Informatikai kockázati leltár és intézkedési terv						
ssz.	***Azonosított kockázat***	***Probléma, kiváltó ok***	**Jellemző értékek**			***Lehetséges intézkedések***
			Hatás (1-5)	***Valószí-nűség (1-5)***	***Kockázati érték (1-25)***	
1. Környezeti kockázatok						
I/1	Lokális tűz - gépterem	épületkarbantartási hiányosságok, szabályok be nem tartása	3-5	1-2	3-10	Távoli adattükrözés (backup gépterem) Mentési adatállományok szeparált helyen történő őrzése Tűzjelző rendszer kiépítése Automatikus tűzoltó rendszer építése Meglévő biztosítások felülvizsgálata
I/2	Lokális tűz - iroda	épületkarbantartási hiányosságok, szabályok be nem tartása	2-4	1-2	2-8	Lokális gépen nem tárolunk adatokat Adatmásolatok készítése, mentések Tűzjelző rendszer kiépítése Tűzoltó készülék elhelyezése Meglévő biztosítások felülvizsgálata
I/3	Vízkár -gépterem	épületkarbantartási hiányosságok, szabályok be nem tartása	3-5	1-2	3-10	Távoli adattükrözés (backup gépterem) Mentési adatállományok szeparált helyen történő őrzése Álpadló, gépek szintjének megemelése Vízhálózattal kapcsolódó csőrendszer megszüntetése a gépterembern Meglévő biztosítások felülvizsgálata
I/4	Vízkár- iroda	épületkarbantartási hiányosságok, szabályok be nem tartása	2-4	1-2	2-8	Lokális gépen nem tárolunk adatokat Adatmásolatok készítése, mentések
I/5	Erősáramú ellátás kiesése	épületkatbantartási hiányosságok, szabályok be nem tartása, külső szolgáltató hibás teljesítése	2-4	1-2	2-8	Szünetmentes áramforrás kiépítése Másodlagos betáplálás kialakítása (szolgáltatói) Redundáns tápellátású berendezések használata
I/6	Gépterem túlmelegedése	épületkatbantartási hiányosságok, szabályok be nem tartása	2-4	1-2	2-8	Erősáramú terhelések tervezése Klíma berendezés alkalmazása
2. Fizikia kockázatok						
II/1	Lopás	biztonsági hiányosságok, figyelmetlenség, összejátszás	1-3	1-3	1-9	Őrszolgálat "Tiszta asztal" politika bevezetése, alkalmazása Beléptető rendszer kialakítása
II/2	Rongálás	szervezetlenség, rossz tervezés, összejátszás	1-2	1-2	1-4	Őrszolgálat "Tiszta asztal" politika bevezetése, alkalmazása Beléptető rendszer kialakítása
II/3	Fizikai betörés	biztonsági hiányosságok, figyelmetlenség	1-2	1-2	1-4	Őrszolgálat "Tiszta asztal" politika alkalmazása, Meglévő biztosítások felülvizsgálata Beléptető rendszer kialakítása Behatolás fizikai korlátozása (rács, biztonsági ajtó)
3. Informatika működtetésénél fellépő kockázatok						
III/1	Szerver hardver meghibásodás	szabályozatlanság, elavult berendezések, mulasztás	2-4	2-4	4-16	Távoli másolatok kialakítása Nagy rendelkezésre állású HW kialakítás (pl. duplikált szerver, load balancer) Külső Cloude szolgáltatás igénybevétele (amely biztosítja a kívánt rendelkezésre állást) Külső szolgáltatóval hibaelhárítási szerződés Felügyeleti rendszer (monitoring) kialakítása, riasztási eljárásrend bevezetése
III/2	Adattároló meghibásodás	szabályozatlanság, elavult berendezések, mulasztás	2-4	2-4	4-16	Távoli másolatok kialakítása Igény szerint szinkron vagy asszinkron adattükrözés DR (Disaster Recovery) terv készítés és tesztelés Felügyeleti rendszer (monitoring) kialakítása, riasztási eljárásrend bevezetése

ssz.	*Azonosított kockázat*	*Probléma, kiváltó ok*	*Hatás (1-5)*	*Valószí-nűség (1-5)*	*Kockázati érték (1-25)*	*Lehetséges intézkedések*
III/3	Adatátviteli eszköz meghibásodás	szabályozatlanság, elavult berendezések, mulasztás	2-3	2-4	4-12	Redundáns hálózat kialakítása Külső kapcsolatoknál (pl. Internet) backup szolgáltató alkalmazása Központi eszközök, hálózati elosztók gépterembe helyezése Felügyeleti rendszer (monitoring) kialakítása, riasztási eljárásrend bevezetése
III/4	Adathordozó sérülése, elvesztése	szabályozatlanság, elavult berendezések, mulasztás	1-3	2-4	2-12	Adathordozók kezelésének szabályozása (kötelezős másolatok készítése, központi /szerveren/ történő adattárolás előírása és alkalmazása Adathordozók (mentési kazetták) nyilvántartása, tárolásuk szabályozása)
III/5	Vírus támadások	szabályozatlanság, elavult eszközök, mulasztás	2-5	2-4	4-20	Wifi hozzáférés korlátozása, vírusvédelem fejlesztése (két szintű vírusvédelem - különböző gyártók -), etikus hacker auditok
III/6	Internetes támadások	szabályozatlanság, elavult eszközök, mulasztás	2-4	2-4	4-16	Tűzfalak alkalmazása Támadás detektáló (IDS) és/vagy ellenük védő eszközök (IPS) használata Etikus hacker auditok
III/7	Illetéktelen behatolás	szabályozatlanság, oktatások elmulasztása, fegyelmezetlenség	2-4	2-4	4-16	Jelszó kezelés felükvizsgálata, újraszabályozása Felhasznólók nyilvántartása Központi jogosultság kezelés kialakítása Jogosultság kiadás, felfüggesztés, visszavonás szabályzása Felhasználói oktatás
III/8	Adatszivárgás (eltulajdonítás)	szabályozatlanság, oktatások elmulasztása, fegyelmezetlenség, visszaélés	2-4	2-4	4-16	Hozzáférések szabályozása, szkenner könyvtár napi törlése, naplók felülvizsgálata Levelezés szabályzása Csatolmányok vizsgálata, korlátozása
III/9	Illetéktelen hozzáférés (Jelszó kezelés)	szabályozatlanság, oktatások elmulasztása, fegyelmezetlenség, visszaélés	2-4	2-4	4-16	Jelszó kezelés felükvizsgálata, újraszabályozása Oktatás Szúrópróba szerinti ellenőrzés
III/10	Operációs rendszer sérülékenység	szabályozatlanság, elavult eszközök, mulasztás	2-4	2-4	4-16	Patch menedzsment kialakítása Központi rendszer upgrade bevezetése Lehetőleg azonos operációs rendszer használata minden munkaállomáson (egységesítés)
III/11	Adathálózathoz való illetéktelen hozzáférés	szabályozatlanság, oktatások elmulasztása, fegyelmezetlenség, visszaélés	2-4	2-4	4-16	Kiemelt jogosultságok speciális kezelésének szabályozása (Root jelszó gyári alapérték megváltoztatása) Adatkábelezés fizikai védelme (álpadló, adatkábelezési csatornák kiépítése)
III/12	Hibaelhárítások elhúzódása	szabályozatlanság, elavult szerződések, szervezési hiányosságok, finanszírozási nehézségek	2-4	2-4	4-16	SLA definiálása Szerződések felülvizsgálata Visszamérése a szolgáltatásoknak Belső erőforrás (informatikus) további biztosítása Hibabejelentő rendszer kialakítása, egységesítése Prioritás meghatározások Eszközgazdálkodás, tartalék berendezések
III/13	Mentési állományok rossz minősége	szabályozatlanság, elavult eszközök, mulasztások	2-4	2-4	4-16	Mentések tesztelése, DRP eljárások kidolgozása, tesztelése (időszakonként és jelentős változásokkor) Mentések megőrzési idejének meghatározása és a mentési rendet ez alapján kell kialakítani Mentések lefutásának (végrehajtásának) ellenőrzése
...	....					
	további informatikai és egyéb szakterületeken azonosítható kockázatok előfizetőink számára elérhetők a letölthető dokumentumok menüpontban					