					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P03					Dokumentum címe: **Elfogadható használati 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	5.10. kontroll	Meghatározza az Elfogadható használati szabályzat (AUP) magatartási szabályait és követelményeit
ISO/IEC 27002:2022	6.1., 6.2., 8.1. és 8.12. kontroll	Iránymutatást ad az információbiztonsági felelősségi körök, a tudatosság, valamint az eszköz- és adatkezelés terén
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Az informatikai eszközök használatához kapcsolódó hozzáférés-szabályozási, tudatossági és magatartási kontrollokat írja elő
GDPR	5. cikk (1) bekezdés f) pont, 32. cikk; (39) preambulumbekezdés	Előírja a bizalmasság és sértetlenség védelmét, a technikai és szervezeti intézkedéseket, valamint a megfelelő használat jogszerű kereteit
NIS2 irányelv	21. cikk (2) bekezdés a)–d) pont	Előírja a működési szabályzatokat és a biztonságos használatra vonatkozó oktatást
DORA-rendelet	5. cikk	A felhasználói magatartás szabályozásával támogatja az IKT-kockázatkezelést
COBIT 2019	APO07, BAI05, DSS05, MEA01	A humánerőforrás-kezelés, a változáskezelés, a biztonsági szolgáltatások irányítása, valamint a megfelelőség és teljesítmény nyomon követése területeit fedi le

1. Cél

1.1 Ez a szabályzat meghatározza a szervezet információs rendszereinek, informatikai erőforrásainak, kommunikációs eszközeinek és információkezelési gyakorlatainak elfogadható és nem elfogadható használatát.

1.2 Biztosítja, hogy valamennyi felhasználó tisztában legyen a vállalati informatikai eszközök használatával kapcsolatos felelősségeivel, és hogy tevékenységük támogassa az információk bizalmasságát, sértetlenségét, rendelkezésre állását és jogszerű kezelését.

1.3 Ez a szabályzat az ISO/IEC 27001:2022 5.10. kontrolljának való megfelelés érdekében a rendszerhasználatra vonatkozó magatartási szabályokat határoz meg, és technikai, valamint eljárási védelmi intézkedéseket ír elő a nem megfelelő használatból, gondatlanságból vagy visszaélésből eredő kockázatok minimalizálására.

1.4 A szabályzat emellett támogatja a kivizsgálási és érvényesítési tevékenységeket, beleértve az incidenskezelést és a szabályszegésekhez kapcsolódó fegyelmi intézkedéseket.

2. Hatály

2.1 Ez a szabályzat minden olyan személyre és szervezetre kiterjed, amely hozzáférést kap a szervezet információs rendszereihez és vagyonelemeihez, ideértve többek között az alábbiakat:

2.1.1 Munkavállalók, vállalkozók, tanácsadók, gyakornokok és munkaerő-kölcsönzés keretében foglalkoztatott munkatársak

2.1.2 Rendszerhozzáféréssel vagy delegált adminisztratív szerepkörrel rendelkező harmadik fél beszállítók

2.1.3 Vendégek vagy partnerek, akik a szervezet tulajdonában álló vagy általa engedélyezett informatikai infrastruktúrát használják

2.2 A hatály a szervezet valamennyi technológiai és adatvagyonára kiterjed, beleértve az alábbiakat:

2.2.1 Munkaállomások, laptopok, mobileszközök és szerverek

2.2.2 Hálózati infrastruktúra és felhőalapú szolgáltatások

2.2.3 E-mail, üzenetküldés, fájltárolás, együttműködési platformok és VPN-ek

2.2.4 Tárolt, továbbított vagy feldolgozás alatt álló adatok, formátumtól és helytől függetlenül

2.2.5 Bármely személyes eszköz, amelyet BYOD (saját eszköz használata) keretében a szervezeti rendszerekhez csatlakoztatnak

2.3 Ez a szabályzat valamennyi munkakörnyezetben alkalmazandó és érvényesíthető, beleértve az alábbiakat:

2.3.1 Vállalati irodák és termelési telephelyek

2.3.2 Távmunkavégzési helyszínek vagy hibrid munkavégzési környezetek

2.3.3 Terepi munkavégzési helyszínek vagy harmadik fél által üzemeltetett telephelyek

2.4 Valamennyi felhasználó esetében e szabályzat tudomásulvétele és betartása a vállalati rendszerekhez való hozzáférés, illetve a vállalati adatok kezelése előfeltétele.

3. Célkitűzések

3.1 A szervezeti informatikai erőforrások elfogadható használatára vonatkozó szabályok meghatározása és érvényesítése.

3.2 A jogosulatlan hozzáférés, az adatszivárgás, valamint a gondatlan vagy rosszindulatú használatból eredő károk megelőzése.

3.3 A vállalati hálózatok, eszközök és adatok védelme a felhasználói magatartásból eredő fenyegetésekkel szemben.

3.4 A jogi és szerződéses kötelezettségek teljesítésének támogatása az informatikai erőforrások irányítása során tanúsított kellő gondosság igazolásával.

3.5 A fegyelmi intézkedések és a kivételkezelési folyamatok egységes és egyértelmű alkalmazásának biztosítása.

3.6 Az etikus, biztonságos és felelős digitális és fizikai informatikai erőforrás-használat kultúrájának erősítése.

4. Szerepkörök és felelősségi körök

4.1 Felső vezetés

4.1.1 Jóváhagyja az Elfogadható használati szabályzatot (AUP), és biztosítja, hogy az összhangban legyen az üzleti célokkal, a szabályozói követelményekkel és a szervezeti értékekkel.

4.1.2 Erőforrásokat biztosít a betartáshoz, a képzéshez, a nyomon követéshez és a szabályzat felülvizsgálatához.

4.1.3 Az IBIR irányítási keretrendszer részeként felülvizsgálja a megfelelőségi helyzetet és a szabályzatsértésekhez kapcsolódó fegyelmi intézkedéseket.

4.2 Informatikai és információbiztonsági csapatok

4.2.1 Technikai védelmi intézkedéseket vezetnek be e szabályzat érvényesítése érdekében, beleértve az alábbiakat:

4.2.2 Tartalomszűrés, kártékonykód-elleni védelem, végpontbiztonság és hálózatfelügyeleti eszközök

4.2.3 E-mail-biztonsági beállítások és adatvesztés-megelőzési (DLP) megoldások

4.2.4 Szoftverekre, hardverekre és webhelyekre vonatkozó tiltólisták és engedélyezőlisták

4.2.5 Nyilvántartást vezetnek a jóváhagyott, illetve tiltott szoftverekről, eszközökről és szolgáltatásokról.

4.2.6 Kivizsgálják az Elfogadható használati szabályzat (AUP) feltételezett megsértéseit, forenzikai bizonyítékokat gyűjtenek, és szükség esetén támogatják a fegyelmi vagy jogi eljárást.

4.2.7 Együttműködnek a humánerőforrás-területtel és a jogi területtel az incidenskezelés, az eszkaláció és a jelentéstételi kötelezettségek teljesítése során.

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

9. Felülvizsgálati és aktualizálási követelmények

9.1 Felülvizsgálatot kiváltó események és gyakoriság

9.1.1 E szabályzatot felül kell vizsgálni:

9.1.1.1 legalább évente egyszer

9.1.1.2 minden jelentős technológiai vagy infrastrukturális változást követően

9.1.1.3 olyan incidensek vagy auditmegállapítások után, amelyek az érvényesítés hiányosságaira mutatnak rá

9.1.1.4 az alkalmazandó jogszabályok vagy szerződések változása esetén

9.2 Felelősség és jóváhagyás

9.2.1 A felülvizsgálati folyamatért az információbiztonsági vezető vagy az általa kijelölt IBIR-vezető felelős.

9.2.2 A módosításokat a felső vezetésnek kell jóváhagynia, és azokat a teljes szervezetben kommunikálni kell.

9.2.3 A frissített feltételek tudomásulvételét a szabályzat újbóli kiadásakor ismételten be kell szerezni.

9.3 Dokumentumkezelés

9.3.1 A szabályzatnak az alábbi metaadatokat és verziókezelési adatokat kell tartalmaznia:

9.3.1.1 Cím, azonosító és osztályozási szint

9.3.1.2 Szabályzatgazda és dokumentumgazda

9.3.1.3 Változáselőzmények és a módosítások indokolása

9.3.1.4 Felülvizsgálat dátuma és a következő ütemezett aktualizálás dátuma

9.3.1.5 A terjesztési és tudomásulvételi naplók hivatkozásai

9.3.2 A mesterpéldányt az IBIR dokumentumtárban, verziókezelés mellett kell megőrizni.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Ezt a szabályzatot a következő szabályzatokkal együtt kell értelmezni:

10.1.1 P1 – Információbiztonsági szabályzat: Meghatározza az elfogadható használatra vonatkozó alapvető magatartási elvárásokat és a felső vezetés elkötelezettségét.

10.1.2 P4 – Hozzáférés-szabályozási szabályzat: Meghatározza a felhasználókhoz, rendszerekhez és adathozzáféréshez kapcsolódó engedélyeket és hozzáférési jogosultságokat, és közvetlenül érvényesíti az elfogadható használat határait.

10.1.3 P6 – Kockázatkezelési szabályzat: Kezeli a magatartással összefüggő kockázatokat, és támogatja a felhasználói eredetű fenyegetésekhez kapcsolódó nyomon követési és kezelési tevékenységeket.

10.1.4 P7 – Beléptetési és kiléptetési szabályzat: Biztosítja, hogy az elfogadható használat feltételeinek tudomásulvétele belépéskor megtörténjen, és a kapcsolódó hozzáférések kilépéskor megszűnjenek.

10.1.5 P9 – Távmunka-szabályzat: Kiterjeszti az elfogadható használatra vonatkozó előírásokat a távoli és hibrid munkakörnyezetekre.

10.2 Ezek a kapcsolódó szabályzatok magatartási, technikai és szerződéses szempontból többrétegű védelmi modellt alkotnak.

11. Hivatkozott szabványok és keretrendszerek

11.1 Ez az Elfogadható használati szabályzat (AUP) nemzetközileg elismert szabványokkal és jogi keretrendszerekkel áll összhangban annak érdekében, hogy a digitális és fizikai információs rendszerek teljes használatára kiterjedő, érvényesíthető, auditálható és kockázatalapú magatartási kontrollokat biztosítson.

11.2 ISO/IEC 27001:2022

11.2.1 5.10. kontroll – Az információk és a kapcsolódó egyéb eszközök elfogadható használata: Ez a szabályzat közvetlenül teljesíti az informatikai erőforrások megfelelő használatát szabályozó előírások meghatározására, kommunikálására és érvényesítésére vonatkozó követelményt.

11.2.2 A melléklet 6.1. kontroll – Az információbiztonságért viselt felelősség: Egyértelmű felelősségi köröket rendel a felhasználói magatartáshoz és a megfelelés felügyeletéhez.

11.2.3 A melléklet 6.2. kontroll – Információbiztonsági tudatosság, oktatás és képzés: A beépített oktatási és szabályzati tudomásulvételi folyamatok az AUP érvényesítésének részét képezik.

11.2.4 A melléklet 8.1. kontroll – Felhasználói végponti eszközök, valamint 8.12. kontroll – Adatvesztés-megelőzés (DLP): Szabályozza a felhasználói végponti eszközök használata során elvárt magatartást, valamint azokat a tevékenységeket, amelyek adatkitettséghez vagy adatszivárgáshoz vezethetnek.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-19 (mobil eszközökre vonatkozó hozzáférés-szabályozás) és AC-20 (külső információs rendszerek használata): Ez a szabályzat meghatározza a BYOD (saját eszköz használata) és a harmadik fél rendszereihez való hozzáférés során alkalmazandó felhasználói kötelezettségeket és korlátozásokat.

11.3.2 PL-4 (Magatartási szabályok): E szabályzattal összhangban részletes, elfogadható használatra vonatkozó követelményeket határoz meg.

11.3.3 AT-2 (biztonságtudatossági képzés): A felhasználói képzés és a dokumentált szabályzati tudomásulvétel támogatja.

11.3.4 AU-2 (audit-események) és AU-12 (auditnaplók előállítása): Az érvényesítés a felhasználói tevékenységek megfigyelésére és a szabálysértésekkel kapcsolatos riasztásokra támaszkodik.

11.4 GDPR (2016/679)

11.4.1 5. cikk (1) bekezdés f) pont: Előírja a személyes adatok biztonságát és sértetlenségét; ez a szabályzat mérsékli az emberi magatartásból és a jogosulatlan használatból eredő kockázatokat.

11.4.2 32. cikk: Előírja a személyes adatok védelmét szolgáló technikai és szervezeti intézkedéseket, például a magatartási kontrollokat és a használati korlátozásokat.

11.4.3 (39) preambulumbekezdés: Kiemeli annak szükségességét, hogy csak a szükséges hozzáférés és a jogosult személyek általi jogszerű adatfelhasználás legyen biztosított.

11.5 NIS2 irányelv (2022/2555)

11.5.1 21. cikk (2) bekezdés a)–d) pont: Megköveteli a biztonságos rendszerhasználatot támogató működési szabályzatokat és képzéseket, amelyeket e szabályzat a magatartási, felügyeleti és érvényesítési folyamatok meghatározásával biztosít.

11.6 DORA-rendelet (2022/2554)

11.6.1 5. cikk: Ez a szabályzat a felhasználó és rendszer közötti interakció szabályainak meghatározásával és a magatartásalapú kiberkockázati kitettség csökkentésével támogatja az IKT-kockázatkezelési keretrendszert.

11.7 COBIT 2019

11.7.1 APO07 – Humánerőforrás-kezelés: A munkavállalói életciklus teljes időtartama alatt érvényesíti a felhasználói felelősségeket és a tudatosságot.

11.7.2 BAI05 – Szervezeti változások kezelése: Az elfogadható használat irányítását beépíti a felhasználói magatartást érintő változási folyamatokba.

11.7.3 DSS05 – Biztonsági szolgáltatások kezelése: Támogatja a felhasználói tevékenységek megfigyelését, a viselkedésalapú riasztásokat és az automatizált válaszmechanizmusokat.

11.7.4 MEA01 – A teljesítmény és a megfelelőség nyomon követése, értékelése és felmérése: A szabályzat meghatározza a felhasználói megfelelésnek a magatartási elvárásokhoz viszonyított nyomon követésére, értékelésére és felmérésére szolgáló mutatókat és mechanizmusokat.