KOMLÓI KÖZÖS ÖNKORMÁNYZATI HIVATAL

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Tartalomjegyzék

VIII. Biztonsági eseménykezelési eljárásrend

IX. Biztonsági osztály

1. sz. melléklet Felhasználói nyilatkozat
2. sz. melléklet Nyilatkozat oktatásról
3. sz. melléklet Informatikai karbantartási napló
4. sz. melléklet Igénylőlap informatikai szolgáltatáshoz
5. sz. melléklet Szerverszoba belépési napló
6. sz. melléklet Biztonsági osztályba sorolás

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 15.§ (1) bekezdés d) pontjában, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 24.§ (3) bekezdésében, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. 30.§ (1) bekezdésében kapott felhatalmazás alapján a Komlói Közös Önkormányzati Hivatal (a továbbiakban: Hivatal) informatikai biztonsági szabályzatát az alábbiakban határozom meg:

I. ÁLTALÁNOS RENDELKEZÉSEK

1.1. A szabályzat célja

A szabályzat célja, hogy biztosítsa a Hivatal és intézményei, alkalmazottai által kezelt adatok vonatkozásában az adatbiztonság követelményeinek érvényesülését. Megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

A számítástechnika alkalmazása során biztosítsa a Hivatalnál az alábbiakat:

- titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- az üzembiztonságot szolgáló karbantartást és fenntartást, az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre való csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartását,
- munkaállomásokon (USER) lekérdezhető adatok körének meghatározását,
- adatállományok biztonságos mentését, a számítógépes rendszerek zavartalan üzemeltetését, a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását, az adatvédelem és adatbiztonság feltételeit,
- a védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.

1.2. A Szabályzat hatálya

Az szabályzat személyi hatálya kiterjed:

- A hivatal minden olyan munkatársára, illetve a hivatallal polgári jogi jogviszonyban álló személyre, aki a munkavégzés, feladatellátás az információ technológiai (továbbiakban: IT) eszközökkel, valamint az általuk kezelt adatokkal kapcsolatba kerül, ezekkel az eszközökkel, adatokkal munkát végez.

- A hivatal informatikai rendszerével, szolgáltatásaival polgári jogi jogviszony alapján vagy más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre a velük kötött szerződésben rögzített mértékben, illetve titoktartási nyilatkozat alapján.

E szabályzat tárgyi hatálya kiterjed:

- a Hivatal tulajdonában lévő valamennyi számítástechnikai, informatikai berendezésre,
- a rendszer- és felhasználói programokra;
- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül;
- az adatok felhasználására, tárolására vonatkozó utasításokra;
- az adathordozók tárolására, felhasználására;
- valamint a számítástechnikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési dokumentáció).

A szabályzat előírásait alkalmazni kell a Hivatal belső szervezeti egységei által vezetett nyilvántartások, adatbázisok és valamennyi egyedileg kezelt adat, elektronikus szolgáltatások illetőleg dokumentumok esetében. A Hivatalban nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, sérülés, törlés vagy megsemmisülés ellen.

Iratokat, adatokat a munkaköri feladat ellátásán kívül a munkahelyről kivinni, a munkahelyen kívül feldolgozni, tárolni csak a jegyző egyetértésével lehet, azzal a feltétellel, hogy az irat, adat tartalmát illetéktelen személy nem ismerheti meg.

II. ALAPFOGALMAK

Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

Adathordozó: olyan anyagi eszköz, közeg, mely alkalmas adatok megőrzésére, tárolására.

Adatbiztonság: az elektronikus, illetve egyéb úton tárolt információk hozzáférhetőségének szintjét határozza meg az adatok által képviselt érték szerint.

Adatfeldolgozás: az adatkezeléshez kapcsolódó technikai feladatok elvégzése.

Adatállomány: az egy nyilvántartásban kezelt adatok összessége.

Adatkezelés: az alkalmazott eljárástól függetlenül adatokon végzett bármely művelet vagy műveletek összessége, így például az adatok gyűjtése, felvétele, rögzítése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összekapcsolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása.

Adatkezelő: az a belső szervezeti egység, amely a személyes, illetőleg a közérdekű adatok körébe tartozó adatok, dokumentumok kezelését, szolgáltatását ellátja.

Adatvédelem: azon biztonsági tényezők összessége, melyek az adatok illetéktelenek általi hozzáférés, természeti csapás, rongálás, lopás kockázati tényezőit megszünteti (csökkenti), továbbá biztosítja az üzemfolytonosságot.

Adatmegsemmisítés: az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

Adatközlő: az a belső szervezeti egység, amely az adatfelelős által szolgáltatott adatokat a jogszabályokban meghatározott módon közzéteszi.

Adattörlés: az adatok felismerhetetlenné tétele olya módon, hogy a helyreállításuk többé nem lehetséges.

Számítógép hálózat: a Hivatalban kiépített integrált számítógép hálózat, a központi kiszolgáló gépet (szervert) és a felhasználói munkaállomásokat összekötő, azok hálózatba kapcsolt működését biztosító része.

Számítástechnikai eszközök: A hálózatra kapcsolódó, vagy attól függetlenül, de azonos funkcióval működő, a Hivatal tulajdonában vagy használatában lévő eszközök (számítógépek, nyomtatók, scannerek, modemek, aktív, ill. passzív hálózati elemek).

Informatikai szolgáltatás: A Hivatal által az informatikai eszközökkel nyújtott szolgáltatások összessége.

Elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme a rendszerben kezelt adatok, bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos.

Biztonsági osztály: az elektronikus információs rendszer védelmének elvárt erőssége.

Biztonsági osztályba sorolás: a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása.

Biztonsági szint: a szervezet felkészültsége a törvényben és végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésre.

Felhasználó: Egy adott elektronikus információs rendszert igénybe vevők köre.

Rendszergazda: Az a felelős személy, aki gondoskodik az informatikai szolgáltatás folyamatos, hatékony és biztonságos működtetéséről.

Login név: A hálózat, felhasználói programok használatához szükséges azonosító név.

Szerver: A számítógépes hálózatban kitüntetett szereppel ellátott nagy teljesítményű központi számítógép(ek), melyen a hálózati munkát lehetővé tevő operációs rendszer fut, és más számítógépeket kapcsol össze.

Szoftver: Szellemi alkotás, mely magában foglalja a programokat, eljárásokat, módszertant és bármilyen kapcsolódó dokumentációt, amelyek az adatfeldolgozó rendszer működésére vonatkoznak. Megjegyzés: A szoftver független a médiumtól, amely rögzíti.

Szoftver beszerzés: A számítógépeken futó különféle célú programok megvásárlása vagy fejlesztetése. A szoftverbeszerzést komplexen kell értelmezni, a megvásárlás (megírás), a telepítés, az oktatás, a betanítás, a dokumentáció beszerzésével együtt.

Külső fejlesztő: A szoftvert vagy szoftverrendszert a Hivatal megrendelésére kifejlesztő szervezet/személy.

Megrendelő: Beszerzéseknél a Hivatal, amely a szoftverterméket vagy rendszert megvásárolja, és szerződéses kapcsolatban áll (hat) a külső fejlesztővel vagy szállítóval.

Végfelhasználó**:** Az a személy, aki a szoftverterméket/rendszert használja.

III. Az adatkezelés, az adatvédelem követelmény rendszere, informatikai rendszerek védelme

3.1. **Az adatvédelem tárgya**:

- a Hivatal működése során keletkezett személyes és közérdekű adatok teljes köre, keletkezésüktől a megsemmisítésükig
- az adathordozók fizikai jellegüktől függetlenül, amelyek személyes, illetőleg közérdekű adatokat tartalmaznak,
- az a fizikai környezet, ahol az adatállomány kezelése, tárolása történik.

3.2. **Az adatkezelés alapkövetelményei:**

Az adatkezelés során biztosítani kell:

- az adott egyén szempontjából fontos adatok helyes, pontos kezelését, hibás adat előfordulása esetén annak észlelésekor hivatalból, valamint az érintett kezdeményezésekor a pontosítást haladéktalanul teljesíteni kell;
- az adott személy adatai kizárólag a jogszabály rendelkezéseivel összhangban kerüljenek feldolgozásra, rögzítésre, felhasználásra, illetőleg ne kerüljenek illetéktelenek birtokába;
- a személyes adatoknak a közérdekű adatokkal való együttes alkalmazásuk esetén nem akadályozhatják a közérdekű adatok nyilvánosságát, szolgáltatását;
- a különböző célú adatok, adatállományok (adatbázisok) folyamatos vezetését, aktualizálást és az adathordozó fajtájától független folyamatos rendelkezésre állását és elérhetőségét az arra jogosultak számára,
- a személyes adatok tekintetében minden esetben biztosítani kell a zárt kezelést és a jogszabályok szerinti előírásoknak megfelelő hozzáférést;
- a különböző adatok, adatállományok (adatbázisok) valódiságát, pontosságát, részletességét, hitelességét;
- a különböző adatok, adatállományok (adatbázisok) jellegétől függően azok bizalmas, illetőleg az adott területre vonatkozó jogszabályok szerinti kezelését,
- a Hivatal gondozásában készült információs rendszerek, adatbázisok folyamatos működését, és szükség szerinti folyamatos hozzáférés lehetőségét, a folyamatos aktualizálást, a közérdekű adatok folyamatos a jogszabályoknak megfelelő szolgáltatását.
- az adatrendszer fizikai biztonságát.

3.3. **Az adatvédelem eszközei:**

Az adatvédelem eszközeiként kell kezelni és folyamatosan biztosítani mindazon igazgatási, iratkezelési, szervezési, személyi, műszaki, technikai, informatikai és egyéb intézkedéseket, melyek elengedhetetlenek az egyes adatok, adatállományok (adatbázisok) zavartalan működéséhez, és védelmet nyújtanak ahhoz, hogy

- illetéktelenek ne jussanak a különböző személyes adatokhoz (személyes adatokat tartalmazó adatbázisokhoz), dokumentumokhoz,
- a különböző adatok (adatbázisok) dokumentumok megsérülésére, meghibásodására ne kerüljön sor,
- az adatkezelés során ismeretek hiánya, hozzá nem értés miatt, emberi mulasztásból károsodásra, adatok, dokumentumok megsemmisülésére ne kerüljön sor,

3.4. **Személyi feltételek biztosítása**

A személyes adatok kezelésével kapcsolatos teendőket csak a hivatal illetékes belső szervezeti egység e feladattal megbízott ügyintézői látnak el. A folyamatos ügyintézés érdekében a megfelelő helyettesítésről gondoskodni kell. A közérdekű adatok folyamatos szolgáltatása érdekében a feladatkör szerint illetékes belső szervezeti egység vezetője felelős a szakterületet jól ismerő és az elektronikus adatkezelésben, tájékoztatásban jártas személy(ek) kijelöléséért.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról a Hivatal adatvédelmi felelősének kell gondoskodnia.

A rendszergazda végzi az informatikai védelmi rendszer biztosítását, a vírusvédelmi szoftverek frissítését, valamint biztosítja a rendszer üzemképességét és a műszaki ellátást, biztonsági másolatot készít, segíti, ellenőrzi a Hivatal dolgozóinak számítástechnikai munkáját.

3.5. **Fizikai, technikai, logikai védelem**

Tűzvédelem

A szerverszoba, illetve az informatikai eszközöket tartalmazó irodák a "D" tűzveszélyességi osztályba tartoznak, amely mérsékelt tűzveszélyes üzemet jelent. A szerverszoba tűz- és villámvédelmi rendszerrel felszerelt helyiség lehet.

Vagyonvédelem, fizikai biztonság

- a szerverszobát biztonsági zárral kell felszerelni,
- a szerverszobába való be- és kilépés rendjét szabályozni kell,
- a szerverszoba kulcsát a hivatali rendszergazda tárolja, onnan csak az arra feljogosítottak vehetik fel,
- a szerverszobát behatolás védelmi rendszerrel kell ellátni,
- munkaidőn túl az irodákban, illetve a szerverszobában csak engedéllyel lehet tartózkodni,
- a szerverszobába történő illetéktelen behatolás tényét az ezt észlelő a jegyzőnek azonnal jelenti,
- az irodahelyiségekben elhelyezett számítástechnikai eszközöket csak a kijelölt köztisztviselők használhatják,
- a számítástechnikai eszközök rendeltetésszerű működéséért a felhasználó felelős.

Logikai védelem

- többszintű hozzáférés biztosítása, az alkalmazásokhoz újabb azonosítás szükséges,
- biztonsági események naplózása, mellyel nyomon követhető a felhasználók által elvégzett tevékenység.

3.6. **Adathordozók védelme, tárolása, hordozása és karbantartása**

- az adathordozókat zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat azonosítóval kell ellátni,

- az adathordozók nyilvántartásában az azonosító adaton kívül a felírás és megőrzés dátumát, jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell feltüntetni,
- az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet,
- az adathordozók megőrzésének idejét a felelős vezető határozza meg,
- olyan adathordozót, amelyet javíthatatlan károsodás ért meg kell semmisíteni oly módon, hogy az eljárás eredményeként semmilyen módon ne legyen helyreállítható (fizikai megsemmisítése, bezúzás, mágneses vagy optikai meghajtó esetén demagnetizálás)

IV. ÜZEMELTETÉSI SZABÁLYOK

4.1 Felhasználókra vonatkozó szabályok

Felhasználó lehet, az önkormányzat képviselője, a Hivatal dolgozója (köztisztviselő és egyéb jogviszony keretében foglalkoztatott), illetve egyéb személy, aki felhasználói jogot kért és kapott. Egyéb személy felhasználói jogot csak jegyzői engedéllyel szerezhet.
A munkaállomás használatba vételével egyidejűleg felhasználó az intézkedés 1. sz. mellékletében lévő nyilatkozat aláírásával magára nézve kötelezőnek elfogadja a hivatali hardver és szoftver eszközök használatának mindenkori szabályait.

A felhasználó joga van:
- tájékoztatást kapni a helyi felhasználói szabályokról, a rendszergazda személyéről, feladat- és hatásköréről,
- a számára megítélt erőforrások biztosítását a rendszergazdától kérni,
- a géphez hozzárendelt szolgáltatásokat a felhasználói kategóriába sorolástól függően igénybe venni.

A felhasználó kötelessége:
- figyelemmel követni az általa használt berendezések és szoftverek állapotát, az esetleges meghibásodást vagy helytelen működést, melyet azonnal jelezni kell a rendszergazdának.
- munkája során figyelemmel kell lenni arra, hogy illetéktelen személyek ne nyerjenek betekintést a feldolgozás alatt álló adatokba,
- a számítógépes infrastruktúrát rendeltetésének megfelelően használni,
- együttműködni a rendszergazdával, köteles figyelembe venni a megfelelő üzemelés érdekében tett javaslatokat,
- vírusfertőzés (vagy annak gyanúja) esetén a rendszergazdát azonnal értesíteni,

A felhasználónak TILOS:
- a számítógép közelében ételt és italt fogyasztani,
- a számítógép és egyéb eszközök (nyomtató, fax, fénymásoló) 30 cm-es körzetében és felett virágot tartani,

- a gépek megbontása, a hardver konfigurációk megváltoztatása,
- más felhasználók munkájának zavarása, anyagainak illetéktelen megtekintése, másolása,
- más felhasználó bejelentkezési nevének, illetve jelszavának használata,
- a hálózat megbontása, átstrukturálása, gépek, eszközök engedély nélküli csatlakoztatása,
- a számára nem engedélyezett erőforrások, szolgáltatások, jogosultságok megszerzése. Az erre irányuló próbálkozás annak sikerétől függetlenül fegyelmi vétségnek minősül.

4.2. Az informatikai biztonság személyi vonatkozásai (oktatás, képzés)

- A felhasználóknak rendelkezniük kell a munkaköri kötelességük ellátásához szükséges számítógépes ismeretekkel.
- Biztosítani kell a felhasználók rendszeres információbiztonsági oktatását, tudatosítását, tájékoztatását.
- A képzés foglalja magába a biztonsági követelményeket, a jogi felelősséget, az óvintézkedéseket, valamint az informatikai eszközök helyes használatát, az informatikai biztonságpolitikában előírtakat.
- A felhasználóknak ismerniük kell a biztonsági felelősségüket, a biztonsági eljárások alkalmazását és az adatfeldolgozó lehetőségek korrekt használatát, hogy ezzel is minimálisra csökkentség a lehetséges biztonsági kockázatokat, és alá kell írniuk az erről szóló nyilatkozatot (2.sz.melléklet).
- Minden felhasználónál tudatosítani kell a biztonsági szabályok megsértésével járó szankciókat, és azokat következetesen be kell tartani.

4.3. Üzemeltetőkre vonatkozó szabályok

<u>Általános üzemeltetési feladatok</u>

A hivatali számítógépes infrastruktúra általános üzemeltetési feladatait a rendszergazda látja el. A rendszergazda a hálózat biztonságos működése érdekében, hiba esetén jogosult valamely berendezést, részhálózatot a hivatali hálózatról a hiba elhárításáig lekapcsolni. Erről a jegyzőt előzetesen értesítenie kell.

<u>A rendszergazda feladatai:</u>

- a hálózati struktúra tervezése, az új elemek becsatlakozásának szabályozása,
- hálózaton működő alkalmazások telepítésének tervezése, telepítése vagy a telepítés szakmai felügyelete, használatuk szabályozása,
- a hálózati forgalom figyelése,
- a hálózati hibák felderítése, az elhárításhoz szükséges intézkedések megtétele,
- a hálózati felhasználók üzemeltetési feladatainak szakmai irányítása.
- a hivatali szintű informatikai alkalmazások felügyelete, folyamatos működésük biztosítása,
- az alkalmazás használatához szükséges hálózati- és erőforrás-hozzáférési jogok biztosítása a felhasználók részére,
- az alkalmazásokkal kapcsolatos, felhasználóktól érkező észrevételek fogadása, a szükséges változtatások, módosítások megtétele, regisztrálása,
- a hálózati struktúra nyilvántartása,
- a felhasználók nyilvántartása és tájékoztatása,

- felhasználói programok havi és rendkívüli frissítése,
- új hardver kiegészítők illesztése a már meglévő konfigurációkhoz,
- hardver változtatások végrehajtása hibajavítás vagy elavulás esetében,
- hardver, szoftver nyilvántartási adatok folyamatos frissítése,
- a felhasználók betanításában való közreműködés,
- felhasználói dokumentációk biztosítása,
- az informatikai alkalmazások felügyelete, folyamatos működésének biztosítása,
- a kormányzati eseménykezelő központ (NEIH) által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseket, szükség esetén belső biztonsági riasztást és figyelmeztetést ad ki.

4.4. Karbantartási eljárásrend

Berendezések karbantartása

Az üzemszerű működés fenntartásához elengedhetetlen, hogy a számítástechnikai eszközök időszakosan karbantartva legyenek.

- számítógépek, perifériák, nyomtatók meghibásodása vagy felhasználó váltása estén, illetve 1 év folyamatos üzemelés után az alapvető karbantartást el kell végezni (felület tisztítása, az eszköz belsejéből a por eltávolítása, érintkezők tisztítása),
- az informatikai rendszereket kiszolgáló szerverek karbantartását évente el kell végezni (tisztítás, portalanítás stb.),
- a működéshez szükséges hálózati kiszolgáló eszközök (switch, router) meghibásodása esetén azokat a tartalék készletből azonnal pótolni kell.

Szoftverek karbantartása

- a rendszergazda köteles a használt szoftverek frissítéseit figyelemmel kísérni, a kritikus frissítéseket haladéktalanul telepíteni,
- az üzemeltetett informatikai rendszerek verzióváltásait annak rendelkezésre állása után azonnal telepíteni kell,
- rendszergazda folyamatosan ellenőrzi, hogy minden használt szoftver üzemeltetési feltételei biztosítottak-e (szükséges memória mennyiség, tárterület).

Az elvégzett karbantartási munkákat a karbantartási naplóban rögzíteni kell. (3. sz. melléklet)

4.5. Elszámoltathatóság és ellenőrizhetőség

- informatikai rendszerek naplózási rendszerének kialakítása (Windows naplófájlok, adatbázisok log fájlok), hogy utólag meg lehessen állapítani az informatikai rendszerben bekövetkezett fontosabb eseményeket, ezáltal ellenőrizni lehessen a hozzáférések jogosultságát, meg lehessen állapítani a felelősséget, valamint illetéktelen hozzáférés megtörténtét,
- a biztonsági napló adatait havonta egy alkalommal a rendszergazdának ellenőrizni kell,

- az esetleges illetéktelen hozzáférést, jogosultságokkal való visszaéléseket - melyek szankciókat vonnak maguk után - jegyzőkönyvben rögzíteni kell,
- a visszaélés tényét a hivatal vezetője felé azonnal jelezni kell,
- a biztonsági naplók és a jegyzőkönyvek archiválandók, adatait védeni kell az illetéktelen hozzáféréstől,
- a naplóállományok megőrzési idejét az iratkezelési szabályzat részeként kell meghatározni.

V. Biztonsági, védelmi előírások, katasztrófa-elhárítás

5.1. A jelszókezelés, azonosítás, hitelesítés szabályai

A jelszó a hozzáférés kezelés alapvető eszköze, így az informatikai biztonság fontos része. Az informatikai rendszert használóknak tisztában kell lenniük a jelszavak fontosságával és a nem megfelelő jelszókezelés következményeivel, mert egy rosszul megválasztott, könnyen kitalálható jelszó nem csak a jelszó tulajdonosára hanem a Hivatal informatikai rendszerére is negatív következményekkel járhat.
A hivatalban működő felhasználói jogosultságait minden esetben a szervezeti egység vezetőjének kezdeményezése alapján a hivatal vezetője határozza meg (4.sz. melléklet). Ennek menedzselése a rendszergazda feladata. A jelszavak két csoportja szerint egyszerű felhasználói vagy adminisztrátori azonosítót véd. A szabályozás ennek függvényében eltérhet. Az un. adminisztrátori jelszavak tárolása zárt borítékban, páncélszekrényben történik, ennek felbontása csak indokolt esetben jegyzőkönyv kiállításával történhet. Az esetleges elfelejtett jelszavak újragenerálását csak a rendszergazda végezheti. A hálózaton adatok megosztása csak ellenőrzött módon, a megfelelő felhasználói jogosultságok beállítása mellett történhet. A számítógépeken működő operációs rendszerek, irodai programcsomagok, valamint bármilyen felhasználói programok ellenőrzése történhet szúrópróbaszerűen, valamint az éves leltározás kapcsán is. Az ellenőrzésre jogosult személy a rendszergazda.

Jelszóvédelem:

- A jelszót a felhasználón kívül kizárólag a rendszergazda ismerheti.
- A jelszót tilos másoknak elmondani, a jelszóról mások előtt beszélni.
- Tilos közös jelszavakat használni.
- A jelszót nem szabad leírni és hozzáférhető helyen tárolni.
- A jelszót nem szabad telefonon vagy e-mailben továbbadni.
- Ne használjuk a programok (böngészők) jelszó megjegyző funkcióját.
- Jelszavunkat ne írjuk be kérdőívekbe, űrlapokba.
- Ha a jelszó kompromittálódott vagy erre utaló jeleket lehet észlelni, azonnal meg kell változatni a jelszót és értesíteni kell a rendszergazdát.

5.2 Biztonsági kritériumok

Annak megelőzése érdekében, hogy az adatkezelésre használt számítástechnikai eszköztárba illetéktelenek bevitelt hajtsanak végre, vagy annak tartalmát illetéktelenül megismerjék, lemásolják, töröljék vagy bármilyen módon megváltoztassák, az adatvédelmi, üzemeltetési, technikai, biztonsági szabályokat be kell tartani.

Az információ vagyon védelmének szabályai:

Titokvédelem: a Hivatal informatikai adatfeldolgozással és kezeléssel, valamint közzététellel foglalkozó minden munkatársának munkája során kötelessége betartani a Hivatal adatvédelmi és adatbiztonsági szabályzatában foglaltakat.
Adatvédelem: Minden felhasználó az általa végzett elektronikus adatfeldolgozás során személyesen felelős az adatvédelmi szabályok és információbiztonsági előírások betartásáért.
Információvédelem: a Hivatal számítógépeiről, szervereiről – a munkahelyi célú felhasználás kivételével – nem engedélyezett programok, minősített adatot tartalmazó adatállományok, illetve a munkavégzés során szerzett egyéb adatok másolása, azok más, illetéktelen személyekkel történő megismertetése. Az adathordozók és nyomtatványok tárolása során gondoskodni kell az illetéktelen személyek elleni hozzáférés megakadályozásáról.
IT biztonság: az informatikai rendszerek által kezelt adatok hitelességének, bizalmasságának, sértetlenségének, rendelkezésre állásának megőrzése.

Információ biztonság követelményei:

Bizalmasság
A Hivatal területén végzett minden ügyfélforgalmi és ügyfél kiszolgálási tevékenység során szem előtt kell tartani az ügyelek adatainak és információinak bizalmas jellegét, ezért az informatikai struktúrát és környezetet ennek megfelelően kell kialakítani.

Sértetlenség
Számítógép vagy programhibából eredő adatvesztés gyanúja esetén a rendszergazdát haladéktalanul értesíteni kell. A mentések és archívumok tárolása és őrzése során biztosítani kell az adatok sértetlenségét.

Rendelkezésre állás
A rendszergazda feladata az informatikai rendszerek folyamatos rendelkezésre állását biztosítani rendszeres adatmentések és szoftvertelepítő készletek megfelelő biztosításával, tárolásával, valamint a szükséges karbantartási tevékenységek elvégzésével.

5.3. Személyi védelmi előírások

Felhasználói jog csak a munkakörnek megfelelő erőforrás-hozzáférés engedélyezése után szerezhető meg.

A rendszergazda gondoskodik a felhasználó hozzáférési jogainak törléséről kilépésekor.

Illetéktelen hozzáférés megakadályozása céljából az alábbi előírásokat kell betartaniuk a felhasználóknak:

- A belépéshez szükséges jelszót biztonságos helyen kell tárolni, soha nem szabad azt a számítógép közelében felírva hagyni.
- Olyan jelszót célszerű választani, amit nem könnyű kitalálni, és a jelszót gyakran meg kell változtatni.
- Óvakodni kell attól, hogy mások jelenlétében gépeljük be a jelszót.
- Amikor nincs szükség a számítógépre, ki kell kapcsolni.

5.4. Szoftvervédelmi előírások

Rendszerszoftver:

Az üzemeltetésért felelős rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

Felhasználói programok:

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni. Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

A Hivatalban dolgozók felhasználói jogosultságát és annak körét a rendszergazda saját nyilvántartásában vezeti.

5.5. Adatok mentése

Az elektronikusan tárolt adatok folyamatosan ki vannak téve a hardver meghibásodási lehetőségének, ezért a biztonság növelés és a károk csökkentése érdekében szükség van rendszeres mentésekre, archiválásra.

Az első szintű védekezés a kiszolgálók védelme. A Hivatalban a szervereken tárolt adatok védelme RAID 1. tükrözéssel megoldott. Az esetleges elemi kár, váratlan egyéb Vis Major (pld. túlfeszültség, tápegység meghibásodása, tűzeset) esemény bekövetkezésekor akár a RAID összes merevlemeze tönkremehet, ezért a helyreállítás érdekében egy külön álló helyiségben NAS szerverre is 5 munkanapi gyakorisággal biztonsági mentések készülnek.

5.6. Az adatok visszaállítása, katasztrófa-elhárítás

A vészhelyzetekből eredő veszteségek csökkentéséhez szükséges, hogy a számítógépes infrastruktúra bármely elemének károsodása esetére "készenlétben álljon" az alkalmazandó megoldás. Az 5.5. pontban részletezett mentési rendszer szolgáltatja a programok és adatok visszaállíthatóságának alapját.

Az adatok visszaállítása történhet valamely vészhelyzetben, a számítógép olyan szintű meghibásodásakor, hogy a rajta tárolt információk már nem másolhatóak új gépre, továbbá az adatrendszer sérülése vagy egyéni igény alapján (pl. visszavonhatatlan hibás rögzítés). Az adatrendszer sérülése esetén a rendszergazda a legfrissebb mentés vagy archiválás alapján elvégzi az adatok visszatöltését és az érintett irodák dolgozóit felkéri a mentés utáni adatváltozások rögzítésére.

Munkaállomás meghibásodása esetén a javítás megkezdése előtt, amennyiben lehetséges, teljes adatmentést kell végezni, ezt követi a felhasználóhoz rendelt operációs rendszer és a felhasználói programok telepítése, konfigurálása.

5.7. Egyéb adatbiztonsági megoldások

A Hivatal vírusellenőrző programjai adatállományának frissítéséről a rendszergazda gondoskodik, az internetről letöltött vagy a program tulajdonosa által küldött frissítési adatállományok alapján.

A hálózaton tárolt nagy adatbázisok megrongálódástól való védelmét szolgálja a szerverek szünetmentes áramforrással való ellátottsága, ami biztosítja a hálózati operációs rendszer részére a szükséges időt a nyitott adatbázisok lezárására, minimalizálva az áramszünetből adódó adatvesztés lehetőségét. A szervereket klimatizált környezetben kell elhelyezni. A helyiségben a villámvédelmet biztosítani kell.

VI. Szoftverekkel kapcsolatos szabályok

6.1. Szoftverek beszerzése

A Hivatal számítógépes rendszerében csak legális, jogtiszta szoftverek üzemeltethetőek. További követelmény, hogy a szoftverek integráltan, összehangoltan működjenek. Ezen célok biztosítása érdekében új szoftverek beszerzése kizárólag a rendszergazda véleménye után lehetséges. A beszerzések során az alábbiak megtartása szükséges.

6.2. Források

A szoftverek beszerzésére fordítható összegeket a Hivatal költségvetése szabja meg. Az egyes szervezeti egységek igényeiket a jegyző felé a költségvetés összeállítása előtt jelzik. A rendszergazda feladata a szükségszerű cserékről, frissítésekről a jegyzővel konzultálni. A rendszergazda véleményezi a beszerezni kívánt szoftver igényeket, véleménye a szoftver tartalmára és árára egyaránt vonatkozik.

6.3. Szoftverek kiválasztása

A szoftverek kiválasztására szóló javaslattétel a rendszergazda feladatkörébe tartozik. A különböző felhasználói igények megfelelő szintű kielégítése érdekében a megfelelő alkalmazói szoftver kiválasztása előtt a rendszergazda konzultál az igénylő iroda szakembereivel.

6.4. Szoftver vásárlás

Szoftver vásárlása csak közvetlenül a szoftver gyártótól, vagy annak hivatalos viszonteladójától történhet. A vásárlásnál figyelembe kell venni a tervezett felhasználói számot. A szoftvert a megfelelő számú felhasználói licensszel együtt kell megvásárolni, illetve regisztráltatni.

6.5. Külső fejlesztés (outsourcing)

Külső fejlesztést csak fejlesztési szerződés alapján lehet végeztetni. A szerződésnek pontos specifikációt és ütemtervet kell tartalmaznia.

6.6. Szoftverek telepítése

Szoftver-telepítését csak a rendszergazda, szerződés alapján a beszállító, illetve meghibásodás esetén a karbantartásra szerződött cég végezhet. Ez egyaránt vonatkozik hálózatos szoftverek esetén a szerverre történő telepítésre és a felhasználókhoz való installálásra is.

6.7. Jogvédelem

A Hivatal rendszerébe, akár hálózatra, akár önálló gépre, csak legálisan beszerzett, jogtiszta szoftver telepíthető, illetve ezen eszközökön csak legálisan beszerzett, jogtiszta szoftverek tarthatóak. Ennek központi ellenőrzéséről a rendszergazda gondoskodik.

6.8. Szoftverek üzemeltetése

A szoftverek üzemeltetési feladatait a rendszergazda látja el. Ez folyamatos tevékenységet igénylő feladat, mind a szoftverkövetés, rendszeres mentés, mind pedig a rendszerhasználat felügyelete, ellenőrzése.

A rendszergazda feladata a felhasználók rendelkezésére állás azok szoftver kezelési, szoftver működési problémáival kapcsolatban. A szoftverek kezelési problémáira helyszíni vagy telefonos segítségnyújtással, dokumentációkkal adhat megoldást.

A felhasználók problémáik megoldását a rendszergazdától közvetlenül kérhetik. A rendszerfelügyelet célja a rendeltetésszerű használat ellenőrzése, biztosítása. Ebbe beletartozik az illegális szoftver- ill. rendszerhasználatok kiderítése és megakadályozása, a vírusfertőzések ellenőrzése, jelentése és megszüntetése éppúgy, mint a nem használt szoftverelemek behatárolása, kivonásukra vagy kiváltásukra történő javaslattétel.

VII. Informatikai védelem

7.1. A helységek és berendezések használatára vonatkozó szabályok

- A szerverszobában a rendszergazdán, valamint az informatikai rendszer üzemeltetését végző gazdálkodó szervezet munkatársán kívül más nem tartózkodhat. Más személyek benntartózkodását a szervezeti egység vezető engedélyezheti. A szobába való belépéseket naplózni kell. (5.sz.melléklet)

- Üzemidőn kívül az ajtókat zárva kell tartani. A szerverszoba kulcsát az adatvédelmi felelős és/vagy a rendszergazda tárolja, onnan csak az arra feljogosítottak vehetik fel. Munkaidőn kívül idegen személy csak felügyelet mellett tartózkodhat a gépteremben. A szerverszoba áramtalanításáért a rendszergazda felelős.

- Az irodákban/szerverszobában a folyamatos, higiénikus munkavégzés feltételeit kell megőrizni. A szerverszobai rend megtartásáért és a biztonságos műszaki üzemeltetésért a rendszergazda a felelős.

- A szerverszobába ételt, italt bevinni és ott elfogyasztani szigorúan TILOS!

- A szerverszobába égő cigarettával belépni és ott dohányozni, valamint tüzet okozó tevékenységet folytatni szigorúan TILOS!

- A szerverszoba takarítását csak a rendszergazda felügyelete mellett, legalább havonta egyszer, a kijelölt személyek végezhetik.

- A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak a rendszergazda és a szervizek szakemberei végezhetnek.

- A számítógépeket csak rendeltetésszerűen és az ütemezett munkák elvégzésére lehet használni. Tilos a számítógépeken játszani, illetve az informatikai rendszer biztonságát veszélyeztető tevékenységet végezni.

- Adathordozókat csak a rendszergazda engedélyével lehet be- és kivinni a szerverszobából.

- Az elektromos hálózatba más - nem a rendszerekhez, illetve azok kiszolgálásához tartozó - berendezéseket csatlakoztatni nem lehet.

- A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabályok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármely beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat. A fenti rendelkezések megsértése esetén az elkövetővel szemben az adatvédelmi felelős fegyelmi felelősségre vonást kezdeményezhet

A számítógépekkel kapcsolatos hibajelentések a felhasználóktól közvetlenül a rendszergazdához futnak be. Szoftveres probléma esetén a rendszergazda gondoskodik a hiba okának feltárásáról és a legrövidebb időn belüli megszüntetéséről, lehetőség szerint a helyszínen, a számítógép elszállítása nélkül.

7.2. Védelmi előírások

- A számítógépeket csak indítójelszóval lehessen elindítani, induláskor minden esetben vírus-ellenőrző programot kell elindítani.
- A feldolgozáshoz szükséges programok elindításához és az adatok hozzáféréséhez jelszóvédelem kell.
- A bizalmas adatállományokat és dokumentumokat titkosítani kell, a titkosítás végezhető az adott szoftverrel, vagy külső programmal is.
- A módosításokról napi mentést kell készíteni, ezeket a heti mentésekig kell megőrizni.
- A teljes anyagról heti mentéseket kell készíteni.
- A teljes anyagról a tárgyévet követő év első munkanapján mentést kell végezni.
- A felhasznált programokról biztonsági másolatot kell készíteni, és azokat az eredeti példánytól külön, tűzbiztos helyen kell tárolni.

7.3. Vírusvédelem

A Hivatal a vírusvédelmi feladatokat az ESET Endpoint Security szoftver segítségével látja el. A vírusvédelemért felelős rendszergazda köteles mind a munkaállomásokon, mint a szervereken a szoftver telepíteni és megfelelő konfigurálásáról gondoskodni.

A munkaállomásokon és szervereken, ha másképp nincs rendelkezés, heti rendszerességgel vírusellenőrzést és vírusirtást kell tartani.

A vírusvédelmi programok adatbázisát naprakészen kell tartani.

Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell az illetékes szakembernek, rendszergazdának. Amennyiben nincs erre lehetőség (pl. munkaidőn kívül), a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni. A gépet addig bekapcsolni nem szabad, amíg azt az arra illetékes szakember, rendszergazda meg nem vizsgálta. A vírusfertőzést jelenteni kell a szervezeti egység vezetőjének, még akkor is, ha semmi hiba nem történt a fertőzés folyamán, valamint a szervezeti egység vezetőjének ki kell deríteni a fertőzés lehetséges okait, és a szükséges védelmi intézkedést meg kell hoznia.

7.4. A levelezés szabályai:

A szabályozás célja, hogy biztosítsák az elektronikus levelezés zavartalanságát, valamint védjék a Hivatal érdekeit. Minden felhasználónak és szervezeti egységnek lehetősége van levelezési címet igényelni, és ezt kizárólagosan hivatalos célra használni. A cím név@komlo.hu.

A hivatal e szabályokra figyelemmel monitorozhatja a hálózatból küldött, illetve fogadott levelek tartalmát az adatvédelmi szabályok és ajánlások figyelembevételével.
A hivatal hálózatán keresztül küldött vagy fogadott levelek központilag vírus- és kémprogram ellenőrzés történik, ami különböző védelmi és szűri funkciókkal egészül ki. A Hivatal hálózatán keresztül küldött levelek központilag Spam ellenőrzésen esnek át.

Alapelvek

- A levelek nem tartalmazhatnak a hatályos magyar jogszabályokba ütköző tartalmat.
- A levelek nem sérthetik mások becsületét, emberi jogait, faji, nemzetiségi hovatartozását, vallási, politikai világnézetét.
- A levelezés nem veszélyeztetheti a hálózati infrastruktúra működését.

Szabályok

- Tilos kéretlen leveleket, hirdetéseket, kör e-maileket küldeni.
- Tilos kör e-maileket reklám anyagokat tovább küldeni.
- Tilos az e-mail címet olyan kereskedelmi listára feltenni, amelyről a hivatali levelező rendszert e-mail szeméttel (spam) terhelhetik meg.
- Tilos a hivatali e-mail cím magánjellegű felhasználása.
- Tilos a hivatali e-mail címet bármely weboldalon regisztrációhoz felhasználni.
- Tilos ismeretlen vagy gyanúsnak tűnő feladótól érkezett levelek mellékletének megnyitása, vagy továbbítása.

7.5. Internethasználat szabályai:

Az internet használata során tilos a közösségi oldalak, chat programok használata, nem szakmai jellegű fájlok letöltése.

7.6. A Hivatali hálózat és hálózatában résztvevő eszközök távoli elérésének szabályozása

A szabályozás célja, hogy meghatározza a Hivatal belső hálózatához való távoli gépről történő csatlakozás szabályait. A cél a hivatal hálózatának és hálózatán tárolt adatok védelme, a hálózati eszközök sebezhetőségének csökkentése. A károk magukban foglalják az érzékeny adatok elvesztését, a hivatal anyagi károsodását és az eszközök rendelkezésre állását.

- A távoli elérésnek VPN (Virtuális magánhálózati) kapcsolaton keresztül kell megvalósulnia
- A rendszerbe való belépéshez szükséges a felhasználó azonosítására szolgáló felhasználói név jelszó megadása.
- A belépési azonosítókat másra átruházni, illetve más azonosítóját használni szigorúan TILOS!

VIII. Biztonsági eseménykezelési eljárásrend

Biztonsági incidensnek számít minden, az informatikával kapcsolatba hozható rendellenes működés, fenyegetés, amely az adatok bizalmasságát, sértetlenségét vagy rendelkezésre állását veszélyezteti.

- Jogosulatlan hozzáférés (informatikai eszközhöz, alkalmazáshoz, adathoz, biztonsági zónához).
- Információs vagyon (eszköz, szoftver, adat stb.) elvesztése, eltulajdonítása, vagy megrongálódása,
- Határincidensek, vírusfertőzések.
- Mentési feladatok végrehajtásának akadályoztatása.
- Működési rendellenességek (információ biztonságot veszélyeztető eszköz hiba, program hiba, információ rendelkezésre állásának elvesztése, hibás adatok stb.).
- Az IBSZ-ben hivatkozott törvények, szabályzatok és előírások megsértésére utaló cselekmények.

A szervezet minden informatikai eszközén folyamatosan figyelni kell a rendszerek esetleges hibaüzeneteit.

Teendők rendszer-, illetve alkalmazáshiba esetén:

- Figyelemmel kell kísérni a működési zavar tüneteit, a képernyőn megjelenő üzeneteket. Rendszer-, vagy alkalmazáshiba esetén az adott számítógépen fel kell függeszteni a munkát, a hibát azonnal jelenteni kell a rendszergazdának. A hibaüzenetet a felhasználó nem törölheti a képernyőről, amíg azt a rendszergazda nem látta. A felhasználó semmiféle kísérletet nem tehet a számítógép rendszert, vagy a hálózat működését érintő hiba megszüntetésére, még akkor sem, ha kellő felhasználói ismeretekkel rendelkezik. A hiba elhárítására csak az illetékes rendszergazda jogosult!
- Amennyiben a rendszerhibát vélhetően külső, illetéktelen beavatkozás vagy vírustámadás okozta, az érintett munkaállomást, számítógépet le kell választani a hálózatról, szükség esetén ki kell kapcsolni és haladéktalanul értesíteni kell a rendszergazdát. Ilyen esetekben fokozottan figyelni kell a hordozható adattárolókra (floppy lemez, Flash memória), melyeket a rendszergazdának vizsgálat céljára át kell adni.
- A Hivatal hozzáférési és egyéb adatvédelmi rendszereinek működési zavarát, a megtett intézkedéseket haladéktalanul jelenteni kell a rendszergazdának.
- A meghibásodott számítógépben használt adathordozók kizárólag a biztonsági ellenőrzést követően használhatók más számítógépekben.

Programhibák jelentése:

A hiba tüneteit, a képernyőn megjelenő minden üzenetet fel kell jegyezni.
A számítógépet el kell szigetelni a hálózattól és használatát beszüntetni.
Az eseményt azonnal jelenteni kell a rendszergazdának.

Az incidensek kezeléséért felelős személy a rendszergazda, aki az eseményt haladéktalanul köteles kivizsgálni és a biztonsági esemény súlyosságától függően köteles a jegyzőnek és az adatvédelmi felelősnek jelenteni. Amennyiben a felelősségre vonás szükségessége fennáll, értesíti a munkáltatók jogkör gyakorlóját arról, hogy a munkavállalóval szemben a kötelességszegés gyanúja esetén alkalmazott eljárást meg kell indítani.

A biztonsági események prioritását mérlegelve kell a helyreállítást megkezdeni. Az ügymenet működésének fenntartására, és a kritikus informatikai folyamatoknak a meghibásodást vagy a megszakadást követően a kívánt időn belüli helyreállítására vonatkozó eljárásokat a Hivatal „Ügymenet-folytonossági Terve" tartalmazza.

IX. Biztonsági osztály

Az állami és önkormányzati szervek elektronikus információbiztonságról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatálya alá tartozó szervezeteket biztonsági szintbe kell sorolni. A biztonsági szintekbe sorolás a 77/2013. (XII.19.) NFM rendelet alapján az informatikai rendszerek biztonsági osztályba sorolása alapján történik. A szervezet besorolási szintje az informatikai rendszerek legmagasabb biztonsági osztályával azonos besorolású, de legalább az Ibtv.9.§ (2) bekezdésében meghatározott 2. biztonsági szintű.

Az elvégzett kockázatelemzés, kárérték becslés és az informatikai rendszerek osztályba sorolása alapján **a Hivatal biztonsági szintje 2.**

A biztonsági szint meghatározását legalább háromévenként, az elektronikus információs rendszer biztonságát érintő változás esetén soron kívül meg kell ismételni.

IX. Záró rendelkezések

A szabályzatban érintett dolgozók munkaköri leírásába be kell építeni a szabályzatban előírt feladatokat.

Jelen szabályzatban nem szabályozott adatvédelemre és adatbiztonságra vonatkozó előírásokat a Komlói Közös Önkormányzati Hivatal adatvédelmi és adatbiztonsági szabályzata tartalmazza.

Jelen szabályzat 2014. július 2. napján lép hatályba. Ezzel egyidejűleg a 2005. január 21. napján kelt Számítástechnika védelmi szabályzat hatályát veszti.

Komló, 2014. július 2.

KOMLÓI KÖZÖS ÖNKORMÁNYZATI HIVATAL JEGYZŐJE

dr. Vaskó Ernő
címzetes főjegyző

1.sz. melléklet

F E L H A S Z N Á L Ó I N Y I L A T K O Z A T

Alulírott ……. a Komlói Közös Önkormányzati Hivatal dolgozója nyilatkozom, hogy a hivatal „Informatikai Biztonsági Szabályzat”-át elolvastam és az abban foglaltakat, mint felhasználó megismertem és elfogadom.

A hivatal számítógépes hálózatát a szabályzatnak megfelelően használom, a hálózati hozzáférést biztosító jelszavamat más személynek nem adom ki, a munkám során tudomásomra jutott információkat megőrzöm, illetéktelen személyek részére nem adom át.

Komló, ……..

……
aláírás

2.sz. melléklet

N Y I L A T K O Z A T

Alulírott ……. a Komlói Közös Önkormányzati Hivatal dolgozója nyilatkozom, hogy a hivatal biztonsági szabályairól és eljárásairól szóló képzésben részesültem.

A képzésen elhangzottakat tudomásul veszem, az informatikai biztonságpolitikában és más szabályzókban előírtakat a lehetséges biztonsági kockázat minimalizálása érdekében napi munkám során betartom.

Komló, ……..

……
aláírás

3.sz. melléklet

KOMLÓI KÖZÖS ÖNKORMÁNYZATI HIVATAL

INFORMATIKAI KARBANTARTÁSI NAPLÓ

Dátum	Eszközazonosító	Elvégzett munka	Aláírás

4. sz. melléklet

IGÉNYLŐLAP
Informatikai szolgáltatáshoz

Felhasználó neve: …….....

Beosztása: …….....

Munkavégzés helye: …….

Hozzáférés hálózati könyvtárakhoz: igen nem

Alkalmazás (ok) telepítése: igen nem

Alkalmazás (ok) neve: …….

…….

Internet hozzáférés: igen nem

E-mail cím: igen nem

Telefonkód: igen nem

Egyéb:

……
……
……
…….

Az igénylést engedélyező vezető neve: …….

Komló, ……

……..

aláírás

5.sz. melléklet

KOMLÓI KÖZÖS ÖNKORMÁNYZATI HIVATAL

SZERVERSZOBA BELÉPÉSI NAPLÓ

Belépés időpontja	Név	Elvégzett munka	Aláírás