INFORMÁCIÓBIZTONSÁGI POLITIKA

A **Debreceni Egyetem** (továbbiakban: Egyetem) vezetősége elkötelezett, hogy az Egyetem a működése és nyújtott szolgáltatásai területén a partnerei, ügyfelei és saját adatai védelmét, és az érdekelt felek információbiztonsági elvárásainak való folyamatos megfelelést meghatározó elemként kezeli. Az Egyetem által kezelt adatok és információk összessége kiemelt értéket képviselő vagyonelem, melyet védeni kell a különböző fenyegetések ellen, ezért az Egyetem törekszik, hogy e vagyonelemek tekintetében is időben állandóan megvalósuljon annak bizalmassága, sértetlensége, rendelkezésre állása.
Az Egyetem által nyújtott szolgáltatásokat magas színvonalon, modern és biztonságosan működő technológiával nyújtja, ahol felügyelt információbiztonsági folyamatokkal biztosítja a kezelt adatok, információk sértetlenségét, bizalmasságát és rendelkezésre állását.
Üzletmenet folytonosságának biztosítása és alapfeladatainak zavartalan ellátása érdekében minden szükséges információ- és adatvédelmi intézkedést megtesz, adatkezelési, információvédelmi folyamatait az adatvédelmi az információbiztonsági elvárásoknak megfelelően alakítja ki.
Az Egyetem működése és az általa nyújtott szolgáltatások teljesítése során elkötelezett a vonatkozó törvényi, valamint az irányadó szabványokban foglalt előírásoknak való maximális megfelelés iránt, így különösen az 41_2015. (VII. 15.) BM rendeletben meghatározott iránymutatásoknak való megfelelés iránt, azáltal, hogy magára nézve a hivatkozott törvényeket és szabványokat kötelezően alkalmazandónak ismeri el.
Az Egyetem vezetése az Információ Biztonsági Politikában (IBP) megfogalmazott elvek és követelmények teljesítését várja el az Egyetem összes munkatársától, beszállítóitól és minden egyéb érdekelt féltől. Az IBP hatálya kiterjed az Egyetem valamennyi folyamatára és szervezeti egységére, így különösen az Egyetem elektronikus információs rendszereire, mely magában foglalja az adathordozókat, alkalmazásokat, szoftvereket, hardver elemeket, a környezeti infrastruktúra elemeit és objektumait, a papír alapú dokumentumokat, továbbá minden eljárására, melyek hatással lehetnek az Egyetem adatvagyonára.
Az Egyetem információbiztonságának folyamatos magas színvonalú fenntartása érdekében az alábbi alapelvek figyelembe vételével információbiztonsági irányítási rendszert (IBIR) vezet be és üzemeltet.
Az IBIR célja, hogy biztosítsa az Egyetem kezelésében lévő adatvagyon bizalmasságát, sértetlenségét és rendelkezésre állását, valamint az elektronikus információs rendszerek elemeinek sértetlenségét és rendelkezésre állását veszélyeztető, mindenkori fenyegetések kockázataival arányos, zárt, teljes körű és folyamatos, a rendszerek telje életciklusára kiterjedő védelmét logikai, fizikai és adminisztratív védelmi intézkedések bevezetésével.

Az Egyetem az információ biztonság területén az alábbi alapelveket érvényesíti:

1. **Bizalmasság:** az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.
2. **Sértetlenség:** a tárolt adat tartalma és tulajdonságai az elvárttal

megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség), a származás ellenőrizhető, megállapitható (letagadhatatlanság), illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

3. **Rendelkezésre állás:** az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatók.
4. **A védelem teljeskörűsége:** az erre vonatkozó alapelvet a fizikai, a logikai és az adminisztrativ védelem területén a következő három dimenzióban kell érvényesíteni:
    a) az összes rendszerelemre;
    b) a rendszerek architektúrájának összes rétegére mind az informatikai infrastruktúra, mind az alkalmazások szintjén;
    c) a központi, illetve a végponti informatikai eszközökre és környezetükre.
5. **A védelem zártsága:** az összes valószínűsithető fenyegetés elleni megelőző védelmi intézkedés végrehajtása megtörténik, és azok összességükben szabályozott és szerves egészet alkotnak.
6. **A védelem kockázatarányossága:** a védelem mértéke és költségei a felmért kockázatokkal arányosak. Cél a szükséges és elégséges védelmi költséggel elért maximalis védelmi képesség.
7. **A védelem folyamatossága:** a kialakitott védelmi intézkedések az időben állandóan valtozó biztonsági környezet és viszonyok mellett is megszakítás nélkül fennállnak a rendszer teljes életciklusa alatt.

1 INFORMÁCIÓBIZTONSÁGI POLITIKA (IBP) SZEREPE

Az információbiztonság az Egyetem életében az informatika nélkülözhetetlenné válásával egyre határozottabban jelenik meg. Ma már nem az a kérdés kell-e, hanem hogy miként lehet a leggazdaságosabban megvalósítani, a leghatékonyabban működtetni.
Ez csak úgy lehetséges, ha az Információbiztonsági Politika:

a) Az első számú vezető elkötelezettségét élvezi és támogatja minden érintett vezető,
b) Az Egyetem egyéb terveivel összhangban, a többi biztonsági területtel (Vagyonbiztonság, Üzembiztonság) szinergiában valósítják meg és működtetik,

c) Ha kellőképpen kommunikált, oktatott,
d) Beépül a szervezet mindennapi életébe, a működési folyamatokba,
e) Része a szervezeti kultúrának, a dolgozók tudatos viselkedésének,
f) A biztonsági intézkedések, funkciók működése ellenőrzött és visszacsatolt, a hiányosságok szankcionáltak,
g) A szervezetben megfelelően képviselik az információ biztonság kérdését, van kijelölt szerepkör, szervezeti egység a menedzselésére.

2 INFORMÁCIÓBIZTONSÁGI POLITIKA CÉLJA

a) Az Egyetem informatikai rendszerei által kezelt információk hitelességének, sértetlenségének, rendelkezésre állásának, funkcionalitásának megőrzésére és fenntartására irányuló intézkedések bevezetése.
b) Az ügyfél, partneri, munkatársi, szerződéses, és egyéb üzleti információk bizalmasságának megőrzése, különös tekintettel az ügyfelek bizalmas adatainak biztonságos kezelésére.
c) Az ügyfeleknek biztosított szolgáltatások jól definiált és magas minőségű információbiztonságának folyamatos biztosítása.
d) Az alkalmazott támogató informatikai, illetve információtechnológiai rendszerek információbiztonságának, illetve információtechnológiai biztonságának fenntartása, beleértve a jogszabályi követelmények előírásainak megfelelő biztosítását is.
e) Az ügyfeleknek nyújtott szolgáltatások üzemeltetése és fejlesztése érdekében alkalmazott támogató folyamatokra, illetve információtechnológiai rendszerekre vonatkozó mindenkori jogszabályi és egyéb szabályozási követelményeknek való megfelelőség folyamatos biztosítása.

Az IBP célja, hogy irányelveket adjon a biztonságért felelős vezető 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.

2.1 A CÉLOK ELÉRÉSÉHEZ ÉS FENNTARTÁSÁHOZ ALAPVETŐ ESZKÖZNEK TEKINTJÜK:

a) A szervezeti, üzleti és szolgáltatás működés folyamatos fejlesztését, a korszerű technológiák bevezetését, és alkalmazását;
b) A szolgáltatások folyamatos fejlesztését a szabályozási követelmények, az ügyfelek és a piac igényei alapján;
c) Folyamatos továbbképzéssel a legmagasabb szakmai kompetencia vagy színvonal elérését;

d) A feladatok és megbízások elvégzéséhez szükséges erőforrások felmérését és biztosítását;
e) Megfelelő és megbízható beszállítók, alvállalkozók kiválasztását és alkalmazását, amelyek elfogadják és teljesítik az információbiztonsági követelményeket;
f) A munkavégzés során – törekvéseink ellenére is - bekövetkező hibák kijavítását;
g) A tevékenységekre vonatkozó szakmai, adat- és információvédelmi, és egyéb jogszabályi követelmények – és ezek változásainak – folyamatosan figyelemmel kísérését, és azok maradéktalan betartását;
h) A védendő ügyfél és saját információs-, illetve adatvagyon fenyegetettségének és azok biztonsági kockázatainak rendszeresen, legalább évente történő felülvizsgálatát és újraértékelését, majd ennek megfelelően az információvédelmi előírások és eljárások aktualizálását;
i) A szolgáltatások feltételeinek folyamatos biztosításához a következő – kiemelkedő kockázatúnak értékelt – incidens kategóriák elfogadhatatlannak tartását és legnagyobb veszélynek értékelését:
    - az ügyfelek adatainak beleegyezés nélküli nyilvánosságra kerülése;
    - adatvesztések, amelyek mentésekből nem állíthatók vissza;
    - hálózati betörés a támogató és szolgáltató informatikai, információtechnológiai rendszerekbe.