozhat,
- csőtörés, csőrepedés,
- növények figyelmetlen locsolása,
- a padlózat felmosása.

7.Zárási rend: a számítógéppel ellátott helyiségek elhagyása esetén a munkaállomás illetéktelen hozzáférés elleni védelme érdekében a felhasználó köteles a munkaállomást zárolni, ha ez nem lehetséges, köteles a munkaállomásból kijelentkezni vagy azt kikapcsolni, amennyiben azt felügyelet nélkül hagyja. A munkaállomást a munkaidő végén vagy a munkavégzés befejezésekor ki kell kapcsolni.
A munkaidő végén a helyiséget elhagyó dolgozó, közös használatú helyiség esetén az azt utoljára elhagyó dolgozó köteles ellenőrizni, hogy minden munkaállomás, periféria kikapcsolt állapotban van-e. Kivételt képeznek a működő szerver gépek, melyek be- és kikapcsolásáról az informatikus-rendszergazda gondoskodik.

8.Szerverterem védelme

A szerverterem behatolásvédelmének biztosítása érdekében az alább szempontokat kell érvényesíteni:
- belépést regisztráló rendszer kialakítása,
- automatán záródó ajtó, amely kifelé kézzel nyitható,
- betörés-riasztó rendszer alkalmazása.

A szerverterem tűzvédelmének biztosítása érdekében az alábbi szempontok figyelembe vétele szükséges:
- tűz-vagy füstriasztó rendszer alkalmazása,
- kézi tűzoltó-berendezések elhelyezése a bejárat közvetlen közelében.

A szerverterem áramellátása érdekében:
- biztosítani kell az épület villámvédelmét,
- a szerverterem független betáplálását,
- a túlfeszültség elleni biztosítást,
- az eszközök szünetmentes tápellátását,
- az érintésvédelem kialakítását, rendszeres felülvizsgálatát.

A szerverterem üzemi hőmérséklet-szabályozása érdekében:
- klíma-berendezést kell üzemeltetni,
- a klíma-berendezés automatikus újraindítását kell biztosítani az esetleges áramszünet megszűnése esetén.

A szerverterem hozzáférési követelményei

A szervertermet folyamatosan zárva kell tartani, akkor is, amikor a helységben munkavégzés folyik. Ha ez nem követhető, a szerverterem bejáratának felügyeletét meg kell oldani.

Kerülni kell a szerverterembe az indokolatlan belépést. Oda csak az arra felhatalmazott személyek léphetnek be.
A szerverterembe az alábbi személyek belépése engedélyezett:
- munkaköri leírása alapján arra jogosult személyi állományi tag,
- adatvédelmi tisztviselő,
- informatikus-rendszergazda,
- karbantartást, telepítést végző személy felügyelet mellett.

A szerverterembe történő belépéseket dokumentálni kell, mely dokumentáció tartalmazza a belépő nevét, a belépés célját, a be- és kilépés idejét.

A szerverteremben csak a folyamatban lévő munkavégzéshez szükséges eszközöket, szerszámokat szabad tartani. A helyiségben tartózkodás ideje alatt az elrendelt munkavégzéstől eltérő tevékenységet (evés, ivás) folytatni nem szabad.

A szerverterem más irányú hasznosítása (raktározás) tilos.

Az elvégzett tevékenységet (telepítés, javítás, karbantartás) dokumentálni kell. A dokumentáció tartalmazza a feladatot végző nevét, a tevékenység leírását, időtartamát.

9.Adatvédelem: az adatvédelem kiterjed az adathordozók, az adatok, dokumentumok, iratok védelmére.

10.Adathordozók: az adatmegőrzés érdekében folyamatosan biztosítani kell, hogy az adathordozó az adott technikai feltételek mellett olvasható maradjon, vagy olvasható állapotba kerüljön.

Az adathordozók kezelése

A Kft.-nek gondoskodnia kell az adattároló eszközök, adathordozók szabályozott és biztonságos kezeléséről, melynek célja megelőzni, hogy jogosulatlanul nyilvánosságra hozzanak, módosíthassanak, töröljenek vagy megsemmisítsenek adathordozón tárolt információkat.

Az adathordozókon tárolt adatokat egyaránt védeni kell a jogosulatlan megismeréstől, módosítástól és megsemmisüléstől. Az adatok védelmét az adathordozók megfelelően biztonságos kezelésével, a szükséges technikai kontrollok és eljárások kialakításával kell biztosítani.

Az adathordozón tárolt programok és operációs rendszerek telepítő lemezeinek elhelyezését az informatikus-rendszergazda biztosítja.

Az adathordozók nyilvántartása

A Kft. által kezelt adatok tárolására és szállítására csak a Kft. tulajdonában vagy kizárólagos használatába álló, és nyilvántartásban szereplő adathordozó használható.

Az adathordozók fizikai védelme

Az adathordozók használata és tárolása során be kell tartani a gyártók által igényelt fizikai követelményeket. Sérült, hibás adathordozó használata adatok tárolására tilos.

Tilos védett adatot tartalmazó adathordozót őrizet nélkül hagyni olyan helyen, ahol ahhoz illetéktelenek hozzáférnek, annak tartalmát megismerhetik, módosíthatják, törölhetik.

Az adathordozók selejtezése

Az adathordozókat, ha további használatukra nincs szükség, selejtezni kell biztonságos adatmentesítést követően.

11.Adatok: az informatikai rendszer biztonsága szempontjából a legfontosabb a feldolgozásban szereplő adatok biztonsága.

Az adatok kezelése

A Kft.-nél be kell tartani a legfontosabb adatvédelmi előírásokat, biztosítani kell az input adatok helyességét, az adatokat feldolgozó szoftver eszközök védelmét, a feldolgozás biztonságának megteremtését.

Adatok rögzítése: az adatbevitel hibátlan műszaki állapotú berendezésen és hibátlan adathordozóra történhet.

Adatok tárolása, mentése

A Kft. alapvető feladatainak ellátásához nélkülözhetetlen állományokat (program és adatállományok) a szervereken vagy külső tároló(ko)n (Storage), az egyéb szintén fontos, de csak egy felhasználó által használt anyagokat (pl.: levelezés, Excel táblázatok) a munkaállomásokon kell tárolni. A felhasználóknak hetente legalább egyszer biztonsági mentést kell végezni a főbb dokumentumokról külső adattárolóra, adathordozóra (pl. Storage, PenDrive).
A munkaállomáson található felhasználói adatok mentéséért a gépen dolgozó személy felelős.
A megosztott meghajtók adattárolásra nem alkalmazhatók, vagyis a saját dokumentumok tárolásáról a felhasználónak a saját munkaállomásán kell gondoskodnia.
Az év végi adatállomány és rendszermentést, valamint biztonsági másolatait az informatikus-rendszergazda felügyeli.

Mentett adatok tárolása, hozzáférés

Az ügyviteli és bérelszámolási adatok biztonsági mentését napi szinten külső adattárolóra (felhő) kell elvégezni a megfelelő biztonsági szabályok betartásával. A mentésre kerülő állományokat a vírusfertőzés lehetősége miatt előzetesen tesztelni, ha szükséges vírus-mentesíteni kell.

A mentett állományok visszatöltése csak körültekintő munkával történhet, a mentés óta esetleg megváltozott programverziók miatt. Ezért a visszatöltés mindig csak az informatikus-rendszergazda jóváhagyásával végezhető. A szerveren másik alkönyvtárba másolt állományok nem tekinthetők mentésnek.

Adatállományok megsemmisítése

Az üzemeltetésre átadott programok által használt régi adatállományok megsemmisítése az üzemeltetés-vezető kezdeményezésére történhet az informatikus-rendszergazda és az érintett szakterület vezetőjének engedélye alapján. A megsemmisítést úgy kell elvégezni, hogy az adatokat ne lehessen visszaállítani.

Adatállományok védelme

A törzsállományokról az üzemeltetési dokumentációban meghatározott időközönként adathordozón másolatot (mentést) kell készíteni és az előírások szerinti időpontig meg kell őrizni. A másolatokról és készítésük pontos időpontjáról (generáció szám) nyilvántartást kell vezetni, amelyből ki kell tűnnie a felülírhatóság időpontjának is.
A szakterületükért felelős osztályvezetők ellenőrzik a területük törzsadatainak karbantartását, felelősek a saját területükről a Kft. rendszerébe kerülő adatok valódiságáért, azok biztonságáért és bizalmas kezeléséért.

12.Dokumentumok

A nyomtatott információk védelmét ugyanúgy kell biztosítani, mint az adathordozókét. Ezek védelmére az Iratkezelési Szabályzatban foglalt rendelkezéseket kell alkalmazni.

A papír alapú dokumentumokat és adathordozókat zárható szekrényben kell őrizni, tárolni, amikor nincsenek használatban, illetve munkaidőn kívül.

A megbízható működéssel kapcsolatos eseményekről (rendszer indítás/leállás, nagyobb üzemzavarok, alap- és felhasználói szoftverekkel kapcsolatos események) gépi naplózásokat kell végezni. A gépi nyilvántartás készítéséről, nyomtatásáról az informatikus-rendszergazda gondoskodik. A nyilvántartásnak tartalmaznia kell az esemény időpontját, az esemény leírását, az esetleges hibaüzenetet, gépi nyilvántartásnál a használó azonosítóját, kézi nyilvántartásnál a felhasználó nevét, aláírását.

13.Iratok

Az informatikai rendszer vagy elemeinek dokumentációját, a rendszer biztonságával kapcsolatos dokumentációkat változásmenedzsment keretében kell aktuális szinten tartani.

14.A hálózat védelme

A Kft. informatikai hálózatát megfelelő tűzfal védelemmel kell ellátni. Csak olyan kapcsolatok lehetnek engedélyezve belső irányban, amelyek a Kft. informatikai működését megkövetelik, és amelyek megfelelnek a naprakész informatikai biztonság elvárásainak (pl. protokollok, nyitott portok, IP-cím hozzáférés, stb.). Fájlok, adatok megosztása csak az informatikus-rendszergazda jóváhagyásával történhet. Külső felhasználók csak az ügyvezető jóváhagyásával férhetnek hozzá az informatikai hálózathoz, megfelelően titkosított csatornán keresztül (pl. AES, DES, WPA, WPA2, stb.) a megfelelő jogkörökkel. A külső felhasználó jelszavaihoz csak az informatikus-rendszergazda férhet hozzá. Illetéktelen behatolás és ennek szándéka esetén az informatikus-rendszergazda haladéktalanul értesíti az ügyvezetőt.

15.A programok védelme

A programvédelem során gondoskodni kell arról, hogy a tárolt programok, mint adatállományok ne károsodjanak. Biztosítani kell, hogy a rendszertervben rögzített követelményeknek megfelelően működjenek, a felhasználók számára mindenhol a legfrissebb verzió álljon rendelkezésre. (Tesztelési előírások betartása.)

Az üzemeltetésre átadott telepített programokat programkönyvtárban kell elhelyezni. Az üzemeltetéssel megbízott dolgozó felelős a mindenkori aktuális állapot rendelkezésre állásáért.

Minden programjavítást, illetve módosítást mind a szervezési, mind a program dokumentációban át kell vezetni. A módosított, illetve bevezetésre kerülő új programot az éles állomány egy másolatával is le kell tesztelni. Üzemszerűen csak azt követően lehet használatba venni, miután bebizonyosodott, hogy a teszt alatt adatvesztés vagy sérülés nem történt.

Az eredeti dokumentációk őrzéséért az adott rendszer üzemeltetésével megbízott dolgozók felelősek. Feladatuk annak biztosítása, hogy a dokumentációhoz az illetékesek bármikor hozzáférhessenek, az illetéktelen személyek pedig azokat ne használhassák.

A használatban lévő operációs rendszert (vagy rendszereket) 1 példányban lemezen kell tárolni. Minden tárolásra kerülő példányt ki kell próbálni (tehát be kell tölteni). Az operációs rendszer esetleges sérülése esetén a tartalék példányok felhasználásakor azokat azonnal pótolni kell.

16.A személyekhez kapcsolódó védelem

Az informatikai rendszer működtetéséhez szükséges személyzet két szempontból is védendő. Egyrészt a rendszer működtetéséhez szükségesek, így maguk is védelmet igényelnek, másrészt ők a rendszer használói, így tőlük is kiindulhatnak fenyegetések.

Az üzemeltető személyzet a feladatait munkaköri leírása alapján végzi, munkájuk során a jelen szabályzatban foglalt rendelkezéseket kötelesek betartani.

A jelen szabályzatban foglaltak megismerése céljából új munkavállaló belépésekor biztosítani kell az informatikai oktatását.

A hálózatos rendszerekbe való belépési rendet a hozzáférési jogosultságokkal összhangban kell kidolgozni.

Az informatikai rendszer biztonságát meghatározó munkakörökben a helyettesítés rendjét a szakterületek osztályvezetői határozzák meg.

Külső partnerek hozzáférési jogosultságait a velük kötött szerződéseknek megfelelően és jelen szabályzat biztonsági, adat- és titokvédelmi előírásainak megfelelően kell kiadni.

17.Mobil eszközök kezelése, használata

Hordozható adathordozónak tekintendő jelen szabályzat szempontjából valamennyi, az asztali számítógépbe, szerverbe, illetve irodatechnikai eszközbe rögzítetten beépített adathordozókon kívüli adathordozó.
A hordozható eszközök (laptop, notebook) szoftvereit, operációs rendszerét az informatikus-rendszergazda telepíti.
A felhasználónak a használatba vétel során ellenőrizni kell a mobil eszköz és tartozékainak meglétét és a védelmi eszközök meglétét (vírusvédelmi eszköz, személyi tűzfal).
A felhasználó köteles a hordozható eszközt a hivatali munkával kapcsolatos feladatokra rendeltetésszerűen használni.
A mobil eszközön minősített, valamint magánjellegű adatok tárolása, feldolgozása nem engedélyezett.
A Kft.-nél a hordozható eszközöket használaton kívül zárható szekrényben kell tárolni.
Az épületből való kivitelhez külön engedély nem szükséges, mivel az arra jogosultak mobilitását szolgálják.

VIII. A szervezet informatikai katasztrófa elhárítás módja, lehetősége

A Katasztrófaterv eljárás vagy tevékenység lépések sorozata, annak biztosítására, hogy a szervezet kritikus információ feldolgozó képességeit helyre lehessen állítani, elfogadhatóan rövid idő alatt, a szükséges aktuális adatokkal katasztrófa után.
Az informatikai katasztrófa olyan esemény, amely az adatfeldolgozó képesség elvesztését okozza hosszabb időre.

A Katasztrófaterv részei:

- a mentési (megelőzési) terv,
- a helyreállítási terv,
- a visszaállítási terv.

Mentési terv: azon lépések sorozata, amelyeket azért hajtanak végre a katasztrófát megelőzően (a normál üzem során), hogy lehetővé tegyék a szervezet számára a reagálást a katasztrófára.

A mentési terv biztosít elmentett eszközöket a helyreállításhoz:

- a szükséges hardver és szoftver konfiguráció rögzítése szükségüzem esetére,
- a biztonsági másolatoknak tűzbiztos helyen, a munkaterületen, illetve a számítógépközponton kívüli raktározása,
- az installált rendszerszoftverek és a fontosabb alkalmazói szoftverek referenciamásolatainak biztonságos raktározása,
- a fontosabb dokumentációk megkettőzése és raktározása,

- biztosítások megkötése a károk enyhítésére.

Helyreállítási terv: azon eljárások sorozata, amelyeket a helyreállítás fázisában hajtanak végre annak érdekében, hogy helyreállítsák az informatikai rendszert.

- Azonnali reakció: válasz a katasztrófahelyzetre, a veszteségek számbavétele, a megfelelő személyek értesítése és a katasztrófaállapot megállapítása.
- Környezeti helyreállítás: az adatfeldolgozó rendszer helyreállítása (operációs rendszer, program termékek és a távközlési hálózat).
- Funkcionális helyreállítás: az informatikai rendszer alkalmazásainak és adatainak helyreállítása, az adatok szinkronizálása a tranzakció naplóval.
- Helyreállítás: az elvesztett vagy késleltetett tranzakciók ismételt bevitele. Az üzemeltetők, a rendszeradminisztrátorok, az alkalmazók és a végfelhasználók együtt munkálkodnak azon, hogy helyreállítsák a normál feldolgozási rendet.

Visszaállítási terv: magában foglalja az informatikai alkalmazások prioritásainak kijelölését,

- hálózati, illetve egyedi pc-s operációs rendszer indítása,
- adatbázisok indítása,
- adatbázis integritásának ellenőrzése, a szükséges korrekciók végrehajtása,
- az alkalmazások indítása.

A külső környezeti hatások közül a legsúlyosabb károkat az elemi csapások okozzák, ezeket általában nem lehet előre látni és megelőzésükre nem lehet intézkedéseket tenni.

Elemi csapás esetén a kár mérséklésére és a gyors, hatékony helyreállításra kell törekedni. Tűz, robbanás esetén a "Tűzriadó terv" szerint kell eljárni. A tűzriadó tervet a Kft. munka-és tűzvédelmi vezetője évente ismétlődő oktatás keretében ismerteti a személyi állománnyal.
Tűzesetek megelőzésére a tűzvédelmi utasítás betartása kötelező. A legfontosabb adatokat, adatbázisokat külső adattárolón (storage, felhő) kell tárolni a hálózat védelmére vonatkozó biztonsági előírásoknak megfelelően.

IX. Vírusvédelem, vírusmenedzsment

A számítógép vírusok olyan programok, melyek működésük közben valamilyen romboló hatást váltanak ki a számítógépben vagy az informatikai rendszer más elemében. A vírusok ellen a Kft. megelőzéssel védekezik. A megelőző intézkedések közé tartozik a Katasztrófa terv megelőzési fejezetében előírt biztonsági másolatok készítése, melyek a rendszer összeomlása esetén a helyreállíthatóságot biztosítják.

Vírusvédelem:

- a Kft.-nél társaságnál minden számítógépen, hálózaton vírusvédelmi szoftvereket kell alkalmazni,
- gondoskodni kell a védelmi szoftverek folyamatos frissítéséről,
- az informatikai rendszerben csak ellenőrzött, illetve vírusmentesített adathordozókat, programokat lehet használni, melyeket használat előtt víruskeresővel ellenőrizni kell,
- a kommunikációs csatornákon érkezett anyagokat minden esetben ellenőrzést követően lehet megnézni és felhasználni,
- az adathordozók mellett rendszeresen, legalább havonta teljes körű vírusellenőrzést kell tartani a rendszerben,

- a vírusellenőrzés a telepített kereső programokkal részben automatikus, részben oktatást követően a felhasználó feladata.

Vírusmenedzsment:

- vírusfertőzés gyanúja, vagy vírusfertőzést jelző hibaüzenet esetén azonnal értesíteni kell az informatikus-rendszergazdát,
- vírusmentesítést csak az informatikus-rendszergazda vagy az általa felhatalmazott, informatikai végzettségű munkatárs végezhet a legújabb verziójú védelmi szoftverekkel,
- hálózatos felhasználás esetén gondoskodni kell a fertőzött terület izolálásáról, lehetőség szerint meg kell akadályozni a vírus elterjedését és károkozását,
- az izolált területeken is el kell végezni az ellenőrzést és szükség esetén a mentesítést,
- a fertőzött munkaállomáson dolgozni csak az informatikus-rendszergazda által elvégzett vírusirtás után szabad,
- a rendszer teljes összeomlása, vagy olyan sérülések esetén, ahol a vírusmentesítés nem elég, a Katasztrófa tervben foglaltak szerint kell eljárni,
- a vírusmentesítést követően ellenőrizni kell a rendszer működőképességét, a keletkezett károkat és gondoskodni kell a program, illetve az adatbázis helyreállításáról,
- a helyreállítást követően vizsgálni kell a vírusfertőzés keletkezését, okát, a felelősséget fel kell tárni, és a megfelelő intézkedéseket (munkáltatói, szabályzatmódosítási, ellenőrzési, stb.) meg kell tenni.

X. Internet-hozzáférés

Internet-hozzáférést csak az ügyviteli folyamatokkal, illetve azok támogatásával kapcsolatos ügyintézésre szabad használni.
Internetezés közben el kell utasítani azokat a felbukkanó párbeszéd-ablakokat, amelyek segédprogramok telepítésére, vagy egyes funkciók kikapcsolására ösztönöznek.

A Kft.-nél csak azokon a hálózati hozzáférési pontokon lehetséges internet hozzáférést létesíteni, ahol nincs elítélti jelenlét.

Az internet hozzáférést az alábbi szinteken lehet kialakítani:

1. szint: nincs internet hozzáférés
2. szint: korlátozott internet hozzáférés
3. szint: teljes internet hozzáférés.

Az internet hozzáférések engedélyezése ügyvezetői hatáskör.

Internet hozzáférést csak olyan munkaállomásokon lehet kiépíteni, amelyek megfelelő operációs rendszerrel, biztonsági frissítésekkel és vírusvédelemmel vannak ellátva.
Internet hozzáférésre csak az az alábbi, legújabb frissítéssel rendelkező böngészőket lehet alkalmazni:

- Google Chrome
- Mozzila Firefox
- Internet Explorer
- Opera.

Internet használat közben kerülni kell a nem ügyintézésre szolgáló letöltéseket (pl. torrent, warez, stb), weboldalakat, amelyek potenciális vírus fenyegetést jelentenek a Kft. informatikai hálózatára. A Kft. az informatikus-rendszergazda útján jogosult az internetet használó számítógépek és felhasználók internet forgalmának ellenőrzésére.

XI. Az elektronikus üzenetküldés (e-mail) szabályai

A Kft.-nél hivatalos elektronikus levelezést a @ipolycipo.hu végződésű e-mail címekkel rendelkező személyek folytathatnak. Részükre bármilyen külső e-mail címre, illetve e-mail címről mind a küldés, mind pedig a fogadás lehetséges és engedélyezett.

Az e-mail cím igénylése az ügyvezető jóváhagyásával történik. Ez alapján az informatikus-rendszergazda feladata a tényleges beállítások elvégzése.

Az e-mail cím megszüntetésére (munkakör megszűnése, dolgozó távozása, stb. esetén) az adott szakterület vezetője indokolt javaslatot tesz az ügyvezető felé. Jóváhagyás után az informatikus-rendszergazda feladata a törlés végrehajtása a megfelelő archiválás után. Az elektronikus levelezésre jogosultak névsorát az informatikus-rendszergazda tartja nyilván és karbantartja.

Az Ipoly Cipőgyár Kft. elektronikus levelező rendszerét a felhasználók csak a hivatalos feladataik elvégzéséhez használhatják.

Hivatalos elektronikus levél csak az Kft. (@ipolycipo.hu) domain névvel végződő e-mail címről küldhető. Az iktatott (aláírt, hivatalos pecséttel ellátott) iratot PDF fájl formátumban be kell szkennelni, amit a fogadó fél e-mail címére el kell küldeni.

A felhasználónak naponta rendszeres időközönként, de legkésőbb a munkanap végéig a postaládáját ellenőriznie kell.

Minden felhasználó saját maga felel valamennyi, általa az elektronikus levelező rendszer használatával közölt információért, tartalomért.

A Kft. vezetői asszisztensének a munkaidő minden órájában ellenőriznie kell, hogy az ipoly@ipolycipo.hu és az ugyvig@ipolycipo.hu címekre érkezett-e a Kft. számára e-mail.

A beérkezett hivatalos levelet a kinyomtatás után iktatni kell. Tekintettel arra, hogy az e-mail fiókok tárhely kapacitása véges, az érkezett leveleket - különös tekintettel a nagyméretű mellékletet tartalmazókra - nyomtatás, iktatás, illetve a mellékletek mentése után törölni kell. Ennek elmulasztása esetén a tárhely megtelik, és a Kft. nem tud elektronikus leveleket fogadni, sem továbbítani erről a címről, ezért ennek karbantartásáról a tárhely felhasználójának gondoskodnia kell.

A szakterületeken az osztályvezetőknek kell gondoskodniuk arról, hogy helyettesítések alkalmával az e-mail forgalom zavartalanul működjön az illetékes felhasználó távolléte alatt is.

A Kft.-n kívüli levelezésre biztosított e-mail címet szigorúan tilos egy harmadik személynek kiadni a cím tulajdonosának hozzájárulása nélkül.

A felhasználónak az elektronikus levelezés során az ismeretlen forrásból származó elektronikus leveleket és csatolt állományokat haladéktalanul le kell törölnie, vagy az informatikus-rendszergazdának jelenteni kell az ismeretlen eredetű fájl tényét és követnie kell az informatikus-rendszergazda utasításait a fájl kezelésével kapcsolatban.

A Kft. rendszerének működése során kerülni kell az olyan eljárásokat, amelyek eredményeképpen mások számára félreértésre okot adó, ezáltal veszélyes, azonosíthatatlan eredetű és rendeltetésű vagy vírus által fertőzött fájl jönne létre és kerülne továbbításra.

XII. Információbiztonsági incidensek kezelése

Biztonsági eseménynek tekintendő minden olyan tevékenység, illetve esemény, amely a Kft. által kezelt, tárolt vagy továbbított információk biztonságát, illetve a Kft. informatikai rendszereinek funkcionális integritását vagy rendelkezésre állását veszélyeztetve kárt okoz, vagy annak veszélyét idézi elő.

Az információbiztonsági eseményeket a felfedezést követően a közvetlen vezető felé jelenteni kell.

XIII. Záró rendelkezések

Jelen szabályzat a kiadása napján, azaz 2021. szeptember hó 30. napján lép hatályba és a visszavonásáig érvényes.

Jelen szabályzat kiadásával egyidejűleg hatályát veszti 2019. július hó 15. napján kiadott Informatikai Biztonsági Szabályzat.

A jelen szabályzatot rendszeres időközönként, de legalább évente egy alkalommal felül kell vizsgálni. Ez a tevékenység az informatikus-rendszergazda és a jogtanácsos feladata.

Balassagyarmat, 2021. szeptember 27.

Készítette:

Nagyné dr. Kívés Krisztina
jogtanácsos