					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P32S					Dokumentum címe: **Üzletmenet-folytonossági és katasztrófa utáni helyreállítási 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	6.1, 6.3, 8. pont	
ISO/IEC 27002:2022	5.29, 5.30 kontroll	
NIST SP 800-53 Rev.5	CP-2, CP-4, CP-6, CP-7	
GDPR	32., 33. cikk	
NIS2 irányelv	21. cikk (2) bekezdés f) pont	
DORA-rendelet	10. cikk	
COBIT 2019	DSS	

1. cél

1.1 Jelen szabályzat biztosítja, hogy a szervezet képes legyen üzleti működésének fenntartására és a létfontosságú IT-szolgáltatások helyreállítására olyan működési zavarok során és azt követően, mint az áramkimaradás, a kibertámadás, a zsarolóvírus-fertőzés vagy a rendszerhiba.

1.2 A szabályzat egyértelmű keretet biztosít az üzletmenet-folytonossági és katasztrófa utáni helyreállítási (BC/DR) tervezéshez, különös tekintettel a dedikált IT-csapattal nem rendelkező KKV-kra.

1.3 Jelen szabályzat támogatja a szervezetet az ISO/IEC 27001:2022, a GDPR, a NIS2, a DORA és a COBIT 2019 szerinti kötelező követelmények teljesítésében, miközben erősíti a működési rezilienciát és az ügyfélbizalmat.

2. hatály

2.1 Jelen szabályzat az alábbiakra terjed ki:

2.1.1 valamennyi üzletmenet-kritikus rendszerre és szolgáltatásra (pl. e-mail, felhőszolgáltatásokban tárolt fájlok, számlázási platformok, ügyfélnyilvántartások)

2.1.2 valamennyi munkavállalóra és külső IT-szolgáltatóra, akik felelősek a BC/DR-felkészültségért és annak végrehajtásáért

2.1.3 a működési zavarok valamennyi típusára, beleértve a kiberbiztonsági incidenseket, hardverhibákat, áramkimaradást, elárasztást és az iroda megközelíthetetlenségét

2.2 A szabályzat az alábbi területekre terjed ki:

2.2.1 biztonsági mentések kezelése

2.2.2 üzletmenet-folytonossági tervezés (BCP)

2.2.3 katasztrófa utáni helyreállítási műveletek

2.2.4 munkatársi képzés és tesztelés

2.2.5 jogi és szabályozási válaszeljárások

3. célkitűzések

3.1 A szervezet kulcsszolgáltatásainak fenntartása nem tervezett működési zavarok esetén is.

3.2 A rendszerek és adatok időben történő helyreállításának biztosítása előre meghatározott helyreállítási időcélokkal (RTO).

3.3 Annak biztosítása, hogy valamennyi munkatárs válsághelyzetben minimális bizonytalanság mellett tudja követni a folytonossági eljárásokat.

3.4 Az adatvédelemre és a működési rezilienciára vonatkozó jogszabályi megfelelés fenntartása, beleértve a GDPR 32. cikkét és a NIS2 21. cikkét.

3.5 A KKV-k számára megfelelő, gyakorlatban alkalmazható és tesztelhető folytonossági és helyreállítási stratégia kialakítása.

4. szerepkörök és felelősségek

4.1 ügyvezető

4.1.1 Felelős a BC/DR-folyamatért és jelen szabályzat végrehajtásáért.

4.1.2 Jóváhagyja az üzletmenet-folytonossági tervet (BCP).

4.1.3 A működési zavarok idején koordinálja az incidenskezelést és a belső kommunikációt.

4.1.4 Gondoskodik a szükséges hatósági bejelentésekről (pl. GDPR szerinti incidensbejelentések).

4.2 külső IT-szolgáltató / rendszergazda

4.2.1 Fenntartja és teszteli a biztonsági mentéseket.

4.2.2 Aktiválás esetén végrehajtja a katasztrófa utáni helyreállítási eljárásokat.

4.2.3 Dokumentál minden helyreállítási intézkedést és rendszer-visszaállítási eseményt.

4.2.4 A kritikus IT-incidenseket haladéktalanul jelenti az ügyvezetőnek.

[... 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 A szabályzat és a terv éves felülvizsgálata

9.1.1 Az ügyvezetőnek biztosítania kell, hogy jelen szabályzatot és a kapcsolódó üzletmenet-folytonossági tervet (BCP) évente legalább egyszer formálisan felülvizsgálják.

9.1.2 A felülvizsgálatnak ki kell terjednie az alábbiakra:

9.1.2.1 az új vagy kialakulóban lévő kockázatok értékelésére

9.1.2.2 az RTO-k és RPO-k ismételt megerősítésére

9.1.2.3 a beszállítói és kapcsolattartási információk ellenőrzésére

9.1.2.4 annak vizsgálatára, hogy a szabályzat összhangban áll-e az IT-rendszerekben, a jogi kötelezettségekben vagy a működésben bekövetkezett változásokkal

9.2 Eseményalapú frissítések

9.2.1 E szabályzatot az alábbi esetekben is frissíteni kell:

9.2.1.1 jelentős incidensek vagy működési zavarok után, különösen akkor, ha a célkitűzések nem teljesültek

9.2.1.2 új jogi vagy szabályozási kötelezettségek esetén (pl. DORA-módosítások)

9.2.1.3 kritikus rendszerekben, felhőplatformokban vagy a személyi állományban bekövetkező változások esetén

9.2.1.4 az éves BCP/DR-tesztek megállapításai alapján

9.3 Változáskezelési folyamat

9.3.1 Minden módosítást az ügyvezetőnek kell jóváhagynia.

9.3.2 Változáselőzmény-nyilvántartást kell vezetni, amely tartalmazza a dátumot, a módosítás leírását és a jóváhagyó személyét.

9.3.3 A frissített szabályzatot minden érintett részére ismételten ki kell adni, beleértve a külső IT-szolgáltatót és a szervezeti egység vezetőit.

9.4 A levont tanulságok dokumentálása

9.4.1 A teszteket vagy valós működési zavarokat követően dokumentált tanulságokat be kell építeni a jövőbeli módosításokba.

9.4.2 E felülvizsgálatoknak ki kell terjedniük a beszállítói teljesítmény értékelésére és a válaszintézkedések megfelelőségének ellenőrzésére is.

10. kapcsolódó szabályzatok és összefüggések

10.1 Jelen szabályzat szorosan kapcsolódik az alábbi KKV-szabályzatokhoz:

10.1.1 P1S – Információbiztonsági szabályzat: meghatározza azokat a magas szintű biztonsági célkitűzéseket, amelyeket a folytonossági és helyreállítási gyakorlatoknak támogatniuk kell.

10.1.2 P4S – Hozzáférés-szabályozási szabályzat: lehetővé teszi a felhasználói hozzáférések vészhelyzeti visszavonását vagy helyreállítását üzleti működési zavarok esetén.

10.1.3 P6S – Kockázatkezelési szabályzat: alapot ad a folytonossághoz kapcsolódó kockázatok azonosításához, értékeléséhez és priorizálásához.

10.1.4 P8S – Információbiztonsági tudatossági és képzési szabályzat: biztosítja, hogy a munkavállalók felkészülten reagáljanak a működési zavarokra, és ismerjék a BCP-t.

10.1.5 P15S – Biztonsági mentési és helyreállítási szabályzat: konkrét technikai eljárásokat ír elő az adatok rendelkezésre állásának és helyreállíthatóságának biztosítására.

10.1.6 P17S – Adatvédelmi és magánszféra-védelmi szabályzat: biztosítja, hogy a folytonossági tervezés tiszteletben tartsa a személyes adatok védelmét, és az incidensek során és azt követően is megfeleljen a GDPR-nak.

10.1.7 P22S – Naplózási és felügyeleti szabályzat: támogatja azon események észlelését, amelyek kiválthatják a BC/DR-folyamatokat, valamint a működési zavarokat követően forenzikai auditnyomot biztosít.

10.1.8 P30S – Incidenskezelési szabályzat: közvetlenül megelőzi a helyreállítási folyamat aktiválását kiberbiztonsági vagy működési incidensek esetén.

10.1.9 P31S – Bizonyítékgyűjtési és forenzikai szabályzat: biztosítja a digitális bizonyítékok rögzítését a folytonossági helyzetek során megfelelőségi, biztosítási vagy vizsgálati célból.

10.2 E szabályzatok együttesen egységes, auditkészültséget támogató keretrendszert alkotnak a reziliencia, az elszámoltathatóság és a kontrollok folytonosságának biztosítása érdekében a KKV teljes működésében.

11. hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001:

11.1.1 A 6.1. pont előírja a kockázatalapú tervezést és kockázatkezelést, beleértve az üzletmenet-folytonosságot és a helyreállítást.

11.1.2 A 6.3. pont hangsúlyozza a folyamatos fejlesztést a működési zavarokat követően.

11.1.3 A 8.1. pont operatív kontrollokat ír elő, amelyek magukban foglalják a dokumentált folytonossági intézkedéseket is.

11.2 ISO/IEC 27002:

11.2.1 Az 5.29. kontroll előírja az üzletmenet-folytonossági intézkedések kialakítását és fenntartását.

11.2.2 Az 5.30. kontroll előírja ezen intézkedések tesztelését és felülvizsgálatát.

11.3 NIST SP 800-53 Rev.5:

11.3.1 A CP-2 meghatározza a vészhelyzeti tervezés követelményeit.

11.3.2 A CP-4 előírja a szervezeti munkatársak vészhelyzeti képzését.

11.3.3 A CP-6 az alternatív tárolási helyszínek követelményeit szabályozza.

11.3.4 A CP-7 az alternatív feldolgozási helyszínekre vonatkozó elvárásokat szabályozza.

11.4 GDPR:

11.4.1 A 32. cikk olyan intézkedéseket ír elő, amelyek biztosítják az adatkezelési rendszerek és szolgáltatások folyamatos rendelkezésre állását és rezilienciáját.

11.4.2 A 33. cikk incidensbejelentési kötelezettséget keletkeztet azokban az esetekben, amikor a folytonosság hiányossága a személyes adatok kompromittálódásához vezet.

11.5 NIS2 irányelv (2022/2555):

11.5.1 A 21. cikk (2) bekezdés f) pontja előírja az üzletmenet-folytonossági tervezést és a válságkezelési képességeket mint a kiberkockázati felkészültség feltételeit.

11.6 DORA-rendelet (2022/2554):

11.6.1 A 10. cikk előírja a digitális működési reziliencia tesztelésének és a helyreállítási képességek bevezetését, különösen a pénzügyi szektorban működő KKV-k számára.

11.7 COBIT 2019:

11.7.1 A DSS04 – üzletmenet-folytonosság kezelése vállalatirányítási útmutatást ad a működési reziliencia fenntartására és ellenőrzésére, beleértve a felelősségi rendet, a tesztelést, a beszállítói integrációt és az eseményt követő felülvizsgálatokat.