

A Magyar Telekom Csoport
Információ biztonsági irányelvei

1. Bevezetés

Jelen Információ Biztonsági Irányelv (továbbiakban: IBI) magas szintű alapelveket fogalmaz meg. Ezek az alapelvek irányadók abban az esetben, ha egy adott területre nem vonatkozik szabályozás, vagy az ellentmond jelen IBI-nek. Az IBI-ben nem érintett kérdésekben az ISO/IEC 27000-es szabványcsalád elveit kell alkalmazni.

1.1. Az IBI célja, szerepe

Az IBI célja felsőszintű iránymutatás és támogatás nyújtása az információvédelemhez az üzleti követelményekkel, az ISO/IEC 27001 szabvánnyal, és a vonatkozó jogszabályokkal összhangban.

1.2. Az IBI hatálya

Az IBI hatálya kiterjed a Magyar Telekom Csoport (továbbiakban Csoport) valamennyi munkavállalójára, tisztségviselőjére, a Csoporttal üzleti kapcsolatba kerülő természetes és jogi személyekre (külső partnerekre). Az IBI vonatkozik minden a Csoport működésével összefüggésben kezelt információra, annak megjelenési módjától (adathordozó, adatrögzítés módja, eszköze) függetlenül és az ezeket kezelő és védő informatikai és nem informatikai eszközökre és rendszerekre.

2. Elkötelezettségi nyilatkozat

A Csoport és tagvállalatai vezetése elkötelezett az információ biztonság üzleti céloknak és jogszabályi környezetnek megfelelő szinten tartása iránt. Ezt a vezetést jelen IBI kiadásával ismeri el.

3. Az információ biztonság szerepe és alapelvei

3.1. Az információ biztonság szerepe

A Csoport és tagvállalatai információbiztonsági intézkedései azt a célt szolgálják, hogy a Csoport – ismert és elfogadható kockázatok mellett – eredményes és hatékony legyen az üzleti céljai elérésében. A szabályozások meg kell, hogy feleljenek a vonatkozó magyar és nemzetközi törvényi, jogszabályi és hatósági környezetnek.

3.2. Az információvédelem alapelvei

Az információkat bizalmasság, integritás és rendelkezésre állás szempontjából kell védeni, egyértelmű, az üzleti célokkal összhangban lévő besorolási elvek alapján.

Az **információ** fogalma nem kizárólag az informatikai rendszerekben kezelt adatokat takarja, hanem többek között az eltávolítható adathordozókat, írott- vagy hanganyagokat, képeket, videókat és élőszóban közölt információkat is. Az információkhoz való **hozzáférés** alatt mind az informatikai, mind a fizikai hozzáférés értendő.

Az információvédelmi intézkedések kidolgozásakor a legjobb gyakorlat (best practice) és az elvárható gondosság alapelvét kell szem előtt tartani.

3.3. Információvédelmi intézkedések irányelvei

3.3.1. Vezetők elkötelezettsége

A vezetés elkötelezett az információbiztonság iránt és a védelmi intézkedések betartásával pozitív példát kell mutasson a munkatársaknak.

3.3.2. Tudatosság, titoktartás

Az információbiztonsági előírások tudatos betartása, a kötelező titoktartás nemcsak a belső munkatársak alapvető felelőssége, hanem kiterjed a külső partnerekre is. A munkatársak körében rendszeres oktatásokkal, képzésekkel és az elsajátított ismeretek számonkérésével kell elérni az információbiztonsági tudatosságot.

3.3.3. Szankcionálás

Az információbiztonsági szabályok megsértése visszatartó erejű szankciókat von maga után. A kivizsgálás és a szankcionálás ne ütközzön a vonatkozó törvényi (Mtk., Ptk., Btk.) előírásokba.

3.3.4. Információ védelem szervezeti keretei, felelősségi és hatáskörök

Az információbiztonság irányítási rendszer a minőségirányítási rendszerrel integráltan működik. Szakmai irányítását az MT Csoport Információ biztonsági vezető látja el. Meg kell határozni az információvédelmi felelősségeket és hatásköröket, ideértve a felhasználói felelősségeket, a hatóságokkal és szakmai érdekcsoportokkal való kapcsolattartást is.

3.3.5. Információk osztályba sorolása

A Csoport által kezelt információkat és az információ kezelő rendszereket az üzleti követelmények alapján, a törvényi és jogszabályi követelmények figyelembe vételével, egyértelmű útmutatás szerint kell védelmi osztályokba sorolni.

3.3.6. Munkatársakkal kapcsolatos biztonsági követelmények

Minden pozícióhoz átvilágítási követelményeket kell megfogalmazni, amelyeket a kiválasztási folyamatban és a munkaviszony során is alkalmazni kell. A felvételt követően mihamarabb el kell végezni a biztonsági követelmények tudatosítását. Az információ kezelési jogosultságokat a mindenkori munkakörrel összhangban kell tartani, a munkaviszony megszűnése esetén pedig vissza kell vonni.

3.3.7. Fizikai biztonság követelményei

A fizikai biztonsági intézkedéseket legalább az érintett információk és információkezelő rendszerek osztályával legyenek összhangban. Definiálni kell a fizikai biztonsági zónákat. Védeni kell az infrastruktúrát, a telephelyen kívüli információ kommunikációs eszközöket és munkahelyeket (pl. távmunkahelyek) is.

3.3.8. Hálózatok védelme

A belső hálózathoz való belső csatlakozási pontokat fizikailag védett zónákon belül kell elhelyezni. A fokozott biztonsági osztályba sorolt rendszereket, különálló, tűzfalal védett alhálózatban kell működtetni. A belső hálózathoz való külső csatlakozás csak kétfaktoros, erős azonosítás után lehetséges.

Ellenőrzés alatt kell tartani a belső hálózatról a külső hálózatra való csatlakozást. Szabályozni kell a vezeték nélküli eszközök és hálózatok (pl.: WLAN, GPRS) használatát, a belső hálózathoz való csatlakoztatását.

3.3.9. Jogosultság kezelés, hozzáférés menedzsment

A jogosultságokat dokumentált kérelem alapján a jogok központi menedzsmentjét és a számon kérhetőséget biztosítva kell megadni.

A rendszerekhez való hozzáféréseket a munkavégzéshez feltétlenül szükséges mértékben kell biztosítani. A kiadott és érvényben lévő jogosultságokat rendszeresen felül kell vizsgálni.

3.3.10. Adattárolás és továbbítás

Az információk osztályának megfelelően kell szabályozni az információk és adathordozók tárolását, kezelését, továbbítását. Az üzletileg védendő információkat lehetőleg központi helyen tároljuk.

3.3.11. Üzemeltetés biztonsági követelményei

Az információkezelő és védelmi rendszerek üzemeltetését a rendszerek besorolásának megfelelő írásos szabályozások alapján kell végezni. Ezek térjenek ki a rendszeres üzemeltetési feladatokra, mentésre, a használat monitorozására, fizika hozzáférésre is. Az üzemeltetésnek biztosítania kell a rendszerrel szemben megkövetelt rendelkezésre állást is.

3.3.12. Felhasználói eszközök (pl. kliensek, mobil eszközök) biztonsági követelményei

A felhasználói eszközöket is osztályba kell sorolni és meg kell határozni a megfelelő védelmi eszközöket, biztonsági beállításokat és használatuk alapvető szabályait. Ezen védelmi eszközök és beállítások használatára kötelezni kell a munkatársakat. Az információkezelő eszközökért, a rajta tárolt információkért a felhasználó felelős.

3.3.13. Biztonsági követelmények a rendszerek fejlesztése, változtatása során

A rendszerek fejlesztése, változtatása során a biztonsági követelmények meghatározásakor az előre látható igényeket is figyelembe kell venni. Új rendszerek esetén a várható besorolással összhangban álló biztonsági követelményeket be kell építeni a specifikációba. Rendszert kizárólag megfelelő tesztelések után lehet használatba venni. Éles üzembe állítás vagy módosítás során a változás menedzsment előírásai szerint kell nyilvántartani és azonosítani az aktuális verziót és konfigurációt.

3.3.14. Külső felekkel való együttműködés információ biztonsági irányelvei

A szabályozásokban megjelenő információbiztonsági követelményeknek a külső felekre ugyanúgy vonatkoznuk kell, mint a Csoport munkatársaira. A külső felekkel kötött szerződésekben rögzíteni kell ezen szabályozásoknak való megfelelést, illetve az esetleges eltéréseket is. Ellenőrizni kell a külső felek szolgáltatásainak teljesítését, a rájuk vonatkozó (szerződéses) információvédelmi előírások betartását.

3.3.15. Folyamatos működés biztosítása

A folyamatos működést az üzleti követelményekkel összhangban, költséghatékony módon szükséges biztosítani. A rendszer működésében előforduló zavarok hatásának csökkentése előre tervezett módon történjen. A tervezett intézkedések végrehajtását az üzleti kockázatoknak megfelelő rendszerességgel tesztelni kell.

3.3.16. Információbiztonsági események kezelése

Az információbiztonsági események kezelésére írásos szabályozást kell készíteni. Minden eseményhez legyen előre meghatározott specifikus intézkedés, vagy legyen hozzárendelve a megfelelő intézkedést meghatározni és elrendelni képes felelős személy. Új helyesbítő tevékenység meghatározása esetén azt be kell építeni a meglévő védelmi intézkedések rendszerébe.

3.3.17. Ellenőrzés, megfelelés igazolása

A biztonsági intézkedések betartását független auditokkal és/vagy belső ellenőrzésekkel kell vizsgálni. Az ellenőrzéseknek ki kell terjedni az információ védelmi szabályozások megfelelőségének, betartásának és működésének vizsgálatára, valamint az információkezelő és információvédelmi rendszerek műszaki megfelelőségének igazolására. Az ellenőrzések során az üzleti, működési, szolgáltatási folyamatok csak elfogadható mértékben korlátozhatóak, az információk nem károsodhatnak.