					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P03S					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. pont	A szabályzat teljes hatálya és alkalmazása szempontjából releváns
ISO/IEC 27002:2022	5.10, 5.11, 5. pont	Iránymutatást ad az elfogadható használatra vonatkozó követelményekhez és kontrollokhoz
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Kiterjed a rendszerek és eszközök használatára, a nyomon követésre és a felhasználói képzésre
GDPR	5. cikk (1) bekezdés f) pont, 32. cikk	Az adatok sértetlenségére és bizalmasságára, valamint a biztonsági intézkedésekre vonatkozó követelmények
NIS2 irányelv	21. cikk (2) bekezdés b) pont	Előírja a megfelelő biztonsági és elfogadható használati szabályzatok alkalmazását
DORA-rendelet	9. cikk	IKT-kockázatkezelési szabályzat, kontrollok és végrehajtás
COBIT 2019	DSS05, BAI08	Biztonsági szolgáltatások és tudáskezelés

1. Cél

1.1. Jelen szabályzat meghatározza a vállalat által biztosított rendszerek, eszközök, internet-hozzáférés, e-mail, felhőszolgáltatások, valamint az üzleti célra használt saját tulajdonú eszközök elfogadható, felelős és biztonságos használatának szabályait.

1.2. A szabályzat biztosítja, hogy az érintettek megértsék kötelezettségeiket a szervezeti informatikai erőforrások használata során, különös tekintettel az adatok sértetlenségének, a magánszféra védelmének és a működés folytonosságának megőrzésére.

1.3. Jelen szabályzat az ISO/IEC 27001:2022 szerinti megfelelést támogatja azáltal, hogy egyértelmű felhasználói magatartási elvárásokat határoz meg, összhangban a jogi, szerződéses és szabályozói követelményekkel.

2. Hatály

2.1. Jelen szabályzat minden olyan személyre kiterjed, aki hozzáfér a vállalat rendszereihez vagy adataihoz, azokat kezeli, vagy azokkal kapcsolatba kerül, ideértve:

2.1.1. a munkavállalókat és szerződéses közreműködőket,

2.1.2. az ideiglenes munkavállalókat és gyakornokokat,

2.1.3. a külső informatikai szolgáltatókat.

2.2. A szabályzat kiterjed:

2.2.1. a vállalati tulajdonú számítógépekre, telefonokra és táblagépekre,

2.2.2. az üzleti használatra jóváhagyott saját tulajdonú eszközökre (BYOD),

2.2.3. a vállalati hálózatokra, felhőplatformokra és szoftverszolgáltatásokra,

2.2.4. az internet-hozzáférésre, az e-mail-rendszerekre, a megosztott tárhelyekre és az üzleti alkalmazásokra.

2.3. Jelen szabályzat valamennyi munkavégzési környezetben – helyszíni, távoli és hibrid munkavégzés esetén egyaránt – a teljes üzleti működés időtartama alatt alkalmazandó.

3. Célkitűzések

3.1. Meghatározni, mi minősül az informatikai rendszerek elfogadható, illetve nem elfogadható használatának.

3.1.1. Csökkenteni a helytelen használatból, a jogosulatlan hozzáférésből vagy rosszindulatú szoftver bejuttatásából eredő biztonsági kockázatokat.

3.1.2. Védeni az üzleti adatokat, az ügyfélinformációkat és a vállalat hírnevét.

3.1.3. Kikényszeríthető szabályokat meghatározni, és biztosítani az elszámoltathatóságot valamennyi felhasználó számára.

3.1.4. Támogatni a nyomon követést és a megfelelést a szabálysértések korai észlelése és a helyesbítő intézkedések megtétele érdekében.

4. Szerepkörök és felelősségi körök

4.1. Ügyvezető

4.1.1. Jóváhagyja jelen szabályzatot, és biztosítja a végrehajtáshoz szükséges erőforrásokat és felhatalmazást.

4.1.2. Felülvizsgálja és jóváhagyja a jelen szabályzat alóli kivételeket.

4.2. Informatikai vezető vagy külső informatikai szolgáltató

4.2.1. Fenntartja a jóváhagyott szoftverek és hardvereszközök nyilvántartását.

4.2.2. Az eszközöket úgy konfigurálja, hogy azok érvényesítsék az elfogadható használat szabályait (pl. tartalomszűrés, hozzáférési naplózás).

4.2.3. Nyomon követi a használatot a lehetséges szabálysértések azonosítása érdekében, és kivizsgálja az incidenseket.

4.2.4. Biztosítja, hogy az üzleti célra használt saját tulajdonú eszközök (BYOD) használata engedélyezett és biztonságos legyen.

[... 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. Éves felülvizsgálat

9.1.1. Jelen szabályzatot az informatikai vezetőnek évente felül kell vizsgálnia, az ügyvezető végső jóváhagyásával, annak biztosítása érdekében, hogy a szabályzat továbbra is összhangban maradjon a technológiahasználati mintázatokkal, a megjelenő kockázatokkal és a megfelelési kötelezettségekkel.

9.2. Soron kívüli felülvizsgálatot kiváltó események

9.2.1. Felülvizsgálatot kell végezni az alábbi esetekben is:

9.2.2. új rendszerek vagy technológiák bevezetése (pl. új felhőszolgáltatás vagy végponti platform),

9.2.3. jelentős szabályzatsértések,

9.2.4. az informatikai használatot érintő jogszabályok vagy szerződéses feltételek módosulása.

9.3. Változások dokumentálása

9.3.1. Minden módosítást verziónaplóban kell rögzíteni, amely legalább az alábbiakat tartalmazza:

9.3.1.1. verziószám,

9.3.1.2. a felülvizsgálat dátuma,

9.3.1.3. a változások összefoglalása,

9.3.1.4. a jóváhagyó megnevezése.

9.4. A szabályzat kommunikálása

9.4.1. Jelen szabályzat módosított változatait minden érintett felhasználóval meg kell osztani. A munkavállalók kötelesek az átvételt és a megértést a biztonságtudatossági kötelezettségeik részeként visszaigazolni.

10. Kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzat több más SME-szabályzattal együtt biztosítja a biztonsági felelősségi körök teljes körű lefedését:

10.1.1. P4S – Hozzáférés-szabályozási szabályzat: Meghatározza az engedélyezett használat és a fiókkorlátozások technikai és eljárási érvényesítését.

10.1.2. P8S – Információbiztonsági tudatossági és képzési szabályzat: Felhasználói oktatást biztosít az elfogadható használat határairól és a bejelentési kötelezettségekről.

10.1.3. P9S – Távmunka-szabályzat: Szabályozza a vállalati rendszerek használatát külső helyszínen vagy otthoni munkavégzés során.

10.1.4. P17S – Adatvédelmi és a magánszféra védelmére vonatkozó szabályzat: Érvényesíti a személyes adatok kezelésére vonatkozó szabályokat, amelyek összefüggnek az elfogadható használat nyomon követésével és a BYOD használatával.

10.1.5. P30S – Incidenskezelési szabályzat: Meghatározza a helytelen használat vagy az elfogadható használati feltételek megsértésének kivizsgálására és kezelésére vonatkozó eljárásokat.

11. Hivatkozott szabványok és keretrendszerek

11.1. ISO/IEC 27001

11.1.1. 5.10. pont – Előírja, hogy a szervezetek határozzák meg és érvényesítsék az információs eszközök elfogadható használatát.

11.2. ISO/IEC 27002

11.2.1. 5.10. kontroll – Iránymutatást ad a rendszerek elfogadható használatához, beleértve az engedélyezett és tiltott magatartásokat.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – A rendszerhasználat kontrolljaival foglalkozik, beleértve a saját tulajdonú eszközöket is.

11.3.2. AC-20 – Előírja a külső rendszerek engedélyezését és nyomon követését.

11.3.3. AT-2 – Hangsúlyozza a felhasználók képzését az elfogadható használati gyakorlatokra.

11.4. GDPR

11.4.1. 5. cikk (1) bekezdés f) pont – Előírja a személyes adatok sértetlenségét és bizalmasságát, amelyet a felhasználói helytelen használat veszélyeztethet.

11.4.2. 32. cikk – Előírja a rendszerek és adatok védelmét szolgáló technikai és szervezési intézkedések bevezetését.

11.5. NIS2 irányelv

11.5.1. 21. cikk (2) bekezdés b) pont – Megköveteli a megfelelő biztonsági szabályzatokat, ideértve az elfogadható használatra vonatkozó szabályokat is, a kiberfenyegetések mérséklése érdekében.

11.6. DORA-rendelet

11.6.1. 9. cikk – Előírja az IKT-kockázatkezelési szabályzatokat, amelyek a használati kontrollokat és végrehajtási mechanizmusokat is magukban foglalják.

11.7. COBIT 2019

11.7.1. DSS05 – Biztonsági szolgáltatások kezelése: hangsúlyozza a felhasználói magatartás szabályzatalapú kontrollját.

11.7.2. BAI08 – Tudás kezelése: foglalkozik a szabályzati felelősségi körök ismeretével és az elfogadható használatra vonatkozó oktatással.