**Informatikai incidens kezelés belső vizsgálati jegyzőkönyve**

**Azonosítószám:** *(Iktatószám)* \*

**Készült:** *(dátum, helység)*

\*

**Jelen vannak:** *(a team tagjai, jegyzőkönyvvezető*)

\*

**Előzmény:** *(a biztonsági esemény jelentésének körülményei)*

\*

**Az esemény;**

**bejelentésének módja:** *(bejelentő felület, OTRS rendszer, email)*

[ ]  Bejelentő felület [ ]  OTRS rendszer (helpdesk) [ ]  email

**bejelentésének időpontja:** *(dátum)*

\*

**bejelentésének személye:** *(név, szervezet)*

\*

**bejelentő, eseményre vonatkozó leírása:**

\*

**Vizsgálati lépések:** *(a biztonsági eseményre vonatkozó elemzés)*

\*

**Megállapítások:** *(a biztonsági eseményre vonatkozó besorolások)*

\*

**Hibaok meghatározása:** *(hogyan következhetett be a biztonsági esemény)*

\*

**Miért következett be?** *(milyen preventiv tevékenység nem lett megvalósítva, mi nem lett végrehajtva-, bevezetve-, elkészítve-, beszerezve)*

\*

**Felelősség megállapítása:** *(egyértelműen és kizárt módon megállapított hiányosság és annak felelőse)*

\*

**Incidenskezelő team:** *(az incidensnek minősített esemény kezelésében IRT (Incident Response Team) eljáró csapat tagja, név, szervezet, beosztás, minőség megnevezéssel)*

\*

**Az incidens azonosítása, ismertetése:** *(az incidens leírása)*

\*

**Az incidens minősítése:** *(az incidens súlyossági szintjének leírása)*

[ ]  Alacsony [ ]  Közepes [ ]  Magas [ ]  Kritikus

**Adatvédelmi incidens kockázat elemzés eredménye:**

Természetes személy adata érintett? Igen [ ]  Nem [ ]  *(tegyen pipát a jelölőnégyzetbe)*

**Személyes adatok köre:** *(amennyiben igen, milyen személyes adatok érintettek)*

\*

**Érintettek köre:** *(amennyiben igen, kik az érintettek –dolgozó, paciens, hallgató, külső személy-)*

\*

**Személyes adatok típusa:** *(amennyiben igen, az adatok minősítése –érzékeny-)*

\*

**Érintettek száma:** *(amennyiben igen, hány személy adata érintett)*

\*

**Személyes adatok száma:** *(amennyiben igen, hány adat érintett személyenként)*

\*

**Elhárítás, felszámolás.**

 **Probléma:** *(az esemény által okozott anomália)*

 \*

 **Mi történt:** *(az esemény hogyan következett be)*

 \*

 **Mi nem történt a prevenció érdekében:** *(hogyan lehetett volna kivédeni az incidens bekövetkezését)*

 \*

 **Mit kellett végrehajtani:** *(milyen feladatok sorozata történt az elhárítás érdekében)*

 \*

 **Hogyan kellett végrehajtani:** *(az elhárítás módszertana, ki, mit, hogyan tett meg kronológiai sorrendben –lényeges a tudásbázis vonatkozásában-)*

\*

**felelős/felelősök:** *(az elhárítás során kiknek volt feladata –a legcsekélyebb feladatnak itélt is-)*

\*

**határidő:** (kronológia sorrend és tevékenységek ideje)

\*

**érintett elektronikus információs rendszer** *(az incidensben érintett minden EIR rendszer)*

\*

**érintett infrastruktúra** *(az incidensben érintett infrastruktúra –szerver, hálózat, wifi, storage, asztali PC, hordozható eszközök beleértve a telefont is )*

\*

**érintett campus** *(az incidensben érintett Egyetemi telephely/telephelyek)*

\*

**érintett szervezeti egység** *(az incidensben érintett Egyetemi szervezeti egység/egységek)*

\*

**tervezett befejezés** *(az elhárítási tevékenység megvalósításának tervezett ideje)*

*\**

**tényleges befejezés** *(az elhárítási tevékenység megvalósításának valós ideje)*

*\**

**Kárcsökkentő intézkedés:**

**folyamat:** *(amennyiben kár következett be, vagy bekövetkezésével számolni lehet, milyen tevékenységgel mérsékelhető annak mértéke)*

\*

**felelős/felelősök:** *(a kárcsökkentő tevékenységet megvalósító személyek)*

\*

**határidő:** *(a kárcsökkentő tevékenységet mikor kellett megkezdeni )*

\*

**tervezett befejezés:** *(a kárcsökkentő tevékenységet mikorra kellett megvalósítani )*

\*

**tényleges befejezés:** *(a kárcsökkentő tevékenységet mikorra valósult meg )*

\*

**Helyreállító intézkedés:**

**folyamat:** *(amennyiben az incidens károkat okoz, milyen intézkedések váltak szükségessé a normál ügymenet visszaállítása céljából)*

\*

**felelős/felelősök:** *(a helyreállító tevékenységet megvalósító személyek)*

\*

**határidő:** *(a helyreállító tevékenységet mikor kellett megkezdeni )*

\*

**tervezett befejezés:** *(a helyreállító tevékenységet mikorra kellett megvalósítani )*

\*

**tényleges befejezés:** *(a helyreállító tevékenységet mikorra valósult meg )*

\*

**Tartalék/redundáns eszköz bevonás:**

**folyamat:** *(amennyiben az incidens olyan károkat okoz, hogy a normál ügymenet fenntartására, biztosítására tartalék/redundáns eszközt/eszközöket kell beüzemelni, milyen intézkedések megtételére került sor, kronológia sorrendben)*

\*

**felelős/felelősök:** *(a tevékenységet megvalósító személyek)*

\*

**határidő:** *(a tevékenységet mikor kellett megkezdeni )*

\*

**tervezett befejezés:** *(a tevékenységet mikorra kellett megvalósítani )*

\*

**tényleges befejezés:** *(a tevékenység mikorra valósult meg )*

\*

**Hosszú távú javító intézkedés meghatározása**

**Folyamat/elem:** *(az incidens jövőbeni elkerülése érdekében végrehajtandó tartós tevékenység)*

\*

**Felelős:** *(a tevékenység biztosítását végző személy/személyek)*

\*

**Tervezett befejezés:** *(a javító intézkedések fenntartásának határideje)*

\*

**Elemzés, okulás:** *(a biztonsági esemény, incidens megelőzésére tehető intézkedések, beruházások, szervezési feladatok-, az elhárítási folyamat elemeinek átgondolása)*

\*

**Maradványkockázat:**

**Leírás:** *(amennyiben az elhárítással, vagy az elhárítást követően egyéb kockázatok léptek fel, azok jellemzői)*

\*

**Kezelés módja:** *(amennyiben maradványkockázat keletkezik, annak elhárításai)*

\*

**Kezelés tervezett ideje:** *(amennyiben maradványkockázat keletkezik, a megoldás határideje)*

\*

**Felelős:** *(amennyiben maradványkockázat keletkezik, annak kezelére kijelölt személyek)*

\*

**Csatolt, az ügyben készített feljegyzés, dokumentum, irat:** *(az esemény kezelése során létrejött bármilyen irat, leirat, feljegyzés, dokumentum)*

 \*

**Tudásbázis aktualizálás:** *(az esemény megoldásának leírata, ismételt kezelés gördülékeny végzésének-, új dolgozó munkájának támogatásához)*

**Felelős:** *(kinek a feladata a tapasztalati anyag elkészítése és feltöltése)*

\*

**Anyag:** *(milyen anyagok lettek feltöltve, rögzítve)*

\*

**Határidő:** *(milyen határidővel történt a feltöltés)*

 \*

**Jegyzőkönyv lezárásra került: Debrecen, \* év \* hó \* nap**

**Aláírások** *(„Jelen vannak” aláírásai)*