					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P34					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**

Jogi nyilatkozat (szerzői jog és felhasználási korlátozások)

(C) 2025 Clarysec LLC. All rights reserved.

Ez a dokumentum a Clarysec LLC szellemi tulajdona. A dokumentum semmilyen része nem másolható, nem használható fel újra, nem terjeszthető és nem módosítható kereskedelmi vagy bevezetési célból előzetes, kifejezett írásbeli engedély nélkül.

A jogosulatlan felhasználás szigorúan tilos, és jogi eljárást vonhat maga után.

Licenceléssel kapcsolatban keresse: info@clarysec.com

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	5.2, 6.1, 7.5, 8	Biztonsági kontrollok és megfelelőségi követelmények alkalmazása
ISO/IEC 27002:2022	5.10, 8.1, 8.5, 8	Részletes kontrollokat biztosít a mobileszköz-kezeléshez
NIST SP 800-53 Rev.5	AC-19, AC-17, CM-7, MP-5, SC-12	Hozzáférés-szabályozási, távoli hozzáférési, konfigurációs és biztonsági követelmények mobileszközökre
GDPR	5. cikk (1) bekezdés f) pont, 25. cikk, 32. cikk	Kötelező adatvédelmi, adattitkosítási és adatkezelés-biztonsági követelmények
NIS2 irányelv	21. cikk (2) bekezdés d) pont	A mobil hozzáférés technikai és szervezeti védelmi intézkedései
DORA-rendelet	9. cikk, 10. cikk	IKT-kockázatkezelési és mobileszközökre vonatkozó biztonsági követelmények
COBIT 2019	APO13.02, DSS01.04, BAI09	Információbiztonsági tervek, eszközkonfiguráció és mobil környezetekre vonatkozó kontrollok

1. Cél

1.1 Jelen szabályzat meghatározza a mobileszközök és a személyes technológiai eszközök BYOD (saját eszköz használata) keretében történő használatára vonatkozó biztonsági, megfelelőségi és működési követelményeket, amennyiben azok a szervezet rendszereihez, alkalmazásaihoz vagy adataihoz férnek hozzá.

1.2 A szabályzat célja annak biztosítása, hogy az okostelefonokon, táblagépeken, laptopokon és hibrid eszközökön keresztül elért vagy kezelt vállalati információk bizalmassága, sértetlensége és rendelkezésre állása fennmaradjon.

1.3 A szabályzat egyúttal előírja azokat a technikai és eljárási kontrollokat, amelyek szükségesek az olyan kockázatok csökkentéséhez, mint az adatszivárgás, az illetéktelen hozzáférés, az eszköz elvesztése vagy eltulajdonítása, illetve a mobilalkalmazások kompromittálódása.

1.4 Jelen szabályzat támogatja a jogszabályi és szerződéses megfelelést, miközben lehetővé teszi a munkavállalók, vállalkozók és engedélyezett harmadik felek számára a biztonságos mobil munkavégzést.

2. Hatály

2.1 Jelen szabályzat valamennyi munkatársra kiterjed — ideértve a munkavállalókat, vállalkozókat, gyakornokokat és harmadik fél szolgáltatókat —, akik mobileszközt használnak a vállalati adatokhoz, rendszerekhez, alkalmazásokhoz vagy kommunikációs platformokhoz való hozzáféréshez.

2.2 A szabályzat minden mobil számítástechnikai eszközre kiterjed, beleértve többek között az alábbiakat:

2.2.1 Okostelefonok és táblagépek (iOS, Android stb.)

2.2.2 Laptopok és ultrabookok (Windows, macOS, Linux)

2.2.3 Adatszinkronizálásra képes viselhető eszközök és hibrid intelligens eszközök

2.3 A szabályzat attól függetlenül alkalmazandó, hogy az eszköz vállalati tulajdonban van, vagy BYOD-megállapodás alapján személyes tulajdonú eszköz.

2.4 A szabályzat minden hozzáférési csatornára kiterjed, beleértve a VPN-t, a virtuális asztali infrastruktúrát, a felhőalapú alkalmazásokat, az e-mailt, az együttműködési platformokat (pl. SharePoint, Teams), valamint a fájlszinkronizálási eszközöket (pl. OneDrive, Dropbox, amennyiben engedélyezettek).

2.5 A szabályzat alkalmazandó távmunkában, helyszíni munkavégzés során, utazás közben, valamint hibrid munkavégzési megállapodások esetén is.

3. Célkitűzések

3.1 Annak kockázatának csökkentése, hogy a nem biztonságos mobileszköz-használat miatt adatok kompromittálódjanak, kiszivárogjanak vagy elveszjenek.

3.2 Következetes és betartható biztonsági kontrollok alkalmazása valamennyi mobil végponton, a tulajdonosi modelltől függetlenül (vállalati vagy BYOD).

3.3 Annak biztosítása, hogy a mobileszköz-használat megfeleljen az ISO/IEC 27001 és az adatvédelemre, adatbiztonságra és kiberbiztonságra vonatkozó egyéb alkalmazandó szabályozási keretrendszerek követelményeinek.

3.4 A mobileszközök biztonságos integrációjának elősegítése a szervezet működési, kommunikációs és együttműködési folyamataiba.

3.5 Egyértelműen meghatározott felelősségi körök és folyamatok biztosítása a mobileszköz-kezeléshez (MDM), ideértve a nyilvántartásba vételt, a távoli törlést, a titkosítást, a hitelesítést és a nyomon követést.

3.6 A saját eszközt használó személyek adatvédelmi jogainak védelme a szervezet érzékeny információinak egyidejű megóvása mellett.

4. Szerepkörök és felelősségek

4.1 Információbiztonsági vezető / IT-biztonsági vezető

4.1.1 Meghatározza a mobil- és BYOD-használatra vonatkozó szabályzatot és technikai szabványokat.

4.1.2 Felügyeli a mobileszköz-kontrollok megfelelőségét, az incidenskezelést és a kivételkezelést.

4.1.3 Együttműködik a jogi és HR-csapatokkal annak biztosítása érdekében, hogy a szabályzat alkalmazása jogilag megalapozott és szervezeti szinten összehangolt legyen.

4.2 IT-rendszergazda / MDM-adminisztrátor

4.2.1 Kezeli a mobileszközök hozzáférésének létrehozását, nyilvántartásba vételét és konfigurálását MDM-megoldásokon keresztül.

4.2.2 Érvényesíti az eszközszintű kontrollokat (pl. titkosítás, PIN-kódok, alkalmazáskontrollok).

4.2.3 Szükség esetén végrehajtja a távoli törlést, az eszköz zárolását és a hozzáférés visszavonását.

[... 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 Jelen szabályzatot legalább évente felül kell vizsgálnia az információbiztonsági vezetőnek vagy a kijelölt személynek annak biztosítása érdekében, hogy összhangban legyen az alábbiakkal:

9.1.1 A mobil operációs rendszerek, MDM-technológiák vagy hitelesítési szabványok változásai

9.1.2 A mobil adatvédelemre hatással lévő jogszabályi vagy szerződéses változások (pl. GDPR, DORA, NIS2)

9.1.3 Az ISO/IEC 27001:2022, az ISO/IEC 27002:2022 vagy a NIST SP 800-53 Rev.5 kontrollkészleteinek módosításai

9.1.4 Auditokból, incidens utáni értékelésekből vagy munkavállalói bejelentésekből származó visszajelzések

9.2 Soron kívüli felülvizsgálatot válthat ki:

9.2.1 Mobileszközöket vagy BYOD-platformokat érintő biztonsági incidens

9.2.2 Beszállítói értesítés a támogatott platformokat érintő magas kockázatú sérülékenységekről

9.2.3 Új, üzleti működéshez használt mobilalkalmazások vagy együttműködési platformok bevezetése

9.3 A szabályzat frissítéseit:

9.3.1 Dokumentálni kell a szabályzat verzióelőzményeiben

9.3.2 Kommunikálni kell valamennyi munkatárs és érintett vállalkozó részére

9.3.3 Meg kell erősíttetni frissített tudomásulvétellel valamennyi BYOD-felhasználóval

9.4 Valamennyi felülvizsgálatot és módosítást formálisan jóvá kell hagynia a felső vezetésnek, és azokat rögzíteni kell a szabályzatváltozási nyilvántartásban.

10. Kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat a szervezet IBIR-keretrendszerének több kulcsfontosságú szabályzatával is kölcsönös függőségben áll. A legfontosabb kapcsolódások:

10.1.1 P1 – Információbiztonsági szabályzat: Meghatározza az összes információbiztonsági kontrollra vonatkozó átfogó irányítási alapelveket, beleértve a mobileszköz-használatot szabályozó kontrollokat is.

10.1.2 P3 – Elfogadható használati szabályzat: Meghatározza a technológiahasználathoz kapcsolódó megengedett magatartásokat és korlátozásokat, amelyek közvetlenül alkalmazandók a mobil- és BYOD-hozzáférésre.

10.1.3 P9 – Távmunka-szabályzat: A mobil munkakörnyezetekre vonatkozó további biztonsági kötelezettségeket szabályozza, kiegészítve a jelen szabályzatban meghatározott mobileszköz-specifikus kontrollokat.

10.1.4 P13 – Adatosztályozási és címkézési szabályzat: Szabályozza, hogy a mobileszközökön kezelt adatokat az osztályozási szintjük alapján hogyan kell kezelni, ami hatással van a tárolásra, továbbításra és a titkosítás érvényesítésére.

10.1.5 P22 – Naplózási és felügyeleti szabályzat: Támogatja a mobil hozzáférések naplóinak gyűjtését és felülvizsgálatát az anomáliák vagy szabálysértések észlelése érdekében.

10.1.6 P30 – Incidenskezelési szabályzat: Szabályozza a mobilitással kapcsolatos incidensek (pl. eszközelvesztés, jogosulatlan hozzáférés) kezelését és eszkalációját.

10.1.7 P33 – Audit- és megfelelőségfelügyeleti szabályzat: Alapot biztosít a mobilbiztonsági megfelelés időszakos ellenőrzéséhez, beleértve a BYOD-szabályzat betartását is.

11. Hivatkozott szabványok és keretrendszerek

11.1 Jelen szabályzat összhangban áll a nemzetközileg elismert kiberbiztonsági keretrendszerekkel és jogi kötelezettségekkel annak érdekében, hogy biztosítsa a mobileszközök és a személyes BYOD-technológiák biztonságos használatát vállalati környezetben.

11.2 ISO/IEC 27001:

11.2.1 5.10 pont – Az információk és egyéb kapcsolódó eszközök elfogadható használata: Előírja a vállalati eszközök — ideértve a mobileszközöket is — felelős használatára vonatkozó kontrollokat.

11.2.2 5.11 pont – Eszközök visszaszolgáltatása: Szabályozza a szervezeti eszközök visszaadására vonatkozó követelményeket, beleértve a mobil eszközök kezeléséhez kapcsolódó kötelezettségeket is.

11.2.3 5.12 pont – Információk osztályozása: Előírja, hogy a mobileszközökön kezelt információkat azok osztályozása alapján kell védeni.

11.2.4 5.13 pont – Információk címkézése: Előírja az információk megfelelő jelölését, amely támogatja a mobileszközökön kezelt adatok biztonságos kezelését.

11.3 ISO/IEC 27002:2022 – 5.10–5.13 kontrollok:

11.3.1 Az 5.10–5.13 kontrollok meghatározzák, hogyan kell az információk és eszközök elfogadható használatát, visszaszolgáltatását, osztályozását és címkézését egy információbiztonság-irányítási rendszer (ISMS) keretében érvényesíteni. E kontrollok részletes végrehajtási iránymutatást adnak a mobil végpontok védelméhez, a konténerizáció érvényesítéséhez, az eszközök sértetlenségének monitorozásához és a BYOD-használat során adatvédelmi szempontból megfelelő konfigurációk biztosításához.

11.4 NIST SP 800-53 Rev.5:

11.4.1 AC-19 – Mobileszközökre vonatkozó hozzáférés-szabályozás: Meghatározza az alapvető védelmi intézkedéseket, beleértve a titkosítást, a hitelesítést és az MDM érvényesítését.

11.4.2 AC-17 – Távoli hozzáférés: Előírja a biztonságos hitelesítést és a munkamenet-védelmi intézkedéseket a távoli mobilfelhasználók számára.

11.4.3 CM-7 – Minimálisan szükséges funkcionalitás: Támogatja a szükségtelen alkalmazások és funkciók eltávolítását a mobil végpontokról a kockázat csökkentése érdekében.

11.4.4 MP-5 – Adathordozók szállításának védelme: Szabályozza az adatok biztonságos továbbítását mobil rendszerekből külső vagy felhőalapú célállomások felé.

11.4.5 SC-12 – Kriptográfiai kulcsok létrehozása és kezelése: Előírja a biztonságos kriptográfiai protokollok használatát a mobil kommunikáció és tárolás során.

11.5 GDPR (2016/679):

11.5.1 5. cikk (1) bekezdés f) pont – Sértetlenség és bizalmas jelleg: Előírja, hogy a szervezeteknek védeniük kell a mobileszközökön kezelt személyes adatokat az illetéktelen vagy jogellenes hozzáféréssel szemben.

11.5.2 25. cikk – Beépített és alapértelmezett adatvédelem: Előírja, hogy az adatvédelmet a BYOD- és MDM-folyamatokba be kell építeni.

11.5.3 32. cikk – Az adatkezelés biztonsága: Kockázatalapú kontrollokat (pl. titkosítás, hitelesítés, hozzáférés-szabályozás) ír elő a mobil platformokon kezelt személyes adatok védelmére.

11.6 NIS2 irányelv (2022/2555):

11.6.1 21. cikk (2) bekezdés d) pont: Előírja, hogy a kritikus rendszerekhez és információkhoz való mobil hozzáférést megfelelő technikai és szervezeti intézkedésekkel kell védeni, például végponti kontrollokkal, titkosítással és monitorozással.

11.7 DORA-rendelet (2022/2554):

11.7.1 9. cikk – IKT-kockázatkezelési keretrendszer: Előírja, hogy a pénzügyi szektor szervezeteinek az operatív reziliencia részeként csökkenteniük kell a mobil- és távoli hozzáférésből eredő kockázatokat.

11.7.2 10. cikk – IKT-rendszerekre vonatkozó biztonsági követelmények: Biztonságos mobilarchitektúrát, monitorozási és reagálási mechanizmusokat követel meg a mobil eredetű kiberfenyegetésekkel szemben.

11.8 COBIT 2019:

11.8.1 APO13.02 – Információbiztonsági terv kialakítása és fenntartása: Előírja, hogy a mobileszköz-használatot, beleértve a BYOD-ot is, integrálni kell a szervezet biztonsági stratégiáiba.

11.8.2 DSS01.04 – Eszközkonfiguráció és sértetlenség kezelése: Alkalmazandó a mobileszközök konfigurációszabályozására és biztonságos bevezetésére.

11.8.3 BAI09.01 – Kontrollok kialakítása és fenntartása: Támogatja a technikai és eljárási védelmi intézkedések bevezetését a biztonságos mobil- és távoli működés érdekében.