IT Biztonsági és Adatvédelmi Incidenskezelési Szabályzat

Hatályos: 2018. május 25-től visszavonásig

1. A SZABÁLYZAT célja és hatálya

Jelen szabályzatban használt fogalmak a Dunanett Nonprofit Kft. Adatvédelmi Szabályzatában kerültek meghatározásra.
A jelen IT biztonsági és Adatvédelmi Incidenskezelés Szabályzat (a továbbiakban: Szabályzat) célja, hogy **az Európai Parlament és a Tanács 2016/679 számú rendeletének (továbbiakban: GDPR) 32. - 34. cikk alapján** a Társaság üzleti folyamataihoz kapcsolódó IT biztonsági és adatvédelmi incidensek fajtáinak összefoglalása, a kapcsolódó felelősségi körök meghatározása, valamint az egyes speciális incidensfajták mint pl. az adatvédelmi incidensek alapvető kezelési módjainak meghatározása és következményeinek minimalizálása valamint jogszabályi kötelezettségeknek való megfelelés.

A Szabályzat alanyi hatálya a Társaság valamennyi munkavállalójára vonatkozik.

A Szabályzat utasítás tárgyi hatálya a Társaság valamennyi működő információs vagyonára, adatvagyonára és IT eljárásra kiterjed.

2. Értelmezések, definiciók

A GDPR 4. cikk 12. pontja alapján„adatvédelmi incidens”: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

Esemény	IT rendszerben észlelt olyan esemény, amely eltér a normális működéstől. Esemény lehet e-mailben érkezett káros kód is, külső támadás, vagy adatvesztés, illetve adathalászat.
IT Biztonsági Incidens	Jelen szabályzat hatálya alatt IT biztonsági Incidensnek minősül minden olyan cselekedet vagy esemény, amely Eseménynek minősül. Így különösen Eseménynek tekinthető, ha a Társaság informatikai eszközei vagy információs vagyona, illetve adatvagyona megsérül, elveszik, azokkal visszaélést követnek el, információ illetve adat szivárgott ki, vagy ezen események bekövetkezhettek volna.
IT Incidens Manager	Kritikus (kiemelt és magas) és közepes incidensek során a Társaság egyes területeinek jelzéseit fogadó, illetve azok kezelését irányító, összefogó munkatárs, aki az incidens kezelése érdekében korlátlanul rendelkezik az IT technikai, technológiai és humán erőforrásai felett.
Adatvédelmi Incidens	Az Adatvédelmi Szabályzatban meghatározott olyan esemény, amely során Személyes Adatok nem az Adatkezelési Szabályzatban meghatározott módon kerülnek kezelésre, vagy felhasználásra továbbá, ha Személyes Adatok bármilyen módon illetéktelen személyek birtokába kerülnek.

Az Adatvédelmi incidenst a továbbiakban jelen szabályzatban IT Biztonsági Incidensnek tekintjük.

3. Szerepek és felelősségek

Szerepek:	Felelősségek:
Felhasználó	Az a személy, aki feladatai teljesítése közben az üzleti folyamatokat működteti, azokban résztvevőként szerepel, IT rendszer, alkalmazás felhasználója. A tudomására jutott ténylegesen bekövetkezett vagy feltételezett eseményeket (IT biztonsági incidensek) azonnal jelzi a közvetlen munkahelyi vezetőnek. Részt vesz az incidens kivizsgálásában, adatot szolgáltat az Incidens Menedzser koordinálása mellett.
Incidens Menedzser	Koordinálja az IT biztonsági incidensek kezelését. Egyezteti és elrendeli a bizonyítékok gyűjtését, kezelését. Részt vesz a szükséges teendők, intézkedések, rendkívüli intézkedések meghatározásában. Tájékoztatást nyújt a vezetői részére. Továbbá az információkkal és adatokkal kapcsolatos IT biztonsági beállításokat és a szabályzatok betartását rendszeresen ellenőrzi, az IT biztonsági incidenseket kivizsgálja. Bizonyítékot gyűjt, kezeli azokat az IT biztonsági incidens kivizsgálásához kapcsolódóan. Meghatározza azokat az IT biztonsági lépéseket, amelyek a későbbiekben a hasonló IT biztonsági incidensek hosszú távú megelőzését lehetővé teszik, illetve ha szükséges kiváltják az érvényben lévő rendkívüli intézkedéseket (Utólagos vizsgálat). Nyilvántartást vezet minden IT biztonsági incidensről;
Rendszergazda	Egy alkalmazás, alkalmazáscsoport, infrastruktúra eszköz, vagy eszközcsoport műszaki üzemeltetésért felelős alkalmazott, vagy a Társasággal szerződéses jogviszonyban álló jogi személy alkalmazottja.
IT vezető	Felelős a helyreállítás megfelelő lebonyolításáért Rendkívüli intézkedések meghozatalában való részvétel Kapcsolódó döntések meghozatala

4. IT Biztonsági incidensek

4.1. IT Biztonsági incidensek észlelése

Az IT rendszerek normálistól eltérő működésének jelentése minden munkatárs feladata. IT biztonsági eseményeket a Felhasználó, az Incidens Manager vagy a Rendszergazda is észlelhet a működtetett IT biztonsági infrastruktúra (pl.: naplóelemző, sérülékenység vizsgáló, behatolás figyelő vagy adatszivárgás megelőző rendszer), valamint az ezen infrastruktúrák jelentéseit kezelő rendszerekből és vizsgálatokból.

Az eseményeket az Incidens Managernek kell jelenteni telefonon, vagy e-mailban.

Amennyiben az észlelt esemény helyszíni vizsgálatot igényel (pl.: ismeretlen eszköz hálózati végpontra csatlakoztatva), úgy az észlelő munkatárs köteles biztosítani a helyszínt, megelőzni az esetleges további károkat és köteles gondoskodni a bizonyítékok megőrzéséről. Tevékenységét az Incidens Menedzser koordinálja.

Laptop vagy mobiltelefon lopás, illetve munkahelyre történő betörés esetén a lopást/betörést kell haladéktalanul az esemény bekövetkezte után a Társaság vezetőjének bejelenteni.

4.2. IT Biztonsági incidens besorolása

Az Eseményt az Incidens Manager minősítheti IT biztonsági incidenssé.

IT Biztonsági incidenssé kell minősíteni minden olyan eseményt, IT incidenst, amely többek között, de nem korlátozva a felsoroltakra:

- lehetővé tehet jogosultsággal visszaélést,
- adatok illetéktelen hozzáférését különös tekintettel Személyes Adatokra vagy
- szolgáltatás-megtagadás támadás (DOS) kivitelezését.

Az incidens besorolásánál figyelembe kell venni:

- incidens kategóriája (külső vagy belső, támadás, visszaélés)
- incidens érintett rendszerek köre (néhány felhasználó, érintett rendszerek)
- incidens elhárítása (beavatkozás lépéseinek meghatározása).
- az incidens során történt-e Személyes Adatokkal visszaélés (adatvédelmi incidens)

Az IT biztonsági incidensek priorizálása a vezetővel történő egyeztetés alapján történik.

Az IT biztonsági események besorolásánál figyelembe kell venni azok okait is. Az IT biztonsági események / incidensek bekövetkezése lehet szándékos vagy véletlen:

- alkalmazottak vagy a vállalaton kívül álló személyek cselekedeteinek hatására
- informatikai eszközökben, hálózatokban és rendszerekben rejlő hiányosságok miatt.

4.3. AZ IT biztonsági incidensek kivizsgálása

Az IT biztonsági incidensekkel kapcsolatos vizsgálatokat az Incidens Menedzser végzi. A vizsgálat információit és eredményeit bizalmas adatként kell kezelni. Amennyiben az incidens Személyes Adatokat is érint, akkor ha az Adatvédelmi Szabályzatban meghatározottak szerint fennállnak a feltételek, akkor az incidenst be kell jelenteni a NAIH-nak.

Az IT biztonsági incidensek kivizsgálása esetén a következő területeket kell vizsgálni és jegyzőkönyvben rögzíteni:

- az IT biztonsági incidens típusa, súlyossága, következményei (Mi történt? Mik a következmények?)
- az incidens bekövetkezésének közvetett és közvetlen okai (Miért történt?)
- az incidens bekövetkezésének körülményei (Hogyan történt?)
- a további károk keletkezésének megakadályozása és kezdeti felszámolásuk megkönnyítése érdekében szükséges teendők
- hasonló IT biztonsági incidensek bekövetkezésének hosszabb távú megelőzése érdekében szükséges intézkedések
- az esetleges felelősök, illetve a személyi felelősségre vonás szükségességének meghatározása

Technológiai jellegű incidensek esetén a kapcsolódó rendszerek log file elemzését is el kell végezni. A vizsgálat folyamán olyan hiteles információk és bizonyítékok begyűjtésére van szükség, amelyek:

- lehetővé teszik a belső problémaelemzést;
- szerződésszegéssel, vagy jogszabálysértéssel kapcsolatos eljárásokban bizonyítékként felhasználhatók;
- az informatikai eszközök, szoftverek beszállítóival, külső szolgáltatókkal folytatott kártérítési tárgyalásokban felhasználhatók;
- adatvédelmi, vagy számítógéppel elkövetett visszaélésekről szóló jogszabályok hatálya alá eső jogi eljárásban bizonyítékként felhasználhatók.

Az elemzés, értékelés, a jelentések elkészítése, a dokumentációk lezárás valamint az incidens hivatalos kommunikálása az Incidens Menedzser feladata.

Amennyiben a további károk megelőzése a Társaság üzleti folyamatainak részleges vagy teljes leállásával, illetve szüneteltetésével jár, az intézkedést csak a Társaság vezetője jóváhagyásával lehet megtenni.

4.4. IT Biztonsági Incidensek következményeinek a felszámolása

Az IT felelős munkavállalójának vagy külsős megbízottnak a feladata minimalizálni az incidens hatását, amennyiben lehetséges, biztosítani a reprodukálhatóságot, valamint megkezdeni a helyreállítást.

Az Incidens Manager felelős az észlelés, illetve a további események jegyzőkönyvbe foglalásáért. Az Incidens Manager a vizsgálat alapján meghatározza az elvárt intézkedéseket, az intézkedések mellé elsődleges kockázatbecslést ad, továbbá koordinálja az incidens megszüntetésének lépéseit.

A következmények felszámolása során törekedni kell arra, hogy az incidens hatása minimalizálható legyen illetve, hogy a helyreállítási folyamat reprodukálhatósága biztosítható legyen.

A következmények felszámolása után az incidens ismételt bekövetkezését meg kell akadályozni.

4.5. IT Biztonsági incidensek utáni felelősségre vonás

Az IT bztonsági jelentés kiértékelése után, amennyiben közvetlen személyes felelősség megállapítható, az ügyvezető dönt a felelősségre vonásról. Amennyiben az incidens büntetőjogi következményekkel jár, a Magyarországi törvényeket kell figyelembe venni.

4.6. IT Biztonsági incidensek utólagos elemzése

Az IT biztonsági incidensek megoldása után az Incidens Manager, a Rendszergazda a szükséges további személyek részvételével Incidenskezelő csoportot alkot. Az elemzés fő feladata meghatározni azokat az IT biztonsági lépéseket, amelyek a későbbiekben a hasonló IT biztonsági incidensek hosszú távú megelőzését lehetővé teszik, illetve ha szükséges kiváltják az érvényben lévő rendkívüli intézkedéseket.

A csoport javaslatot készít az ügyvezető részére a végrehajtandó változásokról.

4.7. IT Biztonsági incidensek dokumentációi

Az IT biztonsági incidensek kivizsgálásáról, a vizsgálat eredményéről minden esetben **IT biztonsági Incidens Jegyzőkönyvet** kell készíteni, és ezt a dokumentumot az IT biztonsági incidensek nyilvántartásában kell őrizni. Minden IT biztonsági Incidens jegyzőkönyv szigorúan bizalmas minősítésű dokumentum, és ennek megfelelően kell kezelni.

4.7.1. AZ IT biztonsági Incidens jegyzőkönyv tartalma:

A biztonsági incidens észlelésével kapcsolatos információtartalom:
- bekövetkezés ideje
- az incidens típusa
- ki és mikor jelentette az incidens észlelését
- kit és mikor értesítettek az incidensről
- kinek és mikor továbbították az incidens tényét (illetve annak kezelését)
- Személyes Adatok érintettek-e

Az incidens kivizsgálásával kapcsolatos információtartalom
- a vizsgálat során végrehajtott műveletek, cselekedetek részletei
- a végrehajtók személye
- a végrehajtás ideje
- valamint az eredmények.

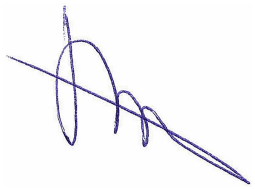
4.7.2. IT Biztonsági incidensek nyilvántartása

Az IT biztonsági incidenseket az Incidens Manager tartja nyilván a jelen szabályzatban meghatározott információk megadásával. Az incidensre vonatkozó dokumentumokat 5 évig kell megőrízni.

4.8. Tájékoztatás

Az IT Biztonsági incidensekről, illetve azok kezelésének módjáról az Incidens Manager tájékoztatást nyújt az érintett munkavállalóknak valamint a Társaság vezetőjének, a partnerek vagy ügyfelek adatait, információit, illetve Személyes Adatokat érintő súlyos IT biztonsági incidens esetén a tájékoztatásnak haladéktalanul meg kell történnie, annak érdekében, hogy a Társaság vezetője dönteni tudjon, hogy az adott Személyes Adatokat is érintő IT Incidenst be kell-e jelenteni – 72 órán belül – a NAIH-hoz. A bejelentés az ügyvezető által kijelölt személy feladata.

Mezőfalva, 2018. május 25.



Simon Zsolt
ügyvezető