Komlói Közös Önkormányzati Hivatal
Informatikai Biztonsági Politika

I. Általános rendelkezések

1. Az intézkedés célja

1.1. Az Informatikai Biztonsági Politika (a továbbiakban: IBP) a Hivatal legfelső vezetésének akaratnyilvánítása a szervezet informatikai rendszerei által kezelt információvagyon bizalmasságának, hitelességének, sértetlenségének, rendelkezésre állásának és funkcionalitásának megőrzésére és fenntartására irányuló intézkedések bevezetésére.
1.2. Az IBP célja irányelveket adni a biztonságért felelős vezetők részére a biztonsági politikánál alacsonyabb szintű szabályozások kialakításához, a jelen és jövőbeli informatikai biztonsági döntéseik meghozatalához, illetve a biztonsági rendszer működtetői és a felhasználók számára a napi rendeltetésszerű tevékenységük gyakorlásához.

2. Az intézkedés hatálya

Az IBP hatálya kiterjed:

- A Hivatal valamennyi vezetőjére, ügyintézőjére, a rendszerek felhasználóira, fejlesztőire, üzemeltetőire.
- A Hivatallal külső, megbízásos (szerződéses) eseti munkakapcsolatban lévő személyekre is, amelyeknek érvényesülését a fenti szerződések tartalmának megfelelő kialakításával kell biztosítani.
- A Hivatal által használt valamennyi informatikai rendszerre, amely felhasználja, feldolgozza, illetve felügyeli, ellenőrzi a keletkező, illetve felhasznált adatokat, információkat.

3. Értelmező rendelkezések

E szabályzat alkalmazásában

- Adat: Értelmezhető, de nem értelmezett elemi ismeret, amely az információt ábrázolja.
- Adatbiztonság: Az adatokba történő jogosulatlan betekintés, az adatok jogosulatlan megszerzése, módosítása és tönkretétele ellen műszaki és szervezési intézkedések és eljárások együttes rendszere.
- Adatbiztonság megsértése: Az a cselekmény vagy mulasztás, amely ellentétben áll az adat védelmére vonatkozó biztonsági szabályokkal, és amelynek következményei az adatot veszélyeztetik.
- Adatfeldolgozás: Az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.
- Adatkezelés: Az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt is) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is.
- Adatvédelem: Az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségére vonatkozik.

- Biztonsági követelmények: A biztonsági követelmények azok a biztonsági elvárások, amelyeket az elfogadhatatlan kockázattal járó fenyegetések csökkentésére (biztonsági kockázatelemzés eredményeként) határoznak meg.
- Biztonsági esemény: Az informatikai rendszer biztonságában beállt olyan kedvezőtlen változás vagy bekövetkező jelentős hatású zavaró esemény, amely nagymértékben rontja az informatikai szolgáltatás minőségét és veszélyezteti a rendszer biztonságát.
- Felhasználó: Az a személy vagy szervezet, aki (amely) egy vagy több informatikai rendszert használ feladatai megoldásához.
- Folyamatos ügyvitel biztosítása: Az informatikai rendszerek folyamatos rendelkezésre állása.
- Hozzáférés: A hozzáférés az informatikai rendszer védelmi mechanizmusa által biztosított (jogosult) erőforrás-használat.
- Informatikai biztonság: A informatikai biztonság az információs rendszer tulajdonsága, amely a rendszer biztonsági követelményeinek és céljainak teljesülését mutatja. Olyan előírások, szabványok betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és bizalmasságát eredményezik, és amelyeket az informatikai rendszerekben vagy komponenseikben, valamint az informatikai rendszerek vagy komponenseik alkalmazása során biztonsági megelőző intézkedésekkel lehet elérni. Informatikai biztonság alatt valamely informatikai rendszer azon állapota értendő, amelyben a kockázatok, amelyek ezen informatikai rendszer bevezetésekor a fenyegető tényezők alapján adottak, az intézkedésekkel elfogadható mértékűre csökkentettünk.)
- Informatikai biztonsági utasítások, eljárások: A kritikus alrendszer területek egyes üzemeltetési eljárásainak részletes leírása.
- Információs vagyon: Adatok, információk, szellemi, erkölcsi javak összessége.
- Katasztrófakezelés, tervezés: Lehetővé teszi, hogy egy esetleges katasztrófa bekövetkezte után az informatikai szolgáltatások ellenőrzött módon, egy előre megállapított szinten helyreállíthatók legyenek, oly módon, hogy előre meghatározzák a helyreállítás során érvényes személyi felelősségeket, illetve a követendő tevékenységeket.
- Kontrollok-óvintézkedések: Mindazok a fizikai, adminisztratív, technikai technológiai módok, eljárások, amelyeket védelmi célból terveztek és a kockázatot csökkentik.
- Kriptográfia: A kriptográfia azoknak a matematikai eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak kutatását, alkalmazását jelenti, amelyek elsődleges célja az információnak illetéktelenek előli elrejtése.
-

II. Az Informatikai Biztonsági Politikával kapcsolatos alapelvek

1. Információvédelem területei

- Azonosítás, hitelesítés;
- Jogosultság kiosztás, ellenőrzés;
- Hitelesség garantálása;
- Sértetlenség garantálása;
- Bizonyítékok rendszerének és folyamatának kialakítása.

2. Az Informatikai Biztonsági Politika a Hivatal tevékenységének szolgálatában

2.1. A Hivatal kezelésében, valamint felügyeletében működő és ezen intézményeket kiszolgáló kommunikációs és informatikai rendszereket az adatok titkosságára, bizalmas jellégére és biztonságára vonatkozó törvényeknek megfelelően kell üzemeltetni.
2.2. Az informatikai rendszerekben adatot, információt és egyéb szellemi tulajdont az intézmény számára jelentkező értékével arányosan kell védeni az illetéktelen betekintéstől, a módosítástól, a sérüléstől, megsemmisüléstől és a nyilvánosságra kerüléstől. A védelemnek biztosítani kell az informatikai rendszer megbízható működését fenyegető káresemények elhárítását, illetve hatásuk minimalizálását a megadott biztonsági követelmények szintjén. A biztonsági szabályok megsértése esetén az IBP hatálya alá eső személyekkel szemben felelősségre vonási eljárást kell kezdeményezni.
2.3. A védelem megvalósítása érdekében a tervezés során a költségvetésben biztosítani kell azokat az anyagi feltételeket, amelyek lehetővé teszik a megfelelő színvonalú technika, valamint a speciális felkészültséget igénylő személyi feltételek megteremtését és folyamatos fenntartását.

3. Az Informatikai Biztonsági Politika helye az informatikai biztonsággal foglalkozó dokumentumok rendszerében

3.1. A Hivatal vezetői az informatikai rendszerek, illetve rendszerelemek teljes életciklusára, az informatikai biztonság elviselhető kockázati szinten tartása érdekében kialakítják az informatikai biztonsági dokumentációs rendszert.
3.2. A Hivatal informatikai biztonságával kapcsolatos szabályokat és elvárásokat az informatikai biztonsági dokumentációs rendszer tartalmazza.

- törvényi előírások és egyéb jogszabályok,
- biztonsági iránylevek, eljárások,
- az Informatikai Biztonsági Politika,
- az Informatikai Biztonsági Szabályzat,
- az alsóbb szintű szabályzatok,
- az Ügymenet folytonossági és Katasztrófa elhárítási Terv,
- biztonsági nyilvántartások, naplók.

3.4. Az Informatikai Biztonsági Politika helye az informatikai biztonsággal foglalkozó dokumentumok rendszerében:

4. A biztonságpolitikai alapelvek és védelmi célkitűzések

A Hivatal az informatikai biztonság területén az alábbi alapelveket és védelmi célkitűzéseket kívánják következetesen érvényesíteni:

- Bizalmasság biztosítása a Hivatal által kezelt, felhasznált adatokhoz való hozzáférés tekintetében, elsősorban a szervereken és a felhasználói munkaállomásokon történő adathozzáférések és az adatkezeléseknél felhasznált adathordozók kezelése, valamint a kommunikáció során.
- Sértetlenség biztosítása a Hivatal teljes adatvagyonára vonatkozóan az adatkezelés, adattárolás és a kommunikáció során.
- A Hivatalnál történő adatkezelések és feldolgozások során követelmény, hogy a pontos és helyes információkat dolgozzák fel, az adatok sértetlenségét megőrizzék a feldolgozás előtt, közben és után.
- Rendelkezésre állás fenntartása elsősorban a Hivatal adatvagyonára vonatkozóan, amelyet biztosítani kell mind a külső, mind pedig a belső adatkérések során.
- Működőképesség fenntartása a Hivatal informatikai rendszereire és rendszerelemeire vonatkozóan, amely az adott informatikai eszköz vagy rendszer elvárt és igényelt üzemelési állapotban való fennmaradását jelenti. Ennek elérése céljából biztosítani kell a megfelelően képzett személyzetet és technikai feltételeket.

III. Tartalmi követelmények

1. A Hivatal és szervei viszonya az informatikai biztonság tekintetében

1.1. A Hivatal és szervei önállóan alakítják ki informatikai biztonsági szabályrendszerüket, azonban ezen szabályok nem mondhatnak ellent a vonatkozó törvényi előírásoknak.

1..2. A Hivatal megfogalmazza az Informatikai Biztonsági Szabályzat, valamint az Ügymenet folytonossági, Katasztrófa Elhárítási Terv készítésének alapelveit.
1.3. A Hivatal és szervei informatikai kapcsolatainak kialakítására illetve biztosítására csak olyan technikai és adminisztratív intézkedések engedélyezhetők, ill. valósíthatók meg, amelyekkel a jogszabályi és egyéb előírásoknak megfelelően biztosítják az informatikai rendszereik védelmét.

2. A Hivatal informatikai biztonságának területeire vonatkozó alapelvek, követelmények

2.1. Logikai védelem

a) Számítógép-hálózati biztonság

Hivatal az informatikai rendszereit logikai, technikai és adminisztratív eszközökkel védi a külső kapcsolatok, egyéb szervezetek és az internet felől érkező támadások ellen.

b) Hozzáférés szabályozás

A felhasználók csak ellenőrzött körülmények között, a szükséges felhasználói jogosultságokkal férhetnek hozzá az informatikai rendszerekhez és szolgáltatásokhoz.
A külső felek nem férhetnek hozzá a számítógépes rendszerekhez, számítógépekhez.
A hozzáférések szabályainak kialakításánál a felhasználói profilokat rendszerenként kell meghatározni a szükségesnél nem több hozzáférési jogosultság elve alapján és ehhez kell a személyeket hozzárendelni.
A felhasználói hozzáférések kezelésére szóló eljárást a felhasználónak a rendszerbeli teljes életciklusán keresztül kell érvényesíteni (az új felhasználók felvételétől, a felhasználó kilépéskor történő jogosultságainak megszüntetéséig).

c) *Adattovábbítás elektronikus úton*

A bizalmas tranzakciók adatainak cseréje a jogszabályokban meghatározottak szerint csak megbízható csatornákon történhet.
A bizalmas információk közé tartoznak a biztonsági eljárásokhoz kapcsolódó információk, a bizalmas tranzakciók adatai, a jelszavak és a kriptográfiai kulcsok. Ezek továbbítására a hagyományos, eljárási rend, illetve elektronikus úton való továbbításukhoz megbízható csatornák kialakítására van szükség, amely a különböző felhasználók és a rendszerek, valamint a különböző rendszerek közötti rejtjelezéssel valósítható meg.

d) *Adatok sértetlenségének, konzisztenciájának biztosítása*

Az adatok bevitele során biztosítani kell a forrás dokumentumok, az adatbeviteli munkakörök és munkaállomások biztonságát és azonosíthatóságát, valamint a bevitt adat ellenőrzését és hibás bemeneti adatok kezelését.
Az informatikai rendszer(ek) üzemeltetése során biztosítani kell a kezelt adatok, információk rendszeres biztonsági mentését. Rendszeres visszaállítási teszteket kell végezni és mindezeket dokumentálni kell.
Megfelelő eljárásokat kell kidolgozni az adathordozók kezelésére, tárolására, nyilvántartására, annak rendszeres, naprakész aktualizálására, valamint ezek megsemmisüléstől és illetéktelen hozzáféréstől történő védelmére. Az eljárások kidolgozásának célja, az ügymenet folytonosságának fenntartása és a szervezet vagyonának megóvása.

Az adathordozók elhelyezése során biztosítani kell, hogy az elhelyezés feltételei megfeleljenek az adatok, információk biztonsági osztályba sorolási modelljében meghatározott követelményeknek.

e) *Szoftverkezelés biztonsága*

A hivatal informatikai rendszereiben kizárólag jogtiszta, az üzemeltetéshez, adatfeldolgozáshoz szükséges, engedélyezett alapprogramok, irodai szoftvercsomagok és feldolgozó programok futtathatók.

Rosszindulatú szoftverek elleni védekezés

A szoftverek és informatikai rendszerek sebezhetőek a rendszerbe bejutó rosszindulatú szoftverek (vírusok, trójai falovak) által.

A rossz szándékú szoftverek kártételeinek megelőzésre megfelelő megelőző, észlelési és korrekciós mechanizmusokat kell alkalmazni.

f) Tűzfalas védelem

Az internetet és az elektronikus levelezést a felhasználók csak a szervezettel kapcsolatos feladataik végzéséhez használhatják.

Az internet használat, levelezés létesítése és üzemeltetése vonatkozásában megfelelő tűzfalas védelmet kell kialakítani a külső támadások, illetve a belső erőforrásokhoz történő jogtalan külső hozzáférések megakadályozása érdekében.

A tűzfalnak el kell rejtenie a belső hálózat struktúráját, valamint megfelelő ellenőrzési és behatolás detektáló, nyomkövetési, naplózási szolgáltatásokat kell biztosítania.

Minden alkalmazással, illetve infrastruktúrával kapcsolatos tevékenységhez kötődő információáramlást minden irányban ellenőrzés alá kell vonni, minden bentről kifelé és kintről befelé haladó információnak át kell haladnia a tűzfalon.

A rendszerbe csak az engedélyezett forgalom léphet be.

2.2. Fizikai védelem

a) Illetéktelen hozzáférés megakadályozása

Az infrastrukturális elemek (pl.: kábelhálózat, szerverszobák) kialakítása során figyelembe kell venni az Informatikai Biztonsági Szabályzatban meghatározott szempontokat is.

b) Az informatikai rendszer környezeti feltételeinek biztosítása

Az informatikai rendszerek külső környezeti hatásoktól való védelmét úgy kell kialakítani, hogy a szervezet vagyona és az ügymenet folytonossága ne legyen veszélyeztetve.

A védelemnek biztonsági osztályba sorolástól függően ki kell terjednie a biztonságos elektromos ellátás, a klimatizálás, a tűz- és villámvédelem biztosítására is.

c) Adminisztratív védelem aktualizálása, karbantartása

Az informatikai rendszerben bekövetkezett változásokat és alkalmazott problémakezelési eljárásokat (tervezés, létrehozás, üzemeltetés-karbantartás, megszüntetés) dokumentált formában, a szabályozó előírásoknak megfelelően kell végezni.

Az informatikai biztonsági dokumentációs rendszer aktualitásának fenntartása érdekében a rendszerben található dokumentumok rendszeres karbantartást igényelnek.

A dokumentációs rendszer dokumentumait felül kell vizsgálni a következő esetekben:

- a szervezet igényei, céljai megváltoznak,
- új területek, szolgáltatások jelennek meg,
- informatikai szolgáltatások szűnnek meg,
- új informatikai technológiák kerülnek bevezetése,

- informatikai technológiák alkalmazása szűnik meg,
- a kockázatelemzés következtében új, lényeges változtatások válnak szükségszerűvé.

2.3. Személyek

a) Informatikai biztonsággal kapcsolatos feladatkörök meghatározása

A felső vezetésnek a szervezeten belül, hogy a dolgozók csak a munkakörükhöz, illetve beosztásukhoz tartozó feladatokat lássák el. Mindenkit tájékoztatni kell arról, hogy milyen mértékű belső ellenőrzési és biztonsági felelősséggel tartozik.

b) Informatikai biztonsági szervezet

Az informatikai biztonság tervezése, alapkövetelményeinek lefektetése, bevezetése és ellenőrzése a szervezet vezetőinek a feladata.

A vezetők igénybe vehetnek biztonsági szakértőket annak érdekében, hogy megfelelő információkkal rendelkezzenek a szervezetük informatikai biztonsági helyzetéről. A szakértők feladata továbbá, hogy gondoskodjanak a különböző szabványok és ajánlások alkalmazásáról. A vezetők igénybe vehetik a szakértőket a biztonsági események kivizsgálása és értékelése során is.

c) Személyekre vonatkozó biztonsági megállapítások

Az informatikai biztonsági követelmények és annak betartásának követelményeit a dolgozóval ismertetni kell.

Mindezek kapcsán az Informatikai Biztonsági Szabályzatban részletesen szabályozni kell a következő területeket:

1. informatikai funkciók meghatározása;
2. munkavállalókkal szembeni követelmények;
3. titoktartási nyilatkozatok.

2.4. Egyéb területek

a) Oktatás, képzés és a biztonságtudatosság fokozása

A Hivatal az informatikai biztonsági dokumentációs rendszerben foglaltak érvényre juttatásának érdekében fontosnak tekintik az informatikai biztonsági képzést, oktatást, az informatikai biztonság tudatosítását.

A biztonsági követelmények maradéktalan teljesülése érdekében oktatást, képzést kell biztosítani minden informatikai szereplő számára az informatikai biztonságtudatosságának fejlesztésével kapcsolatban, valamint a rendszerek üzemeltetéséhez és rendeltetésszerű használatához szükséges biztonsági követelmények elsajátítása érdekében.

b) A folyamatos működés biztosítása

A folyamatos működés tervezésének és biztosításának célja, hogy az ügymenet tevékenységében bekövetkezett zavarokat ellensúlyozni lehessen és a kritikus folyamatok védettek legyenek a nagyobb hibák és katasztrófák következményeitől.

Le kell vonni a bekövetkezett katasztrófák következményeit, vizsgálni kell a szolgáltatások kiesését és a biztonság sérülését.

Az Ügymenet folytonossági és Katasztrófa Elhárítási Terv fejlesztésével és bevezetésével kell biztosítani, hogy az ügymenet szempontjából kritikus folyamatok visszaállíthatóak legyenek egy meghatározott időintervallumon belül. Az ügymenet folyamatos működésének biztosításába bele kell érteni a katasztrófa események következményeinek azonosítását és a rájuk történő reagálást, valamint a legszükségesebb alkalmazások meghatározott időn belüli visszaállítását.

c) *Informatikai biztonsági események észlelése és kezelése*
A Hivatal érdeke, hogy a szervezet informatikai biztonságáért felelős vezetői mielőbb értesüljön a bekövetkezett biztonsági eseményekről. Minden alkalmazottnak (külső vagy belső) ismernie kell azt az eljárást, amelyben jelenthetik az általuk felismert biztonsági eseményeket.
Ennek érdekében:
Informatikai biztonsági esemény bekövetkezésekor, arról a közvetlen munkahelyi vezetőt és az informatikusokat kell értesíteni és foganatosítani kell a megfelelő válaszintézkedéseket.
Az informatikai biztonság terén a védekezés szempontjából fontos, hogy a korábban történt informatikai biztonsági eseményeket időben visszamenőleg tételesen, minden technikai körülményükkel együtt fel lehessen dolgozni.

d) *Rendszerfejlesztések biztonsági követelményei*
A rendszerek biztonsági követelményeinek meghatározása során, rendszer alatt értjük az infrastrukturális elemeket, objektumokat, alkalmazásokat stb. Biztonsági szempontból kiemelkedő, hogy a biztonság, mint kritérium jelen legyen az alkalmazások és szolgáltatások tervezésétől kezdődően az ügymenet folyamataiba történő implementálásig.

e) *Mobil eszközök használata*
Felkészülve a jövő kihívásaira és reagálva az információtechnológiai eszközök fejlődésére és megjelenésére a Hivatal és szervei informatikai infrastruktúrájában szabályozni kell a mobil eszközök használatát .
A mobil eszközök használata során az eszközök jellegüknél fogva speciális kockázatokat hordoznak magukban. A mobil eszközökön történő munkavégzés során nem biztosított a megfelelő védelemmel ellátott környezet, ezért ilyen esetekben speciális védelmet kell biztosítani.

IV. Záró rendelkezések

Az IBP ismerete minden dolgozóra kötelező érvényű.

Jelen dokumentum 2014. január 2-án lép hatályba.

Komló, 2014. január 2.

KOMLÓI KÖZÖS ÖNKORMÁNYZATI HIVATAL JEGYZŐJE

dr. Vaskó Ernő
címzetes főjegyző