					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P34S					Dokumentum címe: **Mobileszköz- és BYOD-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, 6.2, 8. pontok	Az IBIR általános, valamint a mobilhasználatra és a BYOD-ra vonatkozó kontrollkövetelményei
ISO/IEC 27002:2022	5.10–5.13. kontrollok	Részletes kontrollok a mobilhasználat, a BYOD és a távoli hozzáférés területén
NIST SP 800-53 Rev.5	AC-19, AC-20, CM-6, MP-7	Eszközökre, adathordozókra és konfigurációkra vonatkozó kontrollok
GDPR	5(1)(f) cikk	személyes adatok (PII) / mobil végpontok védelme
NIS2 irányelv	21(2)(d) cikk	üzletmenet-kritikus eszközök védelme, beleértve a BYOD-ot
DORA-rendelet	9., 10. cikk	IKT-kockázatkezelés és üzletmenet-folytonosság mobil végpontokra
COBIT 2019	APO13, DSS01, DSS05	IT-irányítási, üzemeltetési és biztonsági szolgáltatási kontrollok

1. cél

1.1. Jelen szabályzat meghatározza a vállalati információkhoz, rendszerekhez vagy szolgáltatásokhoz hozzáférő mobileszközök — ideértve az okostelefonokat, táblagépeket és laptopokat — használatára vonatkozó kötelező biztonsági követelményeket.

1.2. A szabályzat a BYOD (saját eszköz használata) alkalmazását is szabályozza annak érdekében, hogy az ügyfél- és üzleti adatok védelme az eszköz tulajdonosától függetlenül biztosított legyen.

1.3. A szabályzat egységes védelmi követelményeket ír elő a mobil hozzáférésre, támogatja az ISO/IEC 27001 tanúsítási célok teljesítését, valamint megelőzi az elveszett, ellopott vagy nem megfelelően használt mobil végpontokból eredő adatvesztést és kompromittálódást.

1.4. A szabályzat biztosítja, hogy a dedikált IT-csapattal nem rendelkező KKV-k esetében is alkalmazásra kerüljenek a mobilhasználatra vonatkozó technikai és eljárási védelmi intézkedések, beleértve a távmunka-környezeteket és a felhőszolgáltatásokat.

2. hatály

2.1. Jelen szabályzat az alábbi személyekre alkalmazandó: valamennyi munkavállaló, vállalkozó, gyakornok és szolgáltató, aki:

2.1.1. mobileszközt használ vállalati adatok vagy rendszerek elérésére, kezelésére vagy tárolására;

2.1.2. vállalati szolgáltatásokhoz kapcsolódik, ideértve az e-mailt, a megosztott mappákat, a felhőalkalmazásokat vagy a belső rendszereket VPN-en keresztül.

2.2. A szabályzat kiterjed:

2.2.1. valamennyi mobileszközre: okostelefonokra, táblagépekre és laptopokra (vállalati tulajdonú vagy BYOD-eszközök);

2.2.2. valamennyi operációs rendszerre (pl. iOS, Android, Windows, macOS);

2.2.3. valamennyi használati helyszínre (iroda, otthon, távoli helyszín, nyilvános tér).

2.3. A szabályzat valamennyi munkakörnyezetben alkalmazandó, és az eszköz tulajdonjogától függetlenül be kell tartani.

3. célkitűzések

3.1. Adatvesztés megelőzése: biztosítani kell, hogy a mobilhasználat ne tegye ki az érzékeny vállalati vagy ügyféladatokat jogosulatlan hozzáférésnek, eltulajdonításnak vagy visszaélésnek.

3.2. Egyértelmű BYOD-szabályok meghatározása: kikényszeríthető feltételeket kell meghatározni a saját eszközök üzleti célú használatára, biztosítva a jogi és technikai védelmi intézkedéseket.

3.3. Jogszabályi megfelelés támogatása: az ISO/IEC 27001, a GDPR, a NIS2 és az egyéb jogi kötelezettségek követelményeinek teljesítése kikényszeríthető mobilbiztonsági gyakorlatok útján.

3.4. Működési kockázat minimalizálása: csökkenteni kell a mobileszközök nem megfelelő használatából, kompromittálódásából vagy meghibásodásából eredő működési zavarok valószínűségét.

3.5. Ügyfélbizalom fenntartása: igazolni kell az ügyfelek és partnerek számára, hogy adataik mobil- vagy személyes eszközről történő hozzáférés esetén is védettek maradnak.

4. szerepkörök és felelősségek

4.1. Ügyvezető:

4.1.1. felelős jelen szabályzatért;

4.1.2. jóváhagyja a vállalati rendszerekhez történő valamennyi mobil- és BYOD-hozzáférést;

4.1.3. biztosítja, hogy a BYOD-megállapodások aláírása, megőrzése és nyomon követése megtörténjen;

4.1.4. ellenőrzi, hogy a külső IT-szolgáltatók alkalmazzák-e az előírt mobilbiztonsági védelmi intézkedéseket.

4.2. Kijelölt munkatárs vagy IT-támogatás:

4.2.1. támogatja a munkavégzéshez használt mobileszközök beállítását, regisztrációját és konfigurálását;

4.2.2. alkalmazza a mobileszközökhöz kapcsolódó hozzáférés-szabályozási intézkedéseket, alkalmazáskorlátozásokat és felügyeleti szabályokat;

4.2.3. támogatja a mobileszközökkel kapcsolatos incidenskezelést (elveszett, ellopott vagy kompromittálódott eszközök).

[... 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. az ügyvezető köteles jelen szabályzatot legalább 12 havonta egyszer felülvizsgálni.

9.1.2. A felülvizsgálat során ellenőrizni kell az ISO/IEC 27001 követelményeivel való folyamatos összhangot, a mobiltechnológiák változásait és az üzleti működésben bekövetkezett módosításokat.

9.1.3. A frissítések során figyelembe kell venni a közelmúltban történt incidenseket, az auditeredményeket és a szabályozási változásokat is (pl. GDPR, NIS2, DORA).

9.2. Soron kívüli felülvizsgálatot kiváltó események

9.2.1. Jelen szabályzatot haladéktalanul frissíteni kell, ha az alábbiak bármelyike bekövetkezik:

9.2.1.1. jelentős mobilbiztonsági incidens (pl. elveszett vagy feltört eszközön keresztüli adatsértés);

9.2.1.2. a támogatott platformok vagy mobilkezelő eszközök megváltozása;

9.2.1.3. a személyes eszközök használatát vagy az adatvédelmet érintő jogi vagy szabályozási változás;

9.2.1.4. mobileszközökön használt új alkalmazások, szolgáltatások vagy harmadik fél által biztosított eszközök bevezetése.

9.3. A változások dokumentálása

9.3.1. Minden felülvizsgálatot és frissítést dokumentálni kell, beleértve a felülvizsgálat dátumát, a végrehajtott módosításokat és az ügyvezető jóváhagyását.

9.3.2. Auditcélból meg kell őrizni a verziókövetési előzményeket.

9.4. Kommunikáció és hozzáférés

9.4.1. Az ügyvezető köteles biztosítani, hogy valamennyi felhasználó (munkavállalók, vállalkozók, harmadik felek) értesüljön a változásokról.

9.4.2. A frissített verziókat könnyen hozzáférhetővé kell tenni, például megosztott mappákban vagy belső platformokon.

10. kapcsolódó szabályzatok és összefüggések

10.1. Jelen szabályzat a KKV információbiztonsági szabályzati rendszerének részét képezi, és az alábbi szabályzatokkal együtt kell alkalmazni:

10.1.1. P4S – Hozzáférés-szabályozási szabályzat: meghatározza a rendszerekhez való biztonságos hozzáférés kezelésének követelményeit, beleértve a mobileszközökön keresztül elért rendszereket is. Előírja a biztonságos jelszóhasználatot és a munkamenet-védelmi intézkedéseket.

10.1.2. P8S – Információbiztonsági tudatossági és képzési szabályzat: biztosítja, hogy a felhasználók képzést kapjanak a mobileszközök biztonságos használatáról, az incidensjelentésről és a BYOD-feltételekről.

10.1.3. P17S – Adatvédelmi és magánszféra-védelmi szabályzat: meghatározza a személyes és vállalati adatok GDPR-nak megfelelő kezelését mobilplatformokon, különösen akkor, ha munkavégzéshez személyes eszközöket használnak.

10.1.4. P9S – Távmunka-szabályzat: összhangot biztosít a mobilhasználatra vonatkozó elvárásokkal telephelyen kívüli vagy otthoni munkavégzés esetén, beleértve az eszközkezelést és a hálózati hozzáférés védelmi intézkedéseit.

10.1.5. P30S – Incidenskezelési szabályzat: meghatározza a mobileszközökkel kapcsolatos incidensek — beleértve a kompromittálódott vagy elveszett eszközöket — kezelésének keretrendszerét.

10.2. Ezek a kapcsolódó szabályzatok együtt alkotják a dedikált IT-személyzettel nem rendelkező KKV-k mobileszköz-biztonságának teljes kontrollrendszerét, biztosítva a kikényszeríthetőséget, az átláthatóságot és az auditra való felkészültséget.

11. hivatkozott szabványok és keretrendszerek

11.1. Jelen szabályzat az alábbi biztonsági és megfelelési szabványokkal való teljes összhangot támogatja:

11.2. ISO/IEC 27001:

11.2.1. 5.1. pont – Vezetés és elkötelezettség: biztosítja a vezetői felügyeletet és az elszámoltathatóságot a mobil- és BYOD-hozzáférés tekintetében.

11.2.2. 6.1. pont – A kockázatok kezelését célzó intézkedések: előírja a mobilbiztonsági kockázatok értékelését és kezelését.

11.2.3. 8.1. pont – Működéstervezés és -szabályozás: egységes mobilhozzáférési eljárásokat követel meg az üzleti adatok védelme érdekében.

11.3. ISO/IEC 27002:

11.3.1. 5.10. (Mobileszközök használata), 5.11. (Távmunka), 5.12. (Távoli hozzáférés) és 5.13. (BYOD) kontrollok: megvalósítási iránymutatást adnak az eszközkockázatok kezeléséhez kisvállalati környezetben.

11.4. NIST SP 800-53 Rev.5:

11.4.1. AC-19 – Hozzáférés-szabályozás mobileszközökhöz: biztonsági beállításokat ír elő az engedélyezett mobilhasználathoz.

11.4.2. AC-20 – Külső rendszerek használata: szabályozza a BYOD-hoz és a távoli hozzáféréshez kapcsolódó kockázatokat.

11.4.3. CM-6 – Konfigurációs beállítások: előírja a biztonságos alapértelmezett és egyedi beállítások alkalmazását mobilplatformokon.

11.4.4. MP-7 – Adathordozók használata: meghatározza a mobil tárolók és az adathozzáférés megfelelő használatát és korlátozásait.

11.5. GDPR (2016/679):

11.5.1. 5(1)(f) cikk – sértetlenség és bizalmas jelleg: előírja a személyes adatok megfelelő biztonság útján történő védelmét, különösen mobilplatformokon.

11.5.2. 32. cikk – Az adatkezelés biztonsága: kötelezővé teszi a mobileszközökön elért vagy tárolt adatok védelméhez szükséges megfelelő technikai és szervezési intézkedések alkalmazását.

11.6. NIS2 irányelv (2022/2555):

11.6.1. 21(2)(d) cikk – eszközbiztonsági intézkedések: előírja a kritikus üzleti rendszerekhez való hozzáféréshez használt hardverek és szoftverek — beleértve a személyes eszközöket is — biztonsági kontrolljait.

11.7. DORA-rendelet (2022/2554):

11.7.1. 9. cikk – IKT-kockázatkezelési keretrendszer: előírja az üzletmenet-kritikus üzleti kommunikációhoz és felhőszolgáltatásokhoz használt mobil végpontok védelmét.

11.7.2. 10. cikk – IKT-üzletmenet-folytonosság: előírja az üzleti rendszerekhez való folyamatos és biztonságos hozzáférés biztosítását zavarok vagy távmunka esetén is.

11.8. COBIT 2019:

11.8.1. APO13 – Biztonság kezelése: előírja, hogy a szervezet a vállalati kockázatokhoz igazodó mobil- és BYOD-szabályzatokat alkalmazzon.

11.8.2. DSS01 – Üzemeltetés kezelése: biztosítja a biztonságos hozzáférési mechanizmusok technikai megvalósítását.

11.8.3. DSS05 – Biztonsági szolgáltatások kezelése: szabályozza a harmadik felek részvételét a biztonságos mobilkörnyezetek fenntartásában és az incidenskezelés koordinációjában.