					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P30					Dokumentum címe: **Incidenskezelési szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 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

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8.1. pont, 9. pont	Strukturált folyamatok a kockázatkezeléshez és az incidenskezeléshez
ISO/IEC 27002:2022	5.25–5.27 kontrollok	Szerepkörök, jelentéstétel, reagálás és fejlesztés az incidenskezelésben
NIST SP 800-53 Rev.5	IR-1–IR-9	Átfogó incidenskezelési életciklus
EU GDPR	33. cikk (1), 33. cikk (3) a)–d), 34. cikk (1), 34. cikk (2) a)–c)	Incidensbejelentési határidők, jelentéstétel és kommunikáció az érintettekkel
EU NIS2	23. cikk (1)–(4)	A nemzeti hatóság értesítése és strukturált jelentéstétel
EU DORA	17. cikk (1)–(3)	Jelentős IKT-val kapcsolatos incidensek jelentése a pénzügyi szervezetek részéről
COBIT 2019	DSS02, DSS04, MEA	Meghatározza, felügyeli és értékeli az incidenskezelést, a folytonosságot és az értékelést

1. Cél

1.1 Jelen szabályzat formális keretet határoz meg a szervezetet érintő információbiztonsági incidensek azonosítására, jelentésére, elemzésére, elkülönítésére, kezelésére, helyreállítására és az incidenseket követő értékelésére.

1.2 A szabályzat biztosítja az időszerű, összehangolt és hatékony reagálást az operatív fennakadások, a pénzügyi veszteségek, a reputációs károk és a jogszabályi meg nem felelés minimalizálása érdekében.

1.3 A szabályzat továbbá támogatja a szervezet kiberreziliencia-képességének folyamatos fejlesztését a levont tanulságok, valamint az incidenseket követő megállapítások irányítási, eszközhasználati és képzési programokba történő beépítése révén.

2. Hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 Valamennyi munkatársra, ideértve a munkavállalókat, vállalkozókat, tanácsadókat és harmadik fél szolgáltatókat.

2.1.2 Valamennyi információs rendszerre, alkalmazásra, infrastruktúrára, hálózatra és adatra, helyszíni, felhőalapú vagy hibrid környezetben egyaránt.

2.1.3 A biztonsági incidensek valamennyi típusára, beleértve többek között az alábbiakat:

2.1.3.1 Jogosulatlan hozzáférés vagy jogosultságkiterjesztés.

2.1.3.2 Kártevő- és zsarolóvírus-támadások.

2.1.3.3 Szolgáltatásmegtagadásos (DoS/DDoS) támadások.

2.1.3.4 Adatvesztés, adatszivárgás vagy adatkivitel.

2.1.3.5 Belső visszaélés vagy szabályzatsértés.

2.1.3.6 A digitális vagyonelemeket érintő fizikai biztonsági események.

2.2 A szabályzat kiterjed az észlelésre, előzetes értékelésre, kivizsgálásra, eszkalációra, elkülönítésre, a bizonyítékok kezelésére, az értesítésre, a helyreállításra és a gyökérokelemzésre.

3. Célkitűzések

3.1 Ismételhető és skálázható incidensreagálási képesség kialakítása annak érdekében, hogy a biztonsági incidensek gyorsan észlelhetők, osztályozhatók és kezelhetők legyenek.

3.2 A biztonsági események üzleti hatásának minimalizálása strukturált elkülönítési, eltávolítási és rendszer-helyreállítási eljárásokkal.

3.3 Annak biztosítása, hogy az incidensjelentés és az incidensreagálás összhangban álljon a jogi, szabályozási és szerződéses követelményekkel, különösen az incidensbejelentési határidőkre és a bizonyítékok kezelésére vonatkozó előírásokkal.

3.4 Az átláthatóság és az elszámoltathatóság támogatása valamennyi biztonsági incidens megfelelő naplózásával, dokumentálásával és a mutatók nyomon követésével.

3.5 A folyamatos fejlesztés elősegítése incidenseket követő felülvizsgálatokkal, helyesbítő intézkedésekkel és az érintett felek képzésével.

4. Szerepkörök és felelősségek

4.1 Információbiztonsági vezető

4.1.1 Az incidensreagálási keretrendszer tulajdonosa, biztosítja a szabályzat érvényesítését, és felügyeli a szervezetszintű incidenskezelési koordinációt.

4.1.2 Jelentős incidensek esetén elsődleges kapcsolattartóként jár el a szabályozó hatóságok, a felső vezetés és a külső jogi tanácsadók felé.

4.2 Incidensreagálási koordinátor

4.2.1 Koordinálja a szakterületek közötti reagáló csapatokat, kezeli a munkafolyamatokat, és nyomon követi az elkülönítés és helyreállítás állapotát.

4.2.2 Elindítja és vezeti az incidenseket követő felülvizsgálatokat (PIR), valamint biztosítja, hogy a helyesbítő intézkedések naplózásra és végrehajtásra kerüljenek.

4.3 Biztonsági műveleti központ (SOC) / IT-biztonsági elemzők

4.3.1 Figyelemmel kísérik a rendszereket, a SIEM-platformokat és az MDR/XDR-eszközöket a kompromittálódás indikátorai szempontjából.

4.3.2 Elvégzik a kezdeti előzetes értékelést, a súlyossági besorolást és a technikai elkülönítést.

4.3.3 A megerősített vagy magas súlyosságú incidenseket eszkalálják az incidensreagálási koordinátor és az érintett felek felé.

4.4 Valamennyi munkatárs (munkavállalók, vállalkozók, harmadik felek)

4.4.1 Kötelesek minden feltételezett vagy megerősített információbiztonsági incidenst az észleléstől számított egy órán belül a kijelölt csatornákon jelenteni.

4.4.2 Kötelesek a kivizsgálás és az elkülönítési intézkedések során teljes körűen együttműködni.

4.5 Adatvédelmi tisztviselő (DPO) és jogi tanácsadó

4.5.1 Értékelik az incidensek jogi és szabályozási hatását, különösen a személyes vagy szabályozott adatokat érintő esetekben.

4.5.2 Biztosítják, hogy a GDPR, a NIS2 irányelv vagy a DORA rendelet szerinti incidensbejelentések az előírt határidőn belül megtörténjenek, például a GDPR 33. cikke szerint 72 órán belül.

4.6 Felső vezetés / Információbiztonsági Irányító Bizottság (ISSC)

4.6.1 Magas súlyosságú incidensek során stratégiai döntéseket hoznak, beleértve az értesítések jóváhagyását és a nyilvános kommunikációt.

4.6.2 Felülvizsgálják a PIR eredményeit, jóváhagyják a költségvetési és eljárásbeli fejlesztéseket, valamint megerősítik az IBIR frissítéseit.

5. Irányítási követelmények

5.1 A szervezet köteles központi és többszintű incidensreagálási keretrendszert fenntartani az ISO/IEC 27035 szabvánnyal összhangban, amely a következő meghatározott reagálási szakaszokból áll:

5.1.1 Felkészülés.

5.1.2 Észlelés és elemzés.

5.1.3 Elkülönítés, eltávolítás és helyreállítás.

5.1.4 Incidenseket követő felülvizsgálat és tanulságok levonása.

5.2 Valamennyi incidenst a biztonsági incidenskezelő rendszerben (SIMS) kell rögzíteni, beleértve az alábbiakat:

5.2.1 Az észlelés ideje és módja.

5.2.2 Osztályozás / súlyossági szint.

5.2.3 Az érintett rendszerek és adatok.

5.2.4 Elkülönítési, helyreállítási és korrekciós intézkedések.

5.2.5 Bizonyítékok, amennyiben gyűjtésük megtörtént.

5.2.6 Gyökérok és hosszú távú helyesbítő intézkedések.

5.3 Az incidensbesorolásnak többszintű modellt kell követnie:

5.3.1 1. szint: Kritikus (pl. megerősített adatsértés, zsarolóvírussal összefüggő kártevőkitörés, éles rendszer kompromittálódása).

5.3.2 2. szint: Magas (pl. kártevőészlelés, jogosulatlan hozzáférési kísérletek).

5.3.3 3. szint: Közepes / alacsony (pl. adathalászati kísérletek, szabályzatsértések).

5.4 Az incidensreagálási szerepköröket és eszkalációs útvonalakat az incidensreagálási tervben (IRP) kell dokumentálni, és időszakos asztali, valamint éles gyakorlatokkal kell tesztelni.

5.5 Minden incidenssel kapcsolatos kommunikációnak a kommunikációs és eszkalációs mátrix szerint kell történnie, biztosítva az alábbiakat:

5.5.1 Belső értesítés az IT, a jogi és megfelelőségi, a DPO, valamint a vezetői érintettek részére.

5.5.2 Külső kommunikáció a szabályozó hatóságok, ügyfelek vagy a média felé, ahol ez indokolt.

5.5.3 A védett vagy érzékeny tartalmak megőrzése jogi felülvizsgálat mellett.

5.6 A harmadik fél szolgáltatásaival való integrációkat, ideértve a menedzselt észlelési és reagálási szolgáltatást (MDR), a biztonsági incidens- és eseménykezelést (SIEM), valamint a forenzikus elemzést nyújtó szolgáltatókat, egyértelműen meghatározott szolgáltatási szint megállapodások (SLA-k) és titoktartási feltételek szerint kell irányítani.

5.7 Az információbiztonsági vezető köteles évente felülvizsgálni az incidensreagálási programot, beleértve az alábbiakat:

5.7.1 A korábbi incidensekből levont tanulságokat.

5.7.2 Az eszközök frissítéseit.

5.7.3 A csapat összetételét.

5.7.4 Az incidenskezelést vagy incidensbejelentést érintő jogi vagy szabályozási változásokat.

5.8 Az információbiztonsági vezető köteles meghatározni, jóváhagyni és időszakosan felülvizsgálni az incidensreagálás hatékonyságának értékelésére használt valamennyi megfigyelési és mérési szempontot. Ezeket a mutatókat dokumentálni kell, legalább évente felül kell vizsgálni, és fel kell használni az IBIR fejlesztésének, a belső auditok tervezésének és az incidenseket követő helyesbítő intézkedések támogatására. Kötelező mutatók:

5.8.1 Átlagos észlelési idő (MTTD) – az incidens bekövetkezésétől az észlelésig eltelt átlagos idő.

5.8.2 Átlagos elkülönítési idő (MTTC) – az észleléstől a sikeres elkülönítésig eltelt átlagos idő.

5.8.3 A gyökérokelemzéssel (RCA) lezárt incidenseket követő felülvizsgálatok (PIR) aránya – a reagálási életciklus érettségének és elszámoltathatóságának mérőszáma.

5.8.4 A bejelentésköteles incidensek száma – a GDPR, a NIS2 irányelv vagy a DORA rendelet szerint bejelentést igénylő incidensek.

6. A szabályzat végrehajtásának követelményei

6.1 Incidensek azonosítása és előzetes értékelése

6.1.1 Minden munkavállaló köteles a feltételezett incidenseket jóváhagyott csatornákon jelenteni:

6.1.1.1 SOC forródrót.

6.1.1.2 E-mail a security@<organization>.com címre.

6.1.1.3 Incidensportál űrlap.

6.1.2 A kezdeti előzetes értékelést a beérkezéstől számított egy munkaórán belül el kell végezni, beleértve az előzetes súlyossági besorolást.

6.2 Elkülönítés és kockázatcsökkentés

6.2.1 A SOC köteles az érintett rendszereket haladéktalanul elkülöníteni, a kompromittált hitelesítő adatokat visszavonni, illetve a rosszindulatú forgalmat tűzfalas vagy végpontvédelmi eszközökkel blokkolni.

6.2.2 Az átmeneti intézkedéseket az IT- és alkalmazáscsapatokkal összehangolt további intézkedéseknek kell követniük a fenyegetések környezetből történő eltávolítása érdekében.

6.3 Helyreállítás és ellenőrzés

6.3.1 A szolgáltatások helyreállítását a katasztrófa utáni helyreállítási (DR), valamint a Biztonsági mentési és helyreállítási szabályzat (P15) eljárásai szerint kell végrehajtani.

6.3.2 A rendszer újbóli aktiválása előtt ellenőrzést kell végezni annak biztosítására, hogy:

6.3.2.1 Valamennyi kompromittálódási indikátor eltávolításra került.

6.3.2.2 Nem maradt fenn perzisztenciát biztosító mechanizmus.

6.3.2.3 A naplózás, a felügyelet és a riasztások helyreállítása megtörtént.

6.4 Incidensbejelentési követelmények

6.4.1 Ha egy incidens személyes vagy szabályozott adat megerősített vagy valószínűsíthető kitettségét eredményezi, a jogi és megfelelőségi terület, valamint a DPO köteles értékelni az alábbiak alkalmazhatóságát:

6.4.1.1 GDPR 33. cikk (felügyeleti hatóság értesítése 72 órán belül).

6.4.1.2 GDPR 34. cikk (érintettek értesítése magas kockázat esetén).

6.4.1.3 NIS2 23. cikk (értesítés az incidens tudomásra jutását követő 24 órán belül).

6.4.1.4 DORA 17. cikk (súlyos IKT-incidensek jelentése).

6.4.2 Minden incidensbejelentést dokumentálni kell, benyújtás előtt jóvá kell hagyni, és másolatát a SIMS-ben meg kell őrizni.

6.5 Digitális forenzika és bizonyítékkezelés

6.5.1 Amennyiben forenzikus vizsgálat szükséges, a felhatalmazott személyek kötelesek:

6.5.2 Az érintett rendszerekről vagy lemezekről másolatot készíteni írásvédett eljárások alkalmazásával.

6.5.3 Fenntartani a bizonyítéklánc dokumentációját.

6.5.4 A bizonyítékokat titkosított, hozzáférés-szabályozással védett adattárakban tárolni.

6.5.5 A bűnüldöző szervekkel vagy forenzikus szolgáltatókkal történő együttműködést a jogi csapaton és az információbiztonsági vezetőn keresztül koordinálni.

7. Kockázatkezelés és kivételek

7.1 A jelen szabályzatban meghatározott eljárásoktól, szerepköröktől vagy kontrolloktól való bármely eltérést a formális kockázatkezelési és kivételkezelési folyamat szerint kell kezelni.

7.2 Kivételkérelmi követelmények

7.2.1 A kérelmező fél köteles dokumentált indoklást benyújtani, amely legalább az alábbiakat tartalmazza:

7.2.1.1 A be nem tartott konkrét eljárási lépést vagy kontrollt.

7.2.1.2 Az eltérés okát, például szerződéses korlátozásokat vagy örökölt rendszerek korlátait.

7.2.1.3 A kapcsolódó kockázatokat és a lehetséges hatást.

7.2.1.4 A kompenzáló kontrollokat vagy kockázatcsökkentő intézkedéseket.

7.2.1.5 Az érvényességi időszakot és a tervezett rendezési határidőt.

7.3 Felülvizsgálat és jóváhagyás

7.3.1 Az információbiztonsági vezető köteles jóváhagyni valamennyi, incidensreagálással kapcsolatos kivételt.

7.3.2 A szabályozási hatással járó kivételeket, például az incidensbejelentési határidőket érintő eseteket, a jogi csapatnak és az adatvédelmi tisztviselőnek is felül kell vizsgálnia.

7.4 Gyakori kockázati forgatókönyvek

7.4.1.1 Az incidensészlelés késedelme a felügyeleti hiányosságok miatt.

7.4.1.2 Az incidensek gyors elkülönítésének elmaradása, amely továbbterjedést vagy elhúzódó szolgáltatáskiesést eredményez.

7.4.1.3 Nem megfelelő bizonyítékgyűjtés, amely miatt jogi eljárás nem támasztható alá.

7.4.1.4 Az incidensbejelentés elmulasztása a jogszabályi határidőn belül.

7.5 Minden kivételt a kockázati nyilvántartásban kell dokumentálni, és legalább negyedévente felül kell vizsgálni. Ha a kockázati szint növekszik, vagy a kompenzáló kontrollok hatástalannak bizonyulnak, a kivételt vissza kell vonni vagy eszkalálni kell.

8. Betartatás és megfelelés

8.1 A jelen szabályzatnak való megfelelés kötelező valamennyi olyan munkatárs, vállalkozó és szolgáltató számára, aki részt vesz a biztonsági incidensek észlelésében, jelentésében, kezelésében vagy a helyesbítő intézkedések végrehajtásában.

8.2 Felügyelet és ellenőrzés

8.2.1 Az információbiztonsági csapat és a belső ellenőrzési / megfelelőségi funkció időszakosan értékeli az incidensreagálási felkészültséget és a megfelelést az alábbiak révén:

8.2.1.1 Az incidenskezelési jegyek és idővonalak felülvizsgálata.

8.2.1.2 Az elkülönítési és helyreállítási intézkedések ellenőrzése.

8.2.1.3 Az incidensbejelentések és kommunikációs dokumentumok értékelése.

8.2.1.4 Részvétel az asztali gyakorlatok eredményeinek értékelésében vagy azok felülvizsgálata.

8.3 A meg nem felelés esetei különösen:

8.3.1 Az incidensek nem időben történő jelentése.

8.3.2 Biztonsági események jogosulatlan kezelése vagy az eszkalációs útvonalak megkerülése.

8.3.3 Késedelem az elkülönítésben vagy hibás súlyossági besorolás.

8.3.4 Incidenssel kapcsolatos bizonyítékok visszatartása vagy a naplók megőrzésének elmulasztása.

8.3.5 Együttműködés megtagadása aktív kivizsgálás során.

8.4 A szabálysértések következményei

8.4.1 A súlyosságtól függően a szabálysértések az alábbi következményekkel járhatnak:

8.4.1.1 Kötelező ismétlő képzés vagy azonnali, ideiglenes hozzáférés-visszavonás.

8.4.1.2 Fegyelmi eljárás, amely a munkaviszony megszüntetéséig terjedhet.

8.4.1.3 Szerződéses jogorvoslatok harmadik fél általi nem teljesítés esetén.

8.4.1.4 A szabályozó hatóság értesítése, ha azt súlyos gondatlanság esetén jogszabály írja elő.

8.5 Az incidensjelentési és eszkalációs kötelezettség elmulasztása

8.5.1 Ha egy incidens a szabályzat be nem tartása miatt jelentés nélkül marad, és ez szabályozási vagy reputációs kárt okoz, a szervezet jogosult:

8.5.1.1 Jogi vagy szerződéses eljárást kezdeményezni.

8.5.1.2 A biztonsági jogosultságokat újraértékelni.

8.5.1.3 Az eljárásokat és biztonsági szerepköröket a gyökérok alapján frissíteni.

9. Felülvizsgálati és frissítési követelmények

9.1 Jelen szabályzatot legalább évente felül kell vizsgálni, és szükség szerint módosítani kell az alábbiak beépítése érdekében:

9.1.1 A fenyegetési környezet, az incidenstípusok vagy a támadási vektorok változásai.

9.1.2 A jelentős incidensekből, majdnem bekövetkezett eseményekből vagy szabályozói megállapításokból levont tanulságok.

9.1.3 Az alkalmazandó jogszabályok és szabályozások frissítései, például a GDPR, a DORA rendelet és a NIS2 irányelv változásai.

9.1.4 Az incidensreagálási gyakorlatokból és az incidenseket követő felülvizsgálatokból származó visszajelzések.

9.2 A felülvizsgálati folyamat megindításáért és koordinálásáért az információbiztonsági vezető felel, az alábbiakkal egyeztetve:

9.2.1.1 Jogi tanácsadó és DPO.

9.2.1.2 SOC és IT-üzemeltetés.

9.2.1.3 Üzletmenet-folytonossági és kockázatkezelési csapatok.

9.2.1.4 Felső vezetés.

9.3 A szabályzatmódosításokat:

9.3.1 Verziókezelt adattárban kell dokumentálni.

9.3.2 Kommunikálni kell valamennyi érintett csapat felé, és a biztonságtudatossági képzésben frissíteni kell.

9.3.3 A jóváhagyást követő három hónapon belül asztali vagy éles incidensreagálási gyakorlatokkal ellenőrizni kell.

9.4 A kialakulóban lévő kockázatok, auditmegállapítások vagy új jogi kötelezettségek által indokolt sürgős frissítéseket haladéktalanul végre kell hajtani, és a szabályzat változáselőzményeiben rögzíteni kell.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzatot az alábbi szervezeti szabályzatok támogatják, és azokhoz kapcsolódik:

10.1.1 P1 – Információbiztonsági szabályzat: Meghatározza a kockázatalapú, incidenskezelésre felkészült működés átfogó követelményeit.

10.1.2 P5 – Változáskezelési szabályzat: Biztosítja, hogy az infrastruktúrát vagy szolgáltatásokat érintő elkülönítési és helyreállítási tevékenységek formális eljárások szerint történjenek.

10.1.3 P13 – Adatosztályozási és címkézési szabályzat: Támogatja az incidensek súlyossági besorolását az adatok érzékenysége alapján.

10.1.4 P15 – Biztonsági mentési és helyreállítási szabályzat: Támogatja a zsarolóvírusos vagy romboló támadásokból történő helyreállítást a sértetlenség biztosítása mellett.

10.1.5 P18 – Kriptográfiai kontrollok szabályzata: Meghatározza azokat a titkosítási intézkedéseket, amelyek csökkentik az incidensek hatását és az adatkitettség kockázatát.

10.1.6 P22 – Naplózási és felügyeleti szabályzat: Biztosítja a hatékony észleléshez és a forenzikai vizsgálatokhoz szükséges alapvető eseménylláthatóságot, riasztásokat és naplómegőrzést.

10.1.7 P29 – Tesztadat- és tesztkörnyezet-szabályzat: Biztosítja, hogy a nem éles rendszereket érintő incidensek kezelése is strukturált és biztonságos módon történjen.

10.1.8 P33 – Audit- és megfelelésfelügyeleti szabályzat: Strukturált auditokkal és megfelelőségi értékelésekkel igazolja az incidensreagálási felkészültséget és a reagálás hatékonyságát.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001: 8.1. pont – Működéstervezés és -szabályozás: Strukturált folyamatok a kockázatok kezelésére és az incidensreagálás tervezésére.

11.2 ISO/IEC 27002:2022 – 5.25–5.27 kontrollok: Felelősségi körök az incidenskezelés, jelentés, reagálás, kommunikáció és fejlesztés területén.

11.3 NIST SP 800-53 Rev.5: IR-1–IR-9, AU-6, PL-2: Átfogó követelmények az incidensreagálási életciklusra, auditálásra és biztonsági tervezésre.

11.4 EU GDPR: 33/34. cikk: Jelentési kötelezettségek a felügyeleti hatóságok felé, valamint az érintettek értesítésének követelményei, meghatározott kivételekkel.

11.5 EU NIS2 irányelv (2022/2555): 23. cikk: Kötelező nemzeti jelentéstétel, közbenső és végső jelentési kötelezettségekkel.

11.6 EU DORA (2022/2554): 17. cikk: A pénzügyi intézményekre vonatkozó IKT-incidensek hatósági jelentési követelményei.

11.7 COBIT 2019: DSS02, DSS04, MEA01: Szolgáltatási incidensek és folytonosság kezelése, valamint teljesítmény- és megfelelőségfigyelés.