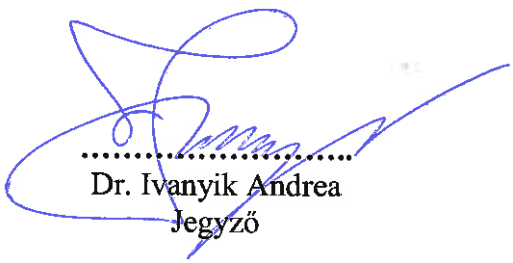
ETYEKI POLGÁRMESTERI HIVATAL

INFORMÁCIÓ BIZTONSÁGI POLITIKA
(IBP)

Jóváhagyom:



.....
Dr. Ivanyik Andrea
Jegyző

2018.06.11.

1 IBP Dokumentum karbantartás

Dokumentum változások története

Verzió	Dátum	Változások leírása	Módosította
1.0	2014.02.20.	1. verzió	Hallai Szabolcs CISA, CISM
1.1	2014.03.19.	Véglegesen kidolgozott 1. verzió	Hallai Szabolcs CISA, CISM
1.2	2018.06.11.	GDPR kapcsán felülvizsgált verzió	Hallai Szabolcs CISA, CISM

2 BEVEZETÉS, vezetői elkötelezettség

Az Etyeki Polgármesteri Hivatal (továbbiakban Hivatal) vezetésének szilárd meggyőződése, hogy az információ a Hivatal és az állampolgárok olyan vagyona, amelyet védeni kell a különböző fenyegetések ellen, a bizalmasság, a sértetlenség és a rendelkezésre állás, illetve az üzletmenet folytonosságának biztosítása érdekében. Ennek érdekében a Hivatal legfelső vezetése a mindenkori Informatikai Biztonsági Stratégiát szem előtt tartva a jelen Információ Biztonsági Politikában (a továbbiakban IBP) meghatározott egyetemleges alapelvek és belső biztonsági alapkövetelmények maradéktalan teljesítését várja el a vezetőségtől, valamennyi munkatársától, beszállítóitól és minden egyéb érdekelt féltől. A Hivatal informatikai biztonságpolitikája kivétel nélkül kiterjed a Hivatal által végzett valamennyi folyamatra és valamennyi szervezeti egységre. A legfelső vezetés biztosítja a teljesítéshez alapvetően szükséges erőforrásokat.

3 A politika célja

Az IBP a Hivatal vezetésének akaratnyilvánítása a szervezet informatikai rendszerei által kezelt információvagyon bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzésére és fenntartására irányuló intézkedések bevezetésére. Az IBP alapul szolgál továbbá a politikánál alacsonyabb szintű szabályozási eszközök, kialakítására és bevezetésére.

Az információ védelem megvalósítása érdekében tervezni és biztosítani kell azokat az anyagi feltételeket, amelyek lehetővé teszik a megfelelő színvonalú technika, valamint a speciális felkészültséget igénylő személyi feltételek megteremtését és folyamatos fenntartását.

4 ÁLTALÁNOS RENDELKEZÉSEK

4.1 Az IBP hatálya

4.1.1 Személyi hatály

Az IBP személyi hatálya kiterjed azon

a) a Hivatal minden munkatársára,

b) a Hivatal informatikai üzemeltetést végző, kiszervezett tevékenységeit ellátó külső partnereire,

c) a Hivatal informatikai üzemeltetést és/vagy fejlesztést végző egyéb szerződéses viszonyban tevékenykedő partnereire.

A jelen szabályzat személyi hatálya alá tartozóknak a politika célkitűzéseit ismerniük és követniük kell.

4.1.2 Tárgyi hatálya

Az IBP tárgyi hatálya kiterjed az Hivatal

a) adathordozóira,

b) alkalmazásaira,

c) alapszoftvereire,

d) hardver elemeire,

e) környezeti infrastruktúra elemeire,

f) objektumaira.

4.1.3 Területi hatálya

Az IBP területi hatálya kiterjed a tárgyi hatálya alá tartozó informatikai erőforrások üzemelési és használati helyszíneire:

a) a Hivatal telephelyére

b) mindenkori bérelt helyiségeire

c) kiszervezett adatfeldolgozási- és üzemeltetési tevékenységeinek külső helyszíneire

d) az otthoni használatra adott eszközökre.

4.2 Minősítése

Az IBP nyilvános dokumentum. Az IBP nyilvánosság számára történő elérhetőségét az Hivatal honlapján nyilvánosan elérhetővé teszi.

4.3 Elhelyezkedése, megfelelősége

Az IBP a szabályozási hierarchia (irányelvek – szabályozások – eljárásrendek – kézikönyvek) legfelsőbb szintjén helyezkedik el és ilyen módon hatással van a teljes szabályozási struktúrára. Ismerete és betartása minden munkatársra kötelező érvényű. Az Információ Biztonsági Politika, majd az erre épülő Informatikai Biztonsági Stratégia és Informatikai Biztonsági Szabályzat kibocsátása, az érintettek körében történő közzététele a Hivatal Jegyzőjének, karbantartatása és folyamatos felülvizsgáltatása az Informatikai biztonsági felelős feladata.
A jelen IBP-ben megfogalmazottak megfelelnek a hazai jogszabályoknak.

4.3.1 Felülvizsgálat

Az IBP-t két évente felül kell vizsgálni, a felülvizsgálat az Információ Biztonsági Felelős feladata.

4.3.2 Kommunikáció

Az IBP-t az Hivatal minden munkatársának ismernie kell, kiemelten azoknak, akik az Hivatal informatikai rendszerét használják és üzemeltetik. Ez utóbbi esetben az IBP megismerését és tudomásul vételét dokumentálni kell.

5 INFORMATIKAI BIZTONSÁGPOLITIKAI ALAPELVEK ÉS CÉLKITŰZÉSEK

A Hivatal az informatikai biztonság területén az alábbi alapelveket és védelmi célkitűzéseket kívánja következetesen érvényesíteni a jogszabályi követelményeknek és Felügyeleti elvárásoknak megfelelően.

5.1 Célkitűzések

Hitelesség biztosítása az Hivatal kezelésében lévő adatok tekintetében. Szükséges, hogy minden kétséget kizáróan megállapítható legyen a bekerülő adat forrása és az adat valóságnak való megfelelőssége, valamint annak biztosítása, hogy az előállítás után megőrzi ezen minőségét.

Bizalmasság biztosítása a Hivatal által kezelt adatokhoz való hozzáférés tekintetében. Érvényesülését elsősorban az informatikai rendszerben történő adathozzáférések és adatkezelés, valamint a Hivatal kommunikációja során kell biztosítani.

Sértetlenség biztosítása a Hivatal adatkezelése, adatfeldolgozása és kommunikációja során. A Hivatal által történő adatkezelés során követelmény, hogy pontos és a valóságnak mindenben megfelelő információk kerüljenek a rendszerben feldolgozásra, és ezen információk sértetlensége az adatkezelés során mindvégig biztosított legyen.

Rendelkezésre állás biztosítása a Hivatal által kezelt adatok tekintetében.
A feldolgozott információ tekintetében követelmény annak visszakereshetősége, melynek záloga az informatikai rendszerek funkcióinak és elérhetőségének folyamatos biztosítása.

5.2 Alapelvek

A védelem teljes körűségének alapelve – A teljes körűségre vonatkozó alapelvet a fizikai, a logikai és az adminisztratív védelem területén a következő három dimenzióban kell érvényesíteni:

a) az összes rendszerelemre,

b) a rendszerek architektúrájának minden rétegére, azaz mind a számítástechnikai infrastruktúra, mind az alkalmazások szintjén,

c) mind a központi, mind a végponti informatikai eszközökre és környezetükre.

A védelem zártságának alapelve – A zárt védelem akkor biztosított, ha az összes valószínűsíthető fenyegetés elleni megelőző védelmi intézkedések megvalósításra kerültek, és azok szerves egységet alkotnak.

A védelem kockázatarányosságának alapelve – A védelem mértéke és költségei a felmért kockázatokkal arányos legyen. Célkitűzés a minimális védelmi költséggel elért maximális védelmi képesség.

A védelem folytonosságának alapelve – Az informatikai rendszerek bevezetése során kialakított védelmi képességeket a rendszer teljes életciklusa alatt folytonosan biztosítani és fejleszteni kell.

A Hivatal kiemelt figyelmet fordít a személyes adatok védelmére, fenntartja és erősíti az adatok védelmét, minden rendelkezésére álló eszközzel gátolja az illetéktelen hozzáférést valamint a személyes adatok nyilvánosságra kerülését. Minden esetben biztosítja az érintettek AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (a továbbiakban: GDPR) szerinti jogait.

5.3 Kritikus sikertényezők

A Hivatal számára az információbiztonság sikeres megvalósítása során kritikus tényezők a következők:

- a biztonsági szabályozó környezet pontos meghatározása,
- a vezetőség elkötelezettsége;
- a biztonsági követelmények, a kockázatbecslés és a kockázatkezelés megértése és helyes alkalmazása;
- a biztonság hatékony menedzselése valamennyi vezető és alkalmazott felé;
- gondoskodás a kellő oktatásról és képzésről;
- átfogó, mindenre kiterjedő és kiegyensúlyozott mérési módszer alkalmazása az információ biztonságmenedzselés teljesítőképességének értékeléséhez és a helyesbítési javaslatok visszacsatolásához.

5.4 Kockázatalapú megközelítés

A Hivatal célul tűzte ki - a kockázatokkal arányos védelem biztosítása érdekében - kockázatelemzés rendszeres, belső szabályozás szerinti elvégzését a fenyegetések, a gyenge pontok, a nem elviselhető kockázatú tényezők meghatározására, valamint az ezek alapján kialakítandó védelmi intézkedésekre.

5.5 Szervezeti és felelősségi kérdések

Az IBP-ben lefektetett elvek kidolgozásának és betartatásának Hivatalon belül, minden esetben kell, hogy legyen felelőse: Információ Biztonsági Felelős - IBF. Az IBF közvetlen a Jegyzőhöz rendelt pozíció kell, hogy legyen. Az IBP elvek betartásának helyzetéről az IBF rendszeresen beszámol a Jegyzőnek, aki az információ biztonsági feladatok megvalósításának feltételeit biztosítja. Az IBP betartása minden munkatárs feladata és annak be nem tartása szigorú szankciókat von maga után.

A személyes adatok védelmének érdekében a Hivatal Adatvédelmi Tisztviselőt nevez ki, akinek feladata az adatkezelési műveletekhez fűződő kockázatok feltárása és a vezetőség informálása a feltárt kockázatokról. Emellett kezeli a személyes adatokkal kapcsolatos panaszokat, eseteket, felügyeli a Hivatalban a személyes adatok kezelését annak érdekében, hogy az adatkezelés a GDPR-ral való összhangban történjen.

5.6 Logikai biztonság

A logikai biztonság területén a Hivatal vezetésének célkitűzései az alábbiak:

- informatikai rendszerek védelmének megteremtése a jogosulatlan hozzáférésektől,
- az informatikai rendszerekhez és alkalmazásokhoz való hozzáférési jogok engedélyezésének hivatalos eljárások keretében történő szabályozása,
- információ, illetve adatvagyon megfelelő védelmi szintjének kialakítása, valamint az információ osztályozása,
- rosszindulatú szoftverek - számítógépvírusok, a hálózati férgek, a trójai falovak és a logikai bombák - elleni védekezés hatékony kialakítása, valamint az Internet használat és elektronikus

levelezés létesítése és üzemeltetése vonatkozásában megfelelő tűzfalas védelmet kialakítása a külső támadások, illetve a belső erőforrásokhoz történő jogtalan külső hozzáférések megakadályozása érdekében,

- biztonsági követelmények érvényesítése minden, a Hivatal külső informatikai adat-, vagy számítástechnikai kapcsolatában, az ennek kialakítására irányuló szerződésekben, vagy megállapodásokban,
- jogosulatlan tevékenységek észlelésének megteremtése,
- informatikai biztonság megteremtése a mobil számítástechnikai és a távmunka végzési eszközök használata esetén. A megkívánt biztonság legyen összemérhető azzal a kockázattal, amelyet az ilyen munkavégzési mód hordoz,
- rendkívüli események kezelésére történő felkészülés,
- alaptevékenységek megszakadásainak leküzdése, és a kritikus szolgálati folyamatok megvédése a nagyobb meghibásodások és a katasztrófák hatásaitól.

5.7 Fizikai és szervezeti biztonság, környezeti infrastruktúra

A fizikai és szervezeti biztonság, környezeti infrastruktúra területén a Hivatal vezetésének célkitűzései az alábbiak:

- a Hivatal objektumának, szervezetének biztonságának szavatolása,
- információ kezelését, feldolgozását végző helyiségek, valamint az egyes eszközök, az abban elhelyezett adattárolók és adathordozók fizikai védelmének biztosítása,
- papíros formában, valamint elektronikusan kezelt és tárolt információk, tárgyi eszközök, vagy szolgálatot teljesítő személyek védelmének biztosítása a különböző eseményektől, mint tűz, víz, áramellátás kimaradása, külső támadások, betörés,
- informatikai, vagy egyéb úton keletkezett adatok és információk kezelése során az előírt fizikai informatikai biztonsági követelmények betartásának elősegítése,
- személyi felelősségek egyértelmű meghatározása és elhatárolása.

5.8 Adminisztratív biztonság

Az adminisztrációs biztonság területén az Hivatal vezetésének célkitűzései az alábbiak:

- az Hivatal folyamatos, zavartalan és hatékony működését biztosító informatikai szabályozó környezet, illetve feltételrendszer megteremtése,
- teljes körű szabályozó környezet kialakítása, mely kiterjed a koncepciókra, szabályzatokra és eljárásrendekre.
- A Hivatal kiemelt figyelmet fordít a felhasznált szoftverek jogtisztaságára, mindent megtesz a jogtiszta szoftver használat érdekében és az illegális használat, illetve másolás ellen.

5.9 Információ Biztonsági incidensek kezelése

A Hivatal célul tűzte ki - a kockázatokkal arányos védelem biztosítása érdekében - kockázat elemzés alapján kialakított incidenskezelést.

5.10 Az információ biztonság ellenőrzése, fenntartása

Az IBP által megkövetelt információ biztonsági irányítási rendszer fenntartása alapvetően fontos stratégia cél. Ennek felelőse az IBF. Az IBF által elvégzendő távlati feladatokat az Informatikai Biztonsági Stratégia, az IBF rendszeres feladatait pedig az Informatikai Biztonsági Szabályzat (a továbbiakban: IBSZ) tartalmazza. A stratégiában elhatározott és az IBSZ-ben előírt feladatok végrehajtásához szükséges feltételek biztosításáért a Jegyző felel.

A Hivatal biztonságirányítási rendszerének fenntartásához elengedhetetlenül szükséges a munkatársak biztonságtudatosságának fejlesztése és fenntartása. Ennek érdekében kell végrehajtani a munkatársak évenkénti biztonsági oktatását.

5.11 Az IBP életciklusa

Az IBP rendszeres felülvizsgálata alapvető fontosságú elvárás, ezért kötelező évenként felülvizsgálni.

6 Az információ biztonság szintjei, defincíója

6.1 Az informatikai biztonság szintjei

Az informatikai biztonság szint besorolását a 2013. évi L törvény szerint kell alkalmazni. A Hivatal az információt megjelenésekor osztályozza, érzékenységi foka és kritikussága szerint, annak érdekében, hogy nyilvánvaló legyen a védettség szintje; így gondoskodik az információvagyon megfelelő védelmi szintjéről, beleértve a különleges kezelést igénylő információkat is;

7 Értelmező rendelkezések

Az IBP-ben használt fogalmak és definíciók értelmezését a 2013 évi L és a GDPR törvények fogalmai és definícióival azonosak.