					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P36S					Dokumentum címe: **Közösségi média és külső kommunikációs 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

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	5.1, 5.2, 6.1, 8. pont	A külső kommunikációra vonatkozó vezetői irányítás, kockázatkezelés és működési kontrollok
ISO/IEC 27002:2022	5.10, 5.11 kontroll	Elfogadható használat és információbiztonság a kommunikáció során
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Magatartási szabályok, audit, incidensjelentés, valamint a nyilvánosan elérhető tartalmak és hozzáférések kezelése
EU GDPR	5., 32., 33. cikk	Az adatvédelem alapelvei, az adatkezelés biztonsága, valamint a nyilvános kommunikációt érintő incidensbejelentés
EU NIS2	21. cikk (2) bekezdés e), 21. cikk (2) bekezdés f)	Az információs rendszerek használatára vonatkozó szabályzatok, valamint az ellátási lánccal és a nyilvános kommunikációval kapcsolatos kockázatok kezelésére vonatkozó szabályzatok
EU DORA	14. cikk (4) bekezdés	Incidenst követő kommunikációs kötelezettségek

1. Cél

1.1. Jelen szabályzat kötelező érvényű előírásokat határoz meg minden nyilvánosan elérhető kommunikációra vonatkozóan — ideértve a közösségimédia-használatot, a sajtókapcsolatokat és a külső digitális tartalmakat — amennyiben azok a vállalatra, annak munkatársaira, ügyfeleire, rendszereire vagy belső működési gyakorlataira hivatkoznak.

1.2. A szabályzat célja a vállalat jó hírnevének védelme, a jogi és szabályozási megfelelés fenntartása, valamint az információszivárgás, a félretájékoztatás és a biztonsági incidensek kockázatának csökkentése.

1.3. A szabályzat elősegíti, hogy a munkatársak és partnerek pozitív és felelős módon vegyenek részt az online kommunikációban, miközben elkerülik a véletlen közzétételeket és a vállalat téves megjelenítését.

1.4. A szabályzat támogatja a KKV ISO/IEC 27001 tanúsításra való felkészültségét azáltal, hogy szabályozza a nyilvánosság vagy külső érdekelt felek számára hozzáférhetővé tett információk kezelését.

2. Hatály

2.1. Jelen szabályzat a szervezettel kapcsolatban álló valamennyi személyre kiterjed, beleértve az alábbiakat:

2.1.1. munkavállalók és vállalkozók

2.1.2. szabadúszók, tanácsadók és harmadik fél beszállítók

2.1.3. gyakornokok vagy részmunkaidős munkatársak, akik részt vesznek az ügyfélkiszolgálásban vagy rendszerhozzáféréssel rendelkeznek

2.2. A szabályzat a szervezetre hivatkozó külső kommunikáció minden formájára alkalmazandó, beleértve az alábbiakat:

2.2.1. közösségimédia-bejegyzések (LinkedIn, Twitter/X, TikTok, Instagram, Facebook stb.)

2.2.2. blogbejegyzések, online fórumok, ügyfélértékelések és hozzászólások

2.2.3. nyilvános szereplések (pl. konferenciák, webináriumok, podcastok)

2.2.4. e-mailek vagy üzenetek újságírók, kormányzati szereplők vagy influenszerek részére

2.2.5. munkahelyi környezetből nyilvánosan megosztott képernyőképek, fényképek vagy videók

2.3. A szabályzat akkor is alkalmazandó, ha az ilyen kommunikáció:

2.3.1. személyes eszközről vagy fiókból történik

2.3.2. a szokásos munkaidőn kívül történik

2.3.3. rosszhiszemű szándék nélkül történik — a véletlen vagy odavetett megjegyzések is a szabályzat hatálya alá tartoznak, ha a vállalatra utalnak

3. Célkitűzések

3.1. Reputációvédelem: a vállalat megítélését sértő jogosulatlan vagy nem megfelelő nyilvános kommunikáció megelőzése

3.2. Adatbiztonság: az érzékeny adatok, belső rendszerek vagy ügyféladatok közösségi médián vagy nyilvános csatornákon keresztüli nem szándékos közzétételének megelőzése

3.3. Jogi és szabályozási megfelelés: annak biztosítása, hogy a vállalatra hivatkozó minden nyilvános tartalom megfeleljen a vonatkozó adatvédelmi és üzleti kommunikációs előírásoknak

3.4. Professzionális magatartás: a felelős részvétel előmozdítása az online kommunikációban és médiaszereplések során, beleértve a személyes fiókok használatát is

3.5. Incidenskezelési felkészültség: egyértelmű, végrehajtható lépések biztosítása véletlen közzététel vagy szabályzatsértés esetére

4. Szerepkörök és felelősségek

4.1. ügyvezető

4.1.1. a szabályzat tulajdonosa és jóváhagyója

4.1.2. felülvizsgálja és jóváhagyja a nyilvánosságnak szánt nyilatkozatokat, sajtószerepléseket és médiainterjúkat

4.1.3. biztosítja, hogy a szabályzat valamennyi munkavállaló és harmadik fél számára egyértelműen kommunikálva legyen

4.1.4. kivizsgálja a jelen szabályzat megsértésének eseteit, és az incidenskezelési eljárásokkal összehangoltan intézkedik

4.2. kijelölt munkavállaló vagy kommunikációs felelős (ha kijelölésre került)

4.2.1. támogatja az ügyvezetőt a külső közzététel előtti tartalmak felülvizsgálatában (pl. blogbejegyzések, előadástémák)

4.2.2. nyilvántartja a jóváhagyott médiaaktivitásokat vagy magas kockázatú közösségimédia-bejegyzéseket

4.2.3. kapacitás függvényében figyelemmel kíséri a vállalatra vonatkozó nyilvános említéseket reputációs vagy biztonsági kockázatok szempontjából

[... 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. Éves felülvizsgálat

9.1.1. Jelen szabályzatot legalább évente egyszer felül kell vizsgálnia az ügyvezetőnek

9.1.2. A felülvizsgálatnak biztosítania kell az összhangot a frissített jogi kötelezettségekkel, az iparági kommunikációs trendekkel és a belső üzleti változásokkal

9.2. Esemény által kiváltott felülvizsgálatok

9.2.1. A jelen szabályzatot haladéktalanul frissíteni kell az alábbi esetekben:

9.2.1.1. jelentős közösségimédia-incidens vagy reputációs probléma után

9.2.1.2. a kommunikációt kezelő harmadik fél beszállítók változása esetén

9.2.1.3. online kommunikációval, médiával vagy márkahasználattal kapcsolatos új jogszabály vagy szabályozási kötelezettség esetén

9.3. Változások dokumentálása

9.3.1. Valamennyi frissítést rögzíteni kell, beleértve a felülvizsgálat dátumát, a változások összefoglalását és az ügyvezető jóváhagyását

9.3.2. Audit- és tanúsítási célból verzióelőzményeket kell vezetni

9.4. Frissítések közzététele

9.4.1. A szabályzat módosításairól valamennyi munkatársat és vállalkozót tájékoztatni kell

9.4.2. A frissített verziókat e-mailben vagy belső portálokon kell közzétenni

9.4.3. Minden nyilvános kommunikációval foglalkozó beszállítónak a munka folytatása előtt tudomásul kell vennie a frissített feltételeket

10. Kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzat az alábbi KKV-szabályzatokkal összehangoltan alkalmazandó:

10.1.1. P3S – Elfogadható használati szabályzat: meghatározza a kommunikációs platformok használatára vonatkozó elfogadható magatartási szabályokat, beleértve a munkaidő alatti közösségimédia-hozzáférést is

10.1.2. P8S – Információbiztonsági tudatossági és képzési szabályzat: biztosítja, hogy a munkatársak képzést kapjanak a túlzott információmegosztás, az adathalászat és az online reputációs fenyegetések kockázatainak felismerésére

10.1.3. P17S – Adatvédelmi és magánszféra-védelmi szabályzat: biztosítja, hogy személyes és ügyféladatok ne kerüljenek megosztásra külső kommunikációban, összhangban a GDPR-ral és más jogi követelményekkel

10.1.4. P30S – Incidenskezelési szabályzat: szabályozza a közösségi média helytelen használatából eredő véletlen nyilvános közzétételre, online fenyegetésekre vagy reputációs támadásokra adott reagálást

10.1.5. P37S – Jogi és szabályozási megfelelési szabályzat: meghatározza a szervezet nyilvános tartalommegosztással kapcsolatos átfogó jogi és szerződéses kötelezettségeit

10.2. E szabályzatokat együttesen kell alkalmazni a biztonságos, tiszteletteljes és jogszerű külső jelenlét fenntartása érdekében.

11. Hivatkozott szabványok és keretrendszerek

11.1. ISO/IEC 27001

11.1.1. 5.1. pont – Vezetés és elkötelezettség: megköveteli a reputációs és információbiztonsági kockázatok vezetői felügyeletét

11.1.2. 6.1. pont – Kockázatkezelés: magában foglalja a kommunikációval kapcsolatos kockázati kitettségeket

11.1.3. 8.1. pont – Működési kontroll: lefedi a külső információközlés szabályait

11.2. ISO/IEC 27002

11.2.1. 5.10 kontroll – információk és eszközök elfogadható használata

11.2.2. 5.11 kontroll – információbiztonság a kommunikáció során

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Magatartási szabályok: az információs erőforrások használatához kapcsolódó megfelelő magatartást szabályozza

11.3.2. AU-7 – Auditcsökkentés és jelentéskészítés: támogatja a nyilvános rendszerhasználat nyomon követését

11.3.3. IR-6 – Incidensjelentés: előírja a reputációs és kommunikációs jogsértésekre adott reagálást

11.3.4. AC-22 – Nyilvánosan elérhető tartalom: biztosítja a külső közzétételek és hozzáférések feletti kontrollt

11.4. GDPR (2016/679)

11.4.1. 5. cikk – A személyes adatok kezelésére vonatkozó alapelvek (pontosság, sértetlenség, elszámoltathatóság)

11.4.2. 32. cikk – Az adatkezelés biztonsága: védintézkedéseket ír elő a nyilvános megosztással kapcsolatban

11.4.3. 33. cikk – Incidensbejelentés: alkalmazandó, ha személyes adatok külső kommunikáció útján kerülnek nyilvánosságra

11.5. EU NIS2 irányelv (2022/2555)

11.5.1. 21. cikk (2) bekezdés e) pont – Az információs rendszerek használatára vonatkozó szabályzatok, beleértve a kommunikációs platformokat is

11.5.2. 21. cikk (2) bekezdés f) pont – A kiberbiztonsági kockázatok kezelésére vonatkozó szabályzatok az ellátási láncban és a nyilvános platformokon

11.6. EU DORA (2022/2554)

11.6.1. 14. cikk (4) bekezdés – Kommunikációs kötelezettségek ügyfelek, harmadik felek és hatóságok felé működési incidenseket követően

11.7. COBIT 2019

11.7.1. APO09 – Szolgáltatási megállapodások kezelése: lefedi a beszállítók és a kommunikációval összefüggő harmadik felek felügyeletét

11.7.2. DSS05 – Biztonsági szolgáltatások kezelése: magában foglalja a nyilvánosan elérhető digitális vagyonelemek védelmét

11.7.3. EDM03 – Kockázatoptimalizálás biztosítása: hangsúlyozza a kommunikációval kapcsolatos reputációs és megfelelési kockázatok kezelését