ÜZLETMENET-FOLYTONOSSÁGI TERV (BCP)

	Név	Aláírás	Dátum
Ellenőrizte:	**Molnár Tímea**		**2021.02.24.**
Jóváhagyta:	**Rajkai György**		**2021.02.24.**

Tartalom

AZ ÜZLETMENET-FOLYTONOSSÁGI TERV CÉLJA

Az üzletmenet folytonossági terv (továbbiakban: **BCP**) készítésének az a célja, hogy kezelni tudja azokat a helyzeteket, amikor az üzleti folyamatokat kiszolgáló erőforrások átfogó sérülése miatt az üzleti folyamatok folyamatos és rendeltetésszerű működése megszakad. Ez azt jelenti, hogy a BCP alapvetően nem a katasztrófa bekövetkezési valószínűségét, hanem – a kritikus folyamatok folytonosságának biztosítása révén – a lehetséges kárkövetkezményeket csökkenti.

A BCP-ben rögzített katasztrófa-elhárítási feladatok a következők szerint vannak csoportosítva:

1. Katasztrófa előtti feladatok, amikor a szervezet megteszi a felkészüléshez szükséges intézkedéseket (felkészülési fázis); az itt felsorolt feladatok végrehajtásával biztosítja a szervezet, hogy teljesíti a vezetők és tulajdonosok által megfogalmazott folytonossági elvárásokat, a kritikus üzleti folyamatok visszaállítását a meghatározott időtartamon belül.
2. Katasztrófa utáni feladatok, amikor a szervezet mozgósítja embereit (válasz fázis), és megkezdi az üzleti folyamatok újraindítását (visszaállítási fázis), majd a normális állapot helyreállítását (helyreállítási fázis).
3. A válasz fázis során történik a katasztrófa felismerése, az érintettek riasztása, az emberi élet és az eszközök mentése. Előzetes helyzetértékelés alapján kihirdetésre kerül a katasztrófa. Az érintettek tájékoztatást kapnak a kialakult helyzetről.
4. A visszaállítás az ideiglenes – általában alternatív helyszínen történő – folyamatműködtetést, a helyreállítás pedig a normális üzletmenetre való visszatérést jelenti.

A BCP nem foglalkozik azokkal a folyamatokkal, amelyek nem befolyásolják közvetlenül, kritikus jelleggel a szervezet működését, sebezhetőségi ablaka nagyobb, mint a 4. fejezetben meghatározott leghosszabb időtartam és ezáltal kijelenthető, hogy ezen folyamatok kiesése működésére nézve nem kritikus.

Ellenben foglalkozik azokkal a kulcsfolyamatokat érintő eseményekkel, amelyek közvetlenül, kritikus jelleggel befolyásolhatják a cég stratégiájában megfogalmazott célok megvalósítását, a célok elérését.

A BCP a szervezet egészére kiterjedő veszélyforrásokkal is foglalkozik, oly mértékben, hogy feltételezi, hogy nem a teljes (emberi erőforrások, fizikai és informatikai környezet) semmisül meg. A terv mindezek mellet érinti azokat a veszélyforrásokat, amelyek alapvetően működési, üzemeltetési jellegűek és a probléma megoldása a normális üzletvitel keretein belül, akár külső fél segítségével is megoldható.

1. Kulcsfolyamatok és kulcsterületek meghatározása:

Kulcsterületek: cégvezetés, operatív vezetés, IT vezetés, partnerkapcsolatok, emberi erőforrások és technikai működtetési területek.

⇒ **Cégvezetés**: cég működésének tervezése, felügyelete, célok, stratégiák meghatározása

⇒ **Operatív vezetés**: munkakoordinálás az adott területen, közvetítés a munkatársak és cégvezetés között, kapcsolattartás a partnerekkel, szolgáltatási folyamat nyomonkövetése

⇒ **IT vezetés**: a cég szoftverfejlesztési és üzemeltetési üzletágának a koordinálása, közvetítés a munkatársak és a cégvezetés között, kapcsolattartás a partnerekkel, szolgáltatási folyamat biztosítása és nyomonkövetése

⇒ **Partnerkapcsolatok** (vevők): kommunikáció, szolgáltatás nyújtása a partnereknek, rendelkezésre állás

⇒ **Beszállító partnerek**: szolgáltatások folyamatos nyújtása, eszközök biztosítása, kapcsolattartás

⇒ **Emberi erőforrásokkal való gazdálkodás**: új dolgozó oktatása, folyamatos továbbképzés, dolgozók magas szintű munkakörülményeinek biztosítása, munkaerő rendelkezére állása

⇒ **Cég technikai működtetése**: informatikai rendszerek, kommunikációs eszközök, infrastruktúra működése

A TERV VÉGREHAJTÁSÁBAN ÉRINTETT SZEREPKÖRÖK, FELADAT- ÉS HATÁSKÖRÖK

Feladatok		Szerepkörök / hatáskör			
Ssz	**Lépés**	**Válságstáb vezetője**	**Válságstáb**	**Rendszergazda**	**Munkatársak**
I.	Válságstáb munkájának a koordinálása	Végrehajt	-	-	-
II.	Erőforrások biztosítása	Dönt	Végrehajt	-	-
III.	Katasztrófa helyzet kihírdetése	Dönt	-	-	-
IV.	Külső, belső kommunikáció	Dönt	Végrehajt	-	-
V.	Feladatok meghatározása és ellenőrzése	-	Dönt	Végrehajt	Végrehajt
VI.	Elemzés és további intézkedések meghozatala	-	Dönt	Végrehajt	Végrehajt

A válságstáb vezetője: Rajkai György vezérigazgató

Helyettese: Buchwald Imre vezérigazgató helyettes

A válságstáb tagjai: Molnár Tímea irodavezető

HÁTTÉRSTRATÉGIÁK

Az egyes erőforrás típusokhoz kapcsolódóan az alábbi háttérstratégiákat határozzuk meg:

Irodai háttérstratégia

Erőforrás típus	Iroda helyiség (Maros utca 23., Budapest)
Háttérstratégia	Katasztrófa helyzetben álljon rendelkezésre egy másik iroda, ahol a válságstáb össze tud ülni, illetve az irányítási funkciók fenntarthatók.
Háttérstratégia alkalmazásának a feltétele	Rendszeres adatmentés, adathordozók biztonságos tárolása az irodán kívül + felhőben. A távmunka lehetősége biztosított legyen.

IT erőforrások háttér stratégiája

Erőforrás típus	Speciális IT erőforrások
Háttérstratégia	Háttér-infrastruktúra biztosítása
Háttérstratégia alkalmazásának a feltétele	Rendelkezésre áll a visszaállítási terv ami a speciális IT erőforrásokra vonatkozik, és a megfelelő szállítói kapcsolat. Adatmentések és kapcsolódó eljárási rendek és dokumentációk is rendelkezésre állnak.

Erőforrás típus	INTEGRA CAFM erőforrások
Háttérstratégia	Folyamatos monitoring és kockázatok feltárása
Háttérstratégia alkalmazásának a feltétele	⇒ az alkalmazás rendszeres biztonsági felülvizsgálata, szükség szerint a feltárt biztonsági kockázatok javítása ⇒ alkalmazáson belüli hibanaplók rendszeres elemzése ⇒ frissítésre szoruló komponensek listájának továbbítása az üzemeltetés felé ⇒ veszélyhelyzet keletkezésekor, az alkalmazáson belüli, azonnali beavatkozást igénylő változtatások, javítások elvégzése ⇒ üzemeltetéstől kapott gyanús tartalmú naplók vizsgálata ⇒ az alkalmazás futtatási környezetének (szerver) monitorozása ⇒ szerver komponensek naprakészen tartása ⇒ a szerver hardware elemeinek folyamatos karbantartása

Erőforrás típus	INTEGRA CAFM erőforrások
	⇒ biztonsági mentések készítése az adatbázisról ⇒ biztonsági mentés készítése a tárolt fájlokról ⇒ az IT fejlesztési csoporttól kapott komponens lista alapján a szükséges frissítések elvégzése ⇒ monitorozási tevékenység alatt keletkezett gyanús tevékenységek továbbítása az IT fejlesztés felé

Erőforrás típus	Általános IT erőforrások
Háttérstratégia	Informatikai és egyéb erőforrások azonnali beszerzése (személyi számítógép, hálózati eszközök, telefon készülékek..)
Háttérstratégia alkalmazásának a feltétele	Meghatározásra került a legfontosabb felhasználók köre, a számukra biztosított szükséges és elégséges IT eszközök, a minimális háttér készlet és a beszerzési források, valamint az elosztás és kiadás rendszere.

Humán erőforrások háttér stratégiája

Erőforrás típus	Speciális kompetenciával rendelkező személyek
Háttérstratégia	A „négy szem elvének” alkalmazása. Kerülni kell az egyedüli munkavégzést
Háttérstratégia alkalmazásának a feltétele	Munkatársak kompetenciájának a folyamatos javítása, a helyettesítési rend meghatározása.

Dokumentumok háttérstratégiája

Erőforrás típus	Dokumentumok
Háttérstratégia	Az üzletmenet folytonosság biztosításához elengedhetetlenül szükséges dokumentumok rendelkezésre állásának biztosítása.
Háttérstratégia alkalmazásának a feltétele	A dokumentumok kezelése az iratkezelési szabályzat szerint.

VÁLASZ FÁZIS

2. Esemény észlelése

Katasztrófa bekövetkeztére utaló jelek például:

- természeti katasztrófa következtében megrongálódott az épület,
- tűz ütött ki az épületben,
- füst észlelhető az épületben,
- vízbetörés az épületben,
- áramkimaradás miatti leállás következett be,
- az informatikai szolgáltatások leállása,
- szoftverben tárolt adatokhoz való jogosulatlan hozzáférés,
- adatok véletlen vagy jogellenes megváltoztatása,
- adatvesztés,
- munkatársak nagyszámú távolmaradása.

Amennyiben a fenti események közül bármelyik bekövetkezett, vagy a felsorolásban nem szereplő, de katasztrófára utaló esemény állt elő, az észlelőnek azonnal értesítenie kell valamelyik partnert.

Az értesített partner feladata eldönteni, hogy valóban vészhelyzetről van-e szó. A vészhelyzet fennállásának mérlegeléséhez szempont, hogy a kiesett folyamat helyreállítása a normál üzletmenetben ill. a megállapított sebezhetőségi ablak időtartamán belül lehetséges-e. Ha igen, akkor össze kell hívni a válságstábot. A riasztás menetét lásd. „RIASZTÁSI TERV” c. mellékletben.

3. Mentési feladatok

Minden katasztrófahelyzetben a legfontosabb és elsődleges feladat az emberi élet megóvása, függetlenül a katasztrófa hatásától. Az emberi életek mentését a cég telephelyére vonatkozó tűzvédelmi szabályzatnak megfelelően kell végrehajtani. Amennyiben indokolt, értesíteni kell a mentőket, a rendőrséget, az irodaház üzemeltetőt is.

Ha a bekövetkezett katasztrófa olyan mértékű, hogy szükség van az iroda, az épület kiürítésére, akkor a telephelyi tűzvédelmi szabályzat szerint kell eljárni.

Az esetleges életveszély elmúltával gondoskodni kell a veszélyeztetett kritikus folyamatokhoz kapcsolódó erőforrások, eszközök és a pótolhatatlan dokumentumok mentéséről is. A technikai mentés hatókörét a válságstáb határozza meg és biztosítja a feladathoz a szükséges munkaerőt.

A helyszínről eltávolított eszközök, berendezések és dokumentumok fizikai védelméről az Információbiztonsági Szabályzatban megfogalmazott intézkedések figyelembe vételével kell gondoskodni.

4. Károk felmérése, üzleti hatások elemzése

A katasztrófa eseményt követően kezdődik a kárfelmérés folyamata, amely nélkülözhetetlen a folyamatokhoz szükséges erőforrások helyreállíthatóságának vagy menthetőségük lehetséges mértékének megítéléséhez.

A kárfelmérés a következő területeken szükséges – ezekért az adott terület felelőse felel:

⇒ személyek, munkatársak,

⇒ beszállítók, alvállalkozók

⇒ létesítmény, infrastruktúra,

⇒ IT és távközlési erőforrások, elektronikus adatok,

⇒ levelezési rendszer

⇒ nem IT erőforrások, eszközök, nyomtatott információk.

A kárfelmérésnek pontosan kell rögzítenie a sérült erőforrások azonosítóját, a sérülés mértékét.

A kárfelmérés során különös figyelemmel kell megvizsgálni, hogy mely, a kritikus folyamatokat támogató erőforrások sérültek.

A károk felméréséről tájékoztatni kell a válságstábot szóban, majd később írásban.

5. Vészhelyzeti terv

	Erőforrás folyamat	Érintett folyamatok	Bekövetkező esemény	Sebezhetőségi ablak	Válasz tevékenység
1.	Cégvezetésben bekövetkező változás	Összes irányítási folyamat	Minden partner / partner egyidejűleg munkaképtelen lesz	Katasztrófa: Ha a kiesés >15 nap	1. Közgyűlés összehívása.
				Krízis: Ha a kiesés > 10 nap, de <15 nap	1. Új vezető átmeneti kijelölése és meghatalmazása.
				Incidens: Ha a kiesés < 10 nap	1. Amennyiben szükséges egyeztetés a kulcspartnerekkel.
2.	Projektvezető	F1; F2;	Egy projektvezető munkaképtelen lesz	Incidens: Ha a kiesés > 30 nap	1. A projektvezetők kijelölik maguk közül a területet, projekteket átvevő személyt. 2. Fel kell mérni, hogy a pillanatnyi helyzetben kik a kulcsmegrendelők, melyek a folyó projektek 3. A projektvezetőkkel fel kell venni a kapcsolatot – tisztázni kell a helyzetet, fel kell mérni a projektek állapotát és a kötelezettségeket.
3.	Irányítási rendszer vezetőségi képviselője	T1; T5; T9;	Az irányítási rendszer vezetőségi képviselője munkaképtelen lesz	Krízis: Ha a kiesés > 60 nap	1. A projektvezetők kijelölik maguk közül a területet, projekteket átvevő személyt. 2. Egyeztetés az irányítási rendszert felügyelő munkatárssal. 3. Munkatársak tájékoztatása. 4. Kapcsolatfelvétel az IT szolgáltatókkal.
				Incidens: Ha a kiesés >30 nap	
4.	Irányítási rendszert felügyelő munkatárs	T3, T4, T5, T6, T7, T8, T9, I5	Az irányítási rendszert felügyelő munkatárs munkaképtelen lesz.	Krízis: Ha a munkaképtelenség > 60 nap	1. Az irányítási rendszer vezetője átveszi a feladatait. 2. Külső tanácsadó bevonása
				Incidens: Ha a munkaképtelenség >30 nap	1. Az irányítási rendszer vezetője átveszi a feladatait. 2. Külső tanácsadó bevonása (ha szükséges)

5.	IT szolgáltató Magyar Telekom Nyrt., Vodafone Zrt.)	T1; T2; T12; T10; T13; F2; F1; F3; F4; F5; F6; F7	IT szolgáltatónál felmerülő problémák miatt teljesítési problémák.	Krízis: Ha a megjelölt szolgáltatási szintet egymást követően kétszer nem teljesíti a szolgáltató. Incidens: Ha a megjelölt szolgáltatási szintet, vagy a szerződésben foglalt szakmai tartalom 95%-át nem teljesíti a szolgáltató.	1. Kapcsolatfelvétel a szolgáltatóval 2. Az irányítási rendszert felügyelő partner és a rendszergazda áttekinti az IT rendszer működését (adatmentések, portok működése, védelem, külső próbálkozások, IT infrastruktúra) 3. A munkatársak figyelmének felhívása 4. Az elemzések alapján intézkedések megtétele (ha az szükséges)
6.	Rendszergazda (.Coimbra ITS Kft.)	T2; T3; T4; T8; T7; T10; T1	A rendszergazda nem tudja ellátni a munkáját.	Krízis: Ha egyáltalán nem tudja ellátni a feladatát Incidens: A rendszergazda kiesik > 30 napra és távolról sem tudja a munkáját végezni.	1. Kapcsolatfelvétel más szolgáltatóval. Felelős: Az irányítási rendszert felügyelő partner 2. A rendszergazdai feladatok azonnali áttekintése, jogosultságok lehatárolása Az irányítási rendszert felügyelő partner egyeztetve a rendszergazdával gondoskodik más szakértő bevonásáról.
7.	Teljes informatikai infrastruktúra	Szolgáltatás nyújtási feladatok; T1;T2; T3; T4; T7; T10; T13	Az informatikai rendszer leáll	Katasztrófa: Ha az eredeti állapot részben sem állítható vissza Krízis: Ha a visszaállítás > 7 nap és/vagy szervercsere szükséges.	1. A projektvezetők tájékoztatják a munkatársakat 2. A projektvezetők felveszik a kapcsolatot az ügyfelekkel 3. Mindenki a saját laptopjára kezd el dolgozni. 4. Szerverbeszerzés és az új rendszer felállítása a rendszerspecifikációk szerint. Felelős: rendszergazda 1 A rendszergazda megkezdi a helyzet felmérését és a rendszer visszaállítását a rendszerdokumentáció szerint. Ha szükséges kezdeményezi eszközök beszerzését. 2. A projektvezetők tájékoztatják a munkatársakat 3. A projektvezetők felveszik a kapcsolatot az ügyfelekkel

				Incidens: Ha a visszaállítás < 2 nap.	4. Mindenki a saját laptopjára kezd el dolgozni.
8.	Technikai működés szünetelése vagy megszűnése	Szolgáltatás nyújtási feladatok; T1 – T13	Külső események (tűz, természeti jelenségek, betörés stb.)	Katasztrófa: Ha a teljes infrastruktúra megsemmisül	1. A projektvezetők informálják az ügyfeleket 2. Az irányítási rendszert felügyelő partner felveszi a kapcsolatot az IT szolgáltatókkal 3. A munkatársak informálása 4. Új iroda bérlése 5. A károk függvényében átmeneti infrastruktúra beszerzése
				Krízis: Ha az informatikai rendszer leáll.	lásd. 7.
				Incidens: Kisebb károk melyek gyorsan és veszteség nélkül helyre állíthatók (pl.: részleges leállás: az esemény csak egy résztevékenységre, projektre gyakorol hatást)	1. A projektvezetők felülvizsgálják az eseményt 2. Azonnali intézkedések meghozatala a felmérés függvényében 3. A munkatársak tájékoztatása
9.	Pénzügyi következmény ekkel járó esemény	F3, F2, T2	Hatósági kötelezés érkezik	Katasztrófa: Ha a cégcsoport valamely tagja pénzügyileg ellehetetlenül.	1. A partnerek áthidaló megoldásokat keresnek 2. Egyeztetések megkezdése az ügyfelekkel
				Krízis: A vállalat hírneve csorbul, tevékenységet vagy projekt teljesítést fel kell függeszteni.	1. A partnerek felveszik a kapcsolatot az ügyfelekkel 2. Intézkedési terv készítése
				Incidens: A kötelezés valamely projekt teljesítését negatívan befolyásolja.	

10.	Emberi erőforrások rendelkezésre állása	Szolgáltatás nyújtási folyamatok, Támogató folyamatok,	Munkatársak kilépése vagy hosszabb időre történő kiesése	Krízis: Ha a munkavállalók 50 %-a kilép egy hónapon belül	1. A projektvezetők felveszik a kapcsolatot az ügyfelekkel 2. Új munkatársak keresésének a beindítása
				Incidens: Ha egy szakterület távozik a vállalattól	1. Vezetőségi egyeztetés 2. Átcsoportosítás vagy külső erőforrások bevonása
				Incidens: Ha egy munkatárs váratlanul átmenetileg hosszabb időre kiesik (>15 nap)	1. Vezetőségi egyeztetés 2. Átcsoportosítás vagy külső erőforrások bevonása
11.	Operatív vezetők	F4 – F6	Minden operatív vezető egyidejűleg munkaképtelen lesz	Katasztrófa: Ha a kiesés >30 nap	1. Projektvezetők összehívása, feladatok átcsoportosítása 2. Új operatív vezető átmeneti kijelölése és meghatalmazása
				Krízis: Ha a kiesés > 10 nap, de <30 nap	1. Projetkvezetők összehívása, feladatok átcsoportosítása 2. Új operatív vezető átmeneti kijelölése és meghatalmazása
				Incidens: Ha a kiesés < 10 nap	1. Amennyiben szükséges, egyeztetés a partnerekkel
12.	Operatív vezetők	F4-F6	Egy operatív vezető munkaképtelen lesz	Krízis: Ha a kiesés > 30 nap	1. Projektvezetők összehívása, feladatok átcsoportosítása 2. Új operatív vezető átmeneti kijelölése és meghatalmazása
				Incidens: Ha a kiesés > 10 nap, de <30 nap	1. Amennyiben szükséges, egyeztetés a partnerekkel
	Beszállítói szolgáltatás		Beszállító / alvállalkozó munkaképtelen lesz	Katasztrófa: Ha a kiesés >30 nap	1. Projektvezetők összehívása, erőforrások átcsoportosítása
				Krízis: Ha a kiesés > 10 nap, de <30 nap	1. Vezetőségi egyeztetés 2. Átcsoportosítás vagy más beszállítók bevonása
				Incidens: Ha a kiesés < 10 nap	1. Vezetőségi egyeztetés 2. Átcsoportosítás vagy más beszállítók bevonása

6. Kockázatok felmérése az INTEGRA CAFM rendszer üzemeltetésével kapcsolatban és az azok megelőzésére tett intézkedések

Kockázat	Következmények	Veszélyforrás	Megelőző intézkedések	Valószínűség	Súlyosság
Adatokhoz való jogosulatlan hozzáférés	Illetéktelenek szerezhetnek meg üzletérzékeny információkat	Szervezeten belüli Szervezeten kívüli	TLS kapcsolat a kommunikáció során Blacklist alapú felhasználói input adat validálás Egyedi felhasználó azonosítás a rendszer használatakor Erős jelszó kényszerítése Alkalmazáson belüli jogosultság kezelés Alkalmazáson belül minden műveletnél jogosultsági szint ellenőrzés Bejelentkezés biztonsági időkorlát Naplózás Biztonsági mentések Szoftveres tűzfal VPN kapcsolat	Alacsony	Alacsony

Adatok vétlen vagy jogellenes megváltoztatása	Hibaértesítők kiküldése elmarad Hibás adatokkal kerül kiküldésre az értesítés Hibás statisztikák készülnek Alkalmazás nem elérhető a felhasználók számára Alkalmazás nem elérhető külső rendszer számára	Szervezeten belüli Szervezeten kívüli	TLS kapcsolat a kommunikáció során Blacklist alapú felhasználói input adat validálás Egyedi azonosítás a rendszer használatakor Erős jelszó kényszerítése Alkalmazáson belüli jogosultság kezelés Alkalmazáson belül minden műveletnél jogosultsági szint ellenőrzés Bejelentkezés biztonsági időkorlát Naplózás Biztonsági mentések Szoftveres tűzfal VPN kapcsolat	Alacsony	Elhanyagolható
Adatvesztés	Hibaértesítők kiküldése elmarad Hibás adatokkal kerül kiküldésre az értesítés Hibás statisztikák készülnek Alkalmazás nem elérhető a felhasználók számára Alkalmazás nem elérhető külső rendszer számára	Hardware meghibásodás Természeti katasztrófa Hacker támadás	TLS kapcsolat a kommunikáció során Blacklist alapú felhasználói input adat validálás Egyedi felhasználó azonosítás a rendszer használatakor Erős jelszó kényszerítése Alkalmazáson belüli jogosultság kezelés Alkalmazáson belül minden műveletnél jogosultsági szint ellenőrzés Bejelentkezés biztonsági időkorlát Naplózás Biztonsági mentések Szoftveres tűzfal VPN kapcsolat	Alacsony	Közepes

7. Az INTEGRA CAFM rendszerrel kapcsolatos már kialakított BCM folyamatok karbantartása, a folyamatok tesztelése

a. Az alkalmazás használata során keletkező naplók folyamatos elemzése, ezek alapján szükséges javítások elvégzése, tesztelése külön teszt környezetben. Sikeres tesztelés után az éles rendszer frissítése.
b. A használt környezeti komponensek frissítéseinek folyamatos nyomon követése – kiemelt figyelemmel a biztonsági frissítésekre. A frissítendő komponensek külön teszt környezetben való tesztelése. Sikeres tesztelés után az éles rendszer frissítése.

Jelentős változtatások esetén a felhasználók írásos tájékoztatást kapnak a módosult, vagy új funkciók használatáról.

Ezek mellett, a következő tesztek kerülnek elvégzésre rendszeres időközönként:

Belső jogosultsági szintek szerinti hozzáférések ellenőrzése

⇒ 'Low privileged user' teszt

⇒ Vétlen vagy rosszindulatú adattörlés / visszaállítás teszt

⇒ Szerver komponensek biztonsági tesztje

Külső hozzáférések ellenőrzése

⇒ Alkalmazás elérhetetlenség teszelése

Az egyes alkalmazás frissítések alkalmával minden esetben teszteljük a frissítéssel közvetlenül vagy közvetve érintett funkciókat.

Teljes rendszert érintő vizsgálatra éves rendszerességgel kerül sor, a legutóbbi 2020-06-01-én történt a következő ütemezés szerint 2021-06-01-én esedékes.

TERV A JÁRVÁNYÜGYI HELYZET KEZELÉSÉRE

Az alkalmazottak helyének és az utazásoknak az áttekintése

Pontosan meghatározzuk, hol vannak a vállalat munkavállalói, és hányan vannak magas kockázatú területen. Felmérjük, hogy szükség van-e az alkalmazottak szállításra, illetve hogy lehetséges-e az otthoni munkavégzés. A tervezett utazásokat felülvizsgáljuk, elhalasztjuk vagy töröljük.

A rendelkezésre álló technika felmérése, szükség esetén kiegészítése

Amennyiben sok alkalmazottnak távolról kell dolgoznia, megvizsgáljuk, hogy rendelkezésre áll-e ehhez a szükséges zechnikai felszerelés. Amennyiben nem, úgy azt központi forrásból pótoljuk, illetve beszerezzük a hiányzó eszközöket.

A folyamatok működése, kommunikáció

A működést nem lehetetleníti el, ha a munkaerő nem az irodában dolgozik. Az iratkezelés digitalizált, így távolról is elérhetők a dokumentumok. Engedélyezett a digitális aláírás a járványügyi helyzet fennállása alatt úgy, hogy a tényleges, papír alapú aláírás a későbbeikben kerül megküldésre.

Az alkalmazottak el tudják érni a központi erőforrás rendszereit távasztalon keresztül, illetve VPN elérés is biztosított. Az email címeket is tudják kezelni alternatív eszközökön. Az adatáramlást a válság nem befolyásolja, mert a napi folyamatos kapcsolattartás e-mailen, internet alapú applikációkon, illetve telefonon biztosított.

A személyes kontaktusok számát a minimálisra csökkentjük, és a digitális meetingeket preferáljuk (zoom, skype, teams). Ezek már nem jelentenek biztonsági kockázatot.

A kommunikáció következetessége és pontossága, valamint a szervezet csúcsáról érkező megerősítés kulcsfontosságú ebben a helyzetben.

Az iroda fenntartása

A cég irodáját fenntartjuk, havonta fertőtlenítő takarítást rendelünk el.

Az irodában kötelezővé tesszük a védőeszközök (maszk) használatát, és a kézfertőtlenítést az érkezéskor, illetve a távozáskor egy automata, érintés nélküli készülékkel. A bejáratnál biztosítunk az alkalmazottaknak, illetve ha szükséges a vendégeknek maszkot.

Az irodába érkezőket feliratokkal is tájékoztatjuk az irodában betartandó szabályokról.

Minimalizáljuk az irodai tartózkodás időtartamát, ösztott munkavégzést vezetünk be ügyeleti rendszerrel, ha szükséges.

FOGALMAK

Katasztrófa: Katasztrófának nevezzük az olyan helyzetet vagy állapotot (pl. egy krízishelyzet során a folyamatok nem visszaállíthatóak; természeti / biológiai eredetű, vagy tűz okozta károk keletkeznek), amely a társaság vagyonában olyan fizikai kárt okozott, ami miatt ott részben vagy teljes mértékben lehetetlenné válik a munkavégzés, az üzletmenet továbbvitele.

Krízis: Egy olyan, a társaság egészét érintő probléma, amelyet az akciótervek segítségével, és ha szükséges, külön a válságstáb felállításával lehet megoldani.

Incidens: Egy olyan szolgáltatáson belüli probléma, amelyet az akciótervek segítségével lehet megoldani.

Üzletmenet-folytonossági terv (BCP): annak leírása, hogyan lehet egy üzleti funkciót fenntartani annak megzavarása alatt és után.

RIASZTÁSI TERV

Név	Beosztás	Elérhetőség (cím, telefon)
Rajkai György	vezérigazgató	*+36 30 757 7428*
Buchwald Imre	vezérigazgató helyettes	*+36 20 401 2624*
Molnár Tímea	irodavezető	*+36 30 389 2000*