| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Ide írja be a bejegyzett jogi személy nevét | | | | | | | |
| Dokumentumszám:<br>P30S | | | | | Dokumentum címe:<br>**Incidenskezelési szabályzat** | | | | | | | |
| Verzió:<br>1.0 | | Hatálybalépés dátuma:<br>01.01.2025 | | | A dokumentum tulajdonosa: | | | | | | | |
| X | Szabályzat | | Szabvány | | Eljárás | | Űrlap | | Nyilvántartás | | Egyéb | |

| **Felülvizsgálati előzmények** | | | | |
|---|---|---|---|---|
| **Felülvizsgálat száma** | **Felülvizsgálat dátuma** | **Változások** | **Felülvizsgálta** | **A folyamat tulajdonosa** |
| | | | | |
| | | | | |

| **Jóváhagyások** | | | |
|---|---|---|---|
| **Név** | **Beosztás** | **Dátum** | **Aláírás** |
| | | | |
| | | | |

Vonatkozó szabványokkal és jogszabályokkal összhangban

| Szabvány/jogszabály | Pont/cikk | Megjegyzés |
|---|---|---|
| ISO/IEC 27001:2022 | 6.1, 6.3, 8. pont | incidenskezelés, folyamatos fejlesztés, működési kontrollok |
| ISO/IEC 27002:2022 | 5.24, 5.25 kontroll | incidensészlelés, felkészültség, tanulás |
| NIST SP 800-53 Rev.5 | IR-4, IR-5, IR-6 | incidenskezelés és nyomon követés, jelentéstétel |
| GDPR | 33. cikk | incidensbejelentési követelmények |
| NIS2 irányelv | 23. cikk | kötelező kiberbiztonsági incidensjelentés |
| DORA-rendelet | 17. cikk | IKT-incidenskezelés |
| COBIT 2019 | DSS02, DSS04 | szolgáltatás- és incidenskezelés, valamint üzletmenet-folytonosság |

**1. Cél**

1.1. Jelen szabályzat meghatározza, hogy a szervezet miként észleli, jelenti és kezeli a digitális rendszereit, adatait vagy szolgáltatásait érintő biztonsági incidenseket.

1.2. A szabályzat támogatja a károk minimalizálását, az ügyféladatok védelmét, valamint a jogszabályi kötelezettségek teljesítését, ideértve a GDPR szerinti 72 órás incidensbejelentési kötelezettséget is.

1.3. A szabályzat egyértelmű felelősségi köröket, kommunikációs lépéseket és incidens utáni teendőket határoz meg, dedikált biztonsági csapattal nem rendelkező kisebb szervezetek esetén is.

**2. Hatály**

**2.1. Jelen szabályzat az alábbiakra terjed ki:**

2.1.1. valamennyi munkavállalóra, vállalkozóra és külső IT-szolgáltatóra

2.1.2. valamennyi, a vállalat által kezelt rendszerre és szolgáltatásra, beleértve a weboldalakat, felhőplatformokat, mobileszközöket, laptopokat és e-mail-fiókokat

**2.1.3. valamennyi incidenstípusra, ideértve különösen az alábbiakat:**

2.1.3.1. adatokhoz vagy rendszerekhez történő jogosulatlan hozzáférés

2.1.3.2. malware- vagy zsarolóvírus-fertőzés

2.1.3.3. adathalászati vagy szociális manipulációs kísérletek

2.1.3.4. kibertámadásból vagy nem megfelelő használatból eredő rendszerleállások

2.1.3.5. érzékeny információk véletlen közzététele vagy törlése

2.1.3.6. üzleti célú eszközök vagy adattároló adathordozók elvesztése vagy eltulajdonítása

**3. Célkitűzések**

3.1. Egyértelmű folyamat kialakítása a biztonsági incidensek felismerésére és eszkalációjára.

3.2. Annak biztosítása, hogy az incidensek jelentése, naplózása és kezelése előre meghatározott határidőkön belül történjen.

3.3. A károk gyors elhatárolásának, az adatok helyreállításának és a szolgáltatások helyreállításának biztosítása.

3.4. Annak biztosítása, hogy az érintett felek (pl. ügyfelek, szabályozó hatóságok) értesítése jogszabályi kötelezettség esetén megtörténjen.

3.5. Az ismételt előfordulás megelőzése gyökérokelemzéssel, helyesbítő intézkedésekkel és a szabályzat fejlesztésével.

3.6. Annak támogatása, hogy a KKV megfeleljen az ISO 27001 tanúsítási követelményeknek, és audit során igazolni tudja az elszámoltathatóságot.

**4. Szerepkörök és felelősségek**

**4.1. ügyvezető**

4.1.1. A szabályzat tulajdonosa, és felel annak végrehajtásáért.

4.1.2. Felügyeli az incidenskezelési tevékenységeket, és jóváhagyja a szabályozó hatóságok vagy ügyfelek felé történő értesítéseket.

4.1.3. Felülvizsgálja az incidens utáni jelentéseket, és biztosítja, hogy szükség esetén sor kerüljön a szabályzat frissítésére.

4.1.4. A koordinációs feladatokat delegálhatja, de az elszámoltathatóságot megtartja.

**4.2. IT-szolgáltató / rendszergazda (belső vagy külső)**

4.2.1. Észleli és kivizsgálja a lehetséges biztonsági incidenseket.

4.2.2. Végrehajtja az elhatárolási és helyreállítási intézkedéseket (pl. hozzáférés letiltása, biztonsági mentésekből történő helyreállítás).

4.2.3. Valamennyi megerősített vagy feltételezett incidensről az észleléstől számított 1 órán belül értesíti az ügyvezetőt.

4.2.4. Incidensnaplót vezet időbélyegekkel, hatásvizsgálattal és a megtett intézkedésekkel.

[ ... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ... ]

**9. Felülvizsgálati és frissítési követelmények**

**9.1. Ütemezett felülvizsgálat**

**9.1.1. Jelen szabályzatot az ügyvezetőnek legalább 12 havonta felül kell vizsgálnia annak biztosítására, hogy:**

9.1.1.1. összhangban legyen az ISO/IEC 27001:2022 kontrolljaival

9.1.1.2. reagáljon az új fenyegetésekre, kockázatokra és incidensekre

9.1.1.3. továbbra is megfeleljen a jogi és szerződéses kötelezettségeknek (pl. GDPR, DORA)

**9.2. Kiváltó események**

**9.2.1. A szabályzatot az alábbi esetekben is felül kell vizsgálni, és szükség szerint frissíteni kell:**

9.2.1.1. bármely magas súlyosságú incidens vagy szabályozó hatósági értesítés után

9.2.1.2. új IT-infrastruktúra bevezetése vagy rendszerváltozások esetén

9.2.1.3. a biztonsági incidensekre vonatkozó jogszabályi követelmények módosulása esetén

**9.3. A felülvizsgálat dokumentálása és terjesztése**

9.3.1. Valamennyi felülvizsgálatot és módosítást a szabályzat változásnaplójában kell dokumentálni.

9.3.2. A frissített verziókat meg kell küldeni minden olyan munkavállalónak, beszállítónak és IT-szolgáltatónak, aki biztonsági vagy rendszerüzemeltetési tevékenységben érintett.

9.3.3. A munkatársi tudatosság bizonyítékait (pl. értekezleti jegyzőkönyvek vagy e-mailes visszaigazolások) az auditra való felkészültség érdekében meg kell őrizni.

**10. Kapcsolódó szabályzatok és összefüggések**

**10.1. Jelen szabályzatot az alábbi KKV-szabályzatokkal összehangoltan kell alkalmazni:**

10.1.1. P1S – Információbiztonsági szabályzat: Meghatározza a bizalmasság, sértetlenség és rendelkezésre állás működés közbeni fenntartására vonatkozó általános elvárásokat, beleértve az incidenskezelést is.

10.1.2. P2S – Irányítási szerepkörök és felelősségek szabályzata: Meghatározza az incidensek észlelésére, jelentésére és eszkalációjára vonatkozó hatásköröket és elszámoltathatósági struktúrákat.

10.1.3. P4S – Hozzáférés-szabályozási szabályzat: Lehetővé teszi a hozzáférési jogosultságok azonnali visszavonását az incidenskezelési intézkedések során.

10.1.4. P8S – Információbiztonsági tudatossági és képzési szabályzat: Biztosítja, hogy valamennyi munkavállaló képes legyen a biztonsági incidensek hatékony azonosítására és jelentésére.

10.1.5. P17S – Adatvédelmi és magánszféra-védelmi szabályzat: Iránymutatást ad a GDPR szerinti jogi incidensbejelentési eljárásokhoz, és támogatja a jogszabályi megfelelést incidensek esetén.

10.1.6. P22S – Naplózási és felügyeleti szabályzat: Biztosítja a biztonsági események észleléséhez, elemzéséhez és auditálásához szükséges eszközöket és láthatóságot.

10.1.7. P31S – Bizonyítékgyűjtési és forenzikai szabályzat: Támogatja az incidensekkel kapcsolatos intézkedések kivizsgálását és jogi védhetőségét a bizonyítékok megfelelő kezelésére vonatkozó előírásokkal.

10.2. Ezek a szabályzatok együttesen alkotják a KKV információbiztonsági incidensek észlelésére, kezelésére és helyreállítására vonatkozó működési keretrendszerét.

## 11. Hivatkozott szabványok és keretrendszerek

### 11.1. ISO/IEC 27001

11.1.1. 6.1. pont – előírja a kockázatkezelés tervezését, beleértve az incidensekre való felkészülést is.

11.1.2. 6.3. pont – támogatja a folyamatos fejlesztést a biztonsági eseményekből levont tanulságok alapján.

11.1.3. 8.1. pont – hangsúlyozza a működési kontrollok szerepét az incidensek és zavarok kezelésében.

### 11.2. ISO/IEC 27002

11.2.1. 5.24 kontroll – strukturált megközelítést ír elő az információbiztonsági incidensek jelentésére, értékelésére és kezelésére.

11.2.2. 5.25 kontroll – az incidensekből való tanulásra összpontosít a jövőbeli felkészültség és a rendszerek rezilienciájának javítása érdekében.

### 11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – meghatározza az incidenskezelési eljárásokat, beleértve az elhatárolást és a helyreállítást is.

11.3.2. IR-5 – követelményeket állapít meg az incidensek nyomon követésére és elemzésére.

11.3.3. IR-6 – előírja a külső és belső incidensjelentési protokollokat.

### 11.4. GDPR

11.4.1. 33. cikk – előírja a személyesadat-sértések szabályozó hatóságok felé történő bejelentését 72 órán belül, a kiterjedésre és a kockázatcsökkentésre vonatkozó részletekkel.

### 11.5. NIS2 irányelv (2022/2555)

11.5.1. 23. cikk – előírja, hogy az alapvető és fontos szervezetek a jelentős incidenseket szabványosított jelentési formátumok használatával jelentsék az illetékes hatóságoknak.

### 11.6. DORA-rendelet (2022/2554)

11.6.1. 17. cikk – előírja, hogy a pénzügyi szervezetek osztályozzák, jelentsék és nyomon kövessék az IKT-val kapcsolatos incidenseket és zavarokat.

**11.7. COBIT 2019**

11.7.1. DSS02 – Szolgáltatási kérelmek és incidensek kezelése: útmutatást ad a működési és biztonsági incidensek hatékony kezeléséhez, az irányítási célokkal összhangban.

11.7.2. DSS04 – Üzletmenet-folytonosság kezelése: összekapcsolja az incidenskezelést a szélesebb üzletmenet-folytonossági és helyreállítási stratégiákkal.