TOKAJ-HEGYALJA EGYETEM

1/2024. (11.01) rektori-kancellári közös utasítás

INFORMATIKAI KATASZTRÓFATERV

/Informatikai biztonsági incidensek kezelése/

Tartalom

1. Bevezetés, általános rendelkezések

1.1. Az utasítás célja és hatálya

Az Informatikai Katasztrófaterv célja, hogy nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény egyes rendelkezéseinek végrehajtásáról szóló 87 / 2015 (IV. 9.) Korm.rendelet 3.§ (3)-(4)bekezdésében foglalt előírások alapján, tekintettel az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (a továbbiakban: Ibtv.) megfogalmazott irányelvekre, valamint az MSZ ISO/IEC 27001 szabvány ajánlásaira pontosan megfogalmazza a Tokaj-Hegyalja Egyetem (továbbiakban: Egyetem) adatainak megőrzésével kapcsolatos elveket, feladatokat és meghatározza az ebből eredő felelősségi köröket és kötelességeket, hogy ezzel biztosítsa az üzletmenet folytonosságát, minimalizálja a katasztrófák bekövetkezésének valószínűségét és az okozott károkat.

Az Informatikai Katasztrófaterv hatálya kiterjed az Egyetemmel munkaviszonyban és munkaviszonyra irányuló egyéb jogviszonyban álló dolgozók, szervezeti egységek közül mindazokra, akik az Egyetem informatikai rendszerével és/vagy adataival valamilyen módon kapcsolatba kerülnek.

1.2. **Értelmező rendelkezések**

a) Adat: az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas.

b) Adat- vagy információbiztonság: Az Egyetem számára kedvező állapot, melyben a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása biztosított.
   - Bizalmasság: A bizalmasság elve biztosítja, hogy az információkhoz csak azok a személyek férhessenek hozzá, akiknek erre jogosultságuk van.
   - Sértetlenség: A sértetlenség elve biztosítja, hogy az információk pontosak, megbízhatóak, és nem változnak meg jogosulatlanul.
   - Rendelkezésre állás: az a tényleges állapot, amikor egy informatikai rendszer szolgáltatásai az arra jogosultak számára egy meghatározott időben rendelkezésre állnak és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva;

c) Informatikai rendszer: Olyan hardver- és szoftverelemek, valamint hálózati infrastruktúra együtteséből áll, amely lehetővé teszi az adatok gyűjtését, feldolgozását, tárolását és továbbítását. Célja az adatok hatékony kezelése és a szervezet működésének támogatása, beleértve az információáramlást, a kommunikációt, az automatizált folyamatokat és az adatbiztonságot. Az informatikai rendszer kiterjedhet helyi (on-premise)

infrastruktúrára vagy felhőalapú megoldásokra, attól függően, hogy milyen módon biztosítja a hozzáférést és a működést.

a) Informatikai Biztonsági esemény: Nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idézhet elő.
b) Informatikai Biztonsági incidens: Olyan biztonsági esemény, amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül.
c) Informatikai vészhelyzet: Olyan állapot, amikor az informatikai szolgáltatások jelentős része nem elérhető, a helyreállítás rövid időn belül nem lehetséges, az üzletmenet folytonosság biztosítása sérül.
d) Informatikai Katasztrófa vészhelyzeti terv: Jelen dokumentumban meghatározott eljárások és intézkedések, amelyek célja az informatikai rendszereket érintő katasztrófák vagy súlyos incidensek esetén a szervezet működésének fenntartása, az adatok védelme és a rendszerek mielőbbi helyreállítása.
e) Észlelés: A biztonsági esemény bekövetkezésének felismerése.
f) IT Katasztrófavédelmi Bizottság: (IRT - Incident Response Team): Az a csapat, amely felelős a katasztrófahelyzetekre való felkészülésért, reagálásért és a helyreállításért.
g) Káresemény: A káresemény az információbiztonság sérülése.
h) Felhasználó: egy adott elektronikus információs rendszert igénybe vevők köre.
i) Redundancia: Az adatok, rendszerek, eszközök több példányban történő tárolása, hogy meghibásodás esetén is elérhetőek maradjanak.
j) Informatikai katasztrófa: Az informatikai katasztrófa olyan biztonsági incidens, amely nagy mértékben zavarja, vagy teljesen leállítja az Egyetem informatikai rendszereinek működését, és amely jelentős negatív hatással lehet az Egyetem üzleti folyamataira, információbiztonságára. Az ilyen katasztrófák azonnali és hatékony reagálást igényelnek a károk minimalizálása és a normál működés mielőbbi helyreállítása érdekében. Típusai:
    - Természeti katasztrófák:
      Árvíz, földrengés, tűzvész, viharok, amelyek fizikai károkat okozhatnak az adatközpontokban, vagy a hálózati infrastruktúrában.
    - Emberi hibák:
      Véletlen adatvesztés, rossz konfigurációk, hibás szoftverfrissítések, amelyek miatt rendszerek és szolgáltatások leállnak.
    - Technológiai hibák:
      Hardverhibák (pl. szerverek meghibásodása, hálózati eszközök

meghibásodása), szoftverhibák (pl. operációs rendszer összeomlása), hálózati meghibásodások, amelyek megszakítják a szolgáltatásokat.
    - Kiberbiztonsági fenyegetések:
      Kiber támadások (pl. hackertámadások, ransomware, adathalászat, DDoS támadás), adatlopás, rendszerek vagy adatok kompromittálása, amelyek veszélyeztetik az adatbiztonságot és az üzletmenetet.
    - Külső partnerek által nyújtott szolgáltatások meghibásodása:
      Elektromos hálózat tartós kiesése, internet szolgáltatás megszakadása, felhőszolgáltatók hibái, külső adatközpontok meghibásodása, amelyek befolyásolják a szervezet működését.
k) DRP (Disaster Recovery Plan) vészhelyzeti terv: Egy olyan stratégia, amely részletesen leírja azokat a lépéseket, intézkedéseket és eljárásokat, amelyeket egy szervezetnek kell végrehajtania, ha súlyos informatikai zavar vagy katasztrófa következik be.

2. Biztonsági m**egelőző** intézkedések

A megelőző intézkedések célja, hogy minimalizálják az informatikai biztonsági események bekövetkezésének valószínűségét és hatását az üzleti folyamatokra és az informatikai rendszerekre.

2.1. Adatvédelmi intézkedések

- Rendszeres biztonsági mentés: Biztonsági mentés készítése minden szerverről, kritikus adatról és alkalmazásról rendszeres időközönként.
- Biztonsági mentések tárolása: A biztonsági mentések tárolása biztonságos, távoli helyszíneken, vagy legalább másik tűzszakaszban történik, hogy fizikai katasztrófák esetén is hozzáférhetők legyenek.
- Hordozható eszközök titkosítása: A hordozható eszközök (notebookok, pendrive-ok, külső merevlemezek) titkosítása az érzékeny adatok védelme érdekében.
- Adatkezelési szabályzat: Az Egyetem adatkezelő és adatfeldolgozó tevékenységének szabályozása.

2.2. Informatikai biztonsági intézkedések

- Fizikai biztonság: Adatközpont fizikai védelmének biztosítása a természeti katasztrófákkal szemben:
    - szünetmentes tápegység,
    - tűzjelző berendezések,
    - tűzoltó készülékek,
    - klimatizálás (automatikus visszakapcsolás áramkimaradás esetén).
- **Tűzfalak és behatolásmegelőző rendszerek (IPS):** Tűzfalak és behatolásmegelőző rendszerek üzemeltetése a hálózat védelme érdekében.

- VPN használata: Az intézmény L2TP/IPsec (Internet Protocol Security) protokollt használ előmegosztott kulccsal és egyedi felhasználónevekkel a VPN kapcsolatokhoz, amely biztonságos adatátvitelt biztosít a távoli felhasználók és az intézmény hálózata között.
- Antivírus és malware védelem: Kliens gépek védelme ESET Endpoint Security szoftverrel, modulok rendszeres frissítése, naprakészen tartása.
- Hozzáférési jogosultságok szabályozása: A hozzáférési jogosultságok megfelelő szabályozása és rendszeres ellenőrzése az illetéktelen hozzáférés megelőzése érdekében.
- A szerverhelyiségbe történő belépés engedélyezésének szabályozása. 3. számú melléklet szerint.

2.3. Rendszeres karbantartás és frissítések

- Szoftverfrissítések: Az operációs rendszerek, alkalmazások és biztonsági szoftverek rendszeres frissítése a legújabb verziókra és biztonsági javításokra.
- Hardver karbantartás: Rendszeres hardverkarbantartás és -ellenőrzés az esetleges meghibásodások megelőzése érdekében.
- Tesztelés: Az adatmentések és a katasztrófahelyreállítási tervek rendszeres, dokumentált tesztelése a hatékonyság biztosítása érdekében.
- **Tartalék erőforrás biztosítása**: Az üzleti folyamatok biztosításához szükséges azokat a tartalék erőforrásokat meghatározni és készleten tartani, amelyek képesek pótolni az incidensek következtében megsérült vagy nem elérhető erőforrásokat. A tartalék eszközök meghatározásakor figyelembe kell venni, hogy a védelem költsége arányos legyen a lehetséges kárral.

2.4. Oktatás és tudatosság

- Képzés: A munkavállalók rendszeres képzése az informatikai biztonság és a katasztrófa megelőzési intézkedések témájában.
- Incidenskezelés: A munkatársak oktatása, hogy tudják, hogyan reagáljanak és hogyan kezeljék az informatikai biztonsági incidenseket.
- Konfigurációk dokumentálása: Az összes IT rendszer konfigurációjának részletes dokumentálása.
- Vészhelyzeti kapcsolattartók:
  1. sz. melléklet Informatikai szervezet elérhetőségei;
  2. sz. melléklet Külső partnerek elérhetőségei, hibabejelentés

2.5. **Külső** partnerek és beszállítók kezelése

- SLA-**k és szerződések:** A külső partnerekkel és beszállítókkal kötött szerződéseknek tartalmazniuk kell a megfelelő titoktartási és biztonsági

követelményeket és azokat a szolgáltatási szintekre vonatkozó elvárásokat, amelyeket a szolgáltatónak teljesítenie kell.

- **Jogszabályok és belső s**zabályzatok betartatása: A külső partnerekkel és beszállítókkal kötött szerződésekben rögzíteni kell minden releváns jogszabályt és előírást, amelyek betartása elvárt a partnertől. Emellett a szerződésben ki kell térni azokra a belső szabályzatokra is, amelyeket a partner köteles megismerni és betartani.

3. IT Katasztrófavédelmi Bizottság

Az IT Katasztrófavédelmi Bizottság (továbbiakban: Bizottság) felelős az informatikai rendszerek vészhelyzeti helyreállításáért, a kritikus rendszerek és szolgáltatások működésének fenntartásáért, valamint a vészhelyzeti helyzetek gyors és hatékony kezeléséért.

Bizottság **vezetője**: Informatikai vezető

Feladata

- Felelős az IT katasztrófavédelmi stratégia kidolgozásáért és végrehajtásáért.
- Koordinálja a bizottság munkáját és irányítja a válsághelyzetekben való reagálást.
- Döntéseket hoz a kritikus rendszerek prioritásairól és helyreállítási folyamatokról.
- Katasztrófa helyzet esetén felelős a vállalat vezetősége felé történő rendszeres tájékoztatásért.
- Dönt a szakértők és / vagy harmadik fél bevonásáról.

Bizottság tagjai: Az Egyetem IT szervezetének tagjai

Feladatuk

- Katasztrófa helyzetek azonosítása.
- Végrehajtani a rendszerek napi karbantartását és monitorozását.
- Az IT rendszerek helyreállításában való közvetlen részvétel.
- Aktív részvétel a katasztrófa-helyreállítási gyakorlatokon és teszteken.
- Szoros együttműködés a koordinátorral és a többi bizottsági taggal a helyreállítás érdekében.

Bizottság speciálisan kijelölt tagjai: Olyan egyetemi dolgozók vagy külső szolgáltatók, akiket a Bizottság vezetője vészhelyzet esetén egy adott informatikai katasztrófa kezelésére jelöl ki. Ezen személyek vagy partnerek a helyzet súlyossága és a szükséges szaktudás alapján kerülnek kiválasztásra, hogy hatékonyan támogassák a Bizottságot és a helyreállítási folyamatot.

Feladatuk

- Speciális feladatok ellátása: Az eseti tagok speciális szakértelemmel rendelkeznek, amely szükséges a konkrét vészhelyzet kezeléséhez.
- A Bizottság munkájának támogatása az adott Informatikai Katasztrófa során.

Koordinátor: Az Egyetem Kancellárja

Feladata

- Felügyeli a bizottság tevékenységét.
- Részt vesz a döntéshozatalban.
- Képviseli az Egyetem érdekeit a vészhelyzeti folyamat során.

4. Informatikai incidensek kezelése

4.1. Incidens észlelés, bejelentés, értékelés

Az informatikai incidensek azonnali jelentése minden felhasználó számára kötelező az Egyetem Informatikai Szervezete felé. Az Informatikai Szervezet elérhetőségeit az 1. melléklet tartalmazza. A bejelentés a 2. mellékletben található bejelentőlap kitöltésével és benyújtásával történhet.

1. szintű incidens: Meghibásodás

Hatókör: A meghibásodás egy olyan kisebb informatikai incidens, amely során egy eszköz, rendszer, vagy alkalmazás nem működik megfelelően. Az ilyen meghibásodás nem zavarja számottevően a normális munkavégzést, nincs adatvesztés vagy adatszivárgás.

Időtartam: Rövid távú, általában néhány órán belül megoldható.

Példák: Egy szerver merevlemezének meghibásodása, egy nyomtató leállása, vagy egy szoftverfunkció működésének zavara mind meghibásodásnak minősül.

Reagálás: Ezek az események általában gyorsan és könnyen orvosolhatók, és nem okoznak fennakadást az üzleti működésben. A meghibásodások kezelése gyakran rutinszerű karbantartási vagy javítási folyamatot igényel.

2. **szintű incidens:** Üzemzavar

Hatókör: Az üzemzavar egy nagyobb kiterjedésű informatikai incidens, amely egy vagy több rendszer működésének részleges vagy teljes leállását okozza. Az üzemzavar már érezhető hatást gyakorolhat az üzleti folyamatokra, de nem jár adatvesztéssel vagy adatszivárgással.

Időtartam: Középtávú, néhány napot vesz igénybe a teljes helyreállítás.

Példák: Üzemzavar alatt például érthetünk egy adatbázis-szerver leállását, ami több alkalmazás működésképtelenségét eredményezi, vagy egy hálózati kapcsolat megszakadását, amely egy részleg munkáját megbénítja. Üzemzavar továbbá a külső szolgáltatók szolgáltatásainak kiesése, például áramszünet, internetkapcsolat kiesése vagy egy harmadik fél által nyújtott felhőszolgáltatás leállása.

Reagálás: Az üzemzavarok kezelése általában gyors beavatkozást igényel a rendszerek mielőbbi helyreállítása érdekében, és előfordulhat, hogy ideiglenes megoldásokra is szükség van, hogy minimalizálják a kiesést. Az üzletmenet folytatásához lehet, hogy tartalék rendszereket vagy szolgáltatásokat kell aktiválni. Lehetséges külső partnerek bevonása.

3. szintű incidens: Informatikai Katasztrófa

Hatókör: Az informatikai katasztrófa a legsúlyosabb informatikai incidensek egyike, amely jelentős hatással van az egész vállalatra vagy annak nagy részére.

Időtartam: Hosszú távú, több napot vagy hetet vesz igénybe a helyreállítás.

Példák: Egy informatikai katasztrófa alatt értjük például egy adatközpont teljes leállását, nagyszabású kibertámadást, amely az egész hálózatot megbénítja, kiterjedt adatszivárgást, adatvesztést, ami a vállalat működésének leállásához vezet.

Reagálás: Informatikai Katasztrófa helyzet azonnali reagálást igényel. A lehető legrövidebb időn belül tájékoztatni kell az IT Katasztrófavédelmi Bizottság vezetőjét. Az informatikai katasztrófa kezelése átfogó vészhelyzeti tervet igényel, amely magában foglalja a rendszerek és adatok helyreállítását, a katasztrófa okainak elemzését, valamint a jövőbeni hasonló események megelőzésére szolgáló intézkedések kidolgozását.

5. Informatikai Katasztrófa vészhelyzeti terv

5.1. IT Katasztrófa azonosítása

Ha a bejelentett vagy észlelt informatikai incidens kezelése során az incidens a 4.1-es pontban leírtak szerint 3. szintű incidensként, Informatikai Katasztrófaként lett értékelve, a lehető legrövidebb időn belül értesíteni és tájékoztatni kell a 3-as pontban rögzített Katasztrófavédelmi Bizottság vezetőjét.

Amennyiben a Bizottság vezetője is megerősíti az incidens biztonsági szintjét, haladéktalanul tájékoztatja az Egyetem Kancellárját, és összehívja a Katasztrófavédelmi Bizottságot. A Bizottság első feladata az incidens átfogó értékelése, beleértve a katasztrófa okainak és lehetséges következményeinek felmérését, valamint a kritikus rendszerek és szolgáltatások állapotának meghatározását.

Az értékelést követően a Bizottság átfogó akciótervet készít, amit folyamatosan frissít a vészhelyzet során. Az akcióterv tartalmazza a katasztrófa azonnali kárelhárítására, korlátozására, megszüntetésére vonatkozó lépéseket, különös tekintettel a kritikus rendszerek és szolgáltatások védelmére. Ezen túlmenően az akcióterv részletesen kitér a rendszerek helyreállítására, a működés visszaállítására vonatkozó lépésekre, valamint az érintett adatok és rendszerek helyreállításának módjaira. Az akciótervnek magában kell foglalnia a kommunikációs stratégiát is, amely biztosítja a releváns belső és külső érintettek folyamatos tájékoztatását a vészhelyzet kezelése során.

5.2. Incidens korlátozása, azonnali kárelhárítás

A kárelhárítás során a Bizottság elsődleges célja, hogy megakadályozza az incidens továbbterjedését, illetve a helyzet súlyosbodását. Ehhez először fel kell mérni az incidens pontos hatókörét és az érintett rendszerek állapotát. A kárelhárítás megkezdésekor minden érintett rendszer és eszköz, amelyet a katasztrófa érinthet, azonnali védelem alá kell, hogy kerüljön. Ennek keretében:

- Izoláció: A fertőzött vagy veszélyeztetett rendszereket és hálózatokat le kell választani a többi rendszerről, hogy megakadályozzuk az incidens további terjedését. Ez magában foglalhatja a hálózati szegmensek lekapcsolását, a kompromittált szerverek elszigetelését, vagy a veszélyeztetett adatokhoz való hozzáférés blokkolását az okozott károk minimalizálása érdekében.

- Védelmi intézkedések: Az érintett rendszereken alkalmazott biztonsági intézkedések megerősítése, például tűzfalak konfigurációjának módosítása, antivírus programok frissítése és futtatása, valamint az érzékeny adatok további védelmének biztosítása.

- Kritikus szolgáltatások átirányítása: Ha a katasztrófa kritikus üzleti szolgáltatásokat érint, szükséges lehet ezen szolgáltatások ideiglenes átirányítása alternatív rendszerekre vagy tartalék megoldások aktiválása, hogy minimalizálják az üzleti működés fennakadását.

- Kommunikáció: A kárelhárítás során folyamatosan tájékoztatni kell a Katasztrófavédelmi Bizottság tagjait és az Egyetem érintett részlegeit az aktuális helyzetről és a megtett intézkedésekről. A hatékony kommunikáció elengedhetetlen a koordinált válaszlépések biztosítása érdekében.

5.3. Incidens megszüntetése, rendszerek helyreállítása

Az incidens megszüntetése során a Bizottság elsődleges célja az esemény kiváltó okainak azonosítása és azok teljes felszámolása. Ehhez elengedhetetlen a probléma gyökerének pontos feltárása, és minden olyan tényező megszüntetése, amely lehetővé tette az incidens bekövetkezését.

- Incidens gyökérokának azonosítása: Az incidens megszüntetésének első lépése, hogy azonosítsuk a pontos kiváltó okokat. Ez magában foglalhatja a sérülékenységek feltárását, a támadási vektorok elemzését, és minden olyan körülmény megértését, amely hozzájárult az incidens bekövetkezéséhez. Ez a log fájlok átvizsgálásával és a rendszerek mélyreható vizsgálatával történik.

- Támadási vektorok lezárása: Az incidens okainak azonosítását követően, el kell zárni azokat a támadási vektorokat, amelyeken keresztül a behatolás vagy a károkozás megtörténhetett. Ez magában foglalhatja a sérülékeny szoftverek frissítését, a rosszindulatú hozzáférések letiltását, az érintett felhasználói fiókok felfüggesztését, és minden olyan hozzáférési útvonal megszüntetését, amelyet a támadók kihasználhattak.

- Érintett rendszerek megtisztítása: Az incidens során érintett rendszerek teljes körű tisztítása elengedhetetlen. Ez magában foglalja a rosszindulatú szoftverek eltávolítását, az érintett fájlok és adatok ellenőrzését, és szükség esetén a fertőzött rendszerek újratelepítését. Minden érintett rendszer esetében meg kell győződni arról, hogy az eredeti problémák megszűntek, és hogy nincsenek további rejtett fenyegetések.

- **Sebezhetőségek kijavítása:** Az incidens lezárásához szükséges a támadók által kihasznált sebezhetőségek kijavítása. Ez magában foglalhatja a szoftverek javítását, konfigurációk módosítását, valamint a biztonsági

beállítások szigorítását. Ezen túlmenően javasolt a biztonsági irányelvek felülvizsgálata és frissítése annak érdekében, hogy a hasonló incidensek a jövőben megelőzhetők legyenek.

- Érintett rendszerek és eszközök validálása: Az incidens során érintett rendszerek és eszközök ellenőrzése szükséges annak biztosítása érdekében, hogy a helyreállítás és a sebezhetőség javítására vonatkozó lépések sikeresek voltak, és hogy a rendszerek mentesek bármilyen további fenyegetéstől.

Az incidens megszüntetése során elvégzett lépések kulcsfontosságúak a rendszerek hosszú távú biztonságának biztosítása érdekében, és megalapozzák a későbbi helyreállítási és működés visszaállítási folyamatokat.

5.4. **Működés visszaállítása**

A Bizottság feladata a rendszerek helyreállítását követően a normál üzleti működés visszaállítása, ezzel biztosítva az Egyetem minden érintett területe számára, hogy zökkenőmentesen folytathassa tevékenységét:

- Folyamatok és szolgáltatások újraindítása: A helyreállított rendszerekhez kapcsolódó összes üzleti folyamatot és szolgáltatást fokozatosan újra kell indítani. Ez magában foglalja a kritikus alkalmazások elindítását, a felhasználói hozzáférések visszaállítását, valamint az adatforgalom és a kommunikáció normál állapotának helyreállítását.

- Felhasználói támogatás biztosítása: Az incidens utáni működés visszaállításának részeként létfontosságú a felhasználói támogatás megszervezése. Ez magában foglalhatja a felhasználói problémák gyors megoldását, a helyreállított rendszerek használatával kapcsolatos útmutatók biztosítását, valamint a felhasználók tájékoztatását az új biztonsági intézkedésekről.

- Átmeneti megoldások lezárása: Amennyiben az incidens ideje alatt átmeneti megoldásokra volt szükség (pl. ideiglenes rendszerek, alternatív munkafolyamatok), ezek megszüntetése és a normál folyamatokba való visszatérés.

5.5. Utólagos elemzés és jelentés

Az informatikai incidens észlelésének kezdetétől a helyreállítás befejezéséig minden eseményről és intézkedésről időrendben naplót kell vezetni. A Katasztrófa napló vezetése a Bizottság vezetőjének, illetve tagjainak a kötelessége.

A Katasztrófa napló a vezetők, a résztvevők számára információforrásként szolgál a helyreállítás folyamata során, valamint az informatikai katasztrófahelyzet utólagos elemzésekor, és az Informatikai Katasztrófaterv felülvizsgálatára is lehetőséget nyújt.

Folyamatos monitoring és visszacsatolás: Az incidens megszüntetése után is folyamatos monitoring szükséges annak érdekében, hogy időben észleljük, ha a megszüntetési lépések nem voltak teljes mértékben sikeresek, vagy ha újabb fenyegetések merülnek fel. A monitoring során szerzett tapasztalatokat visszacsatolásként kell felhasználni a biztonsági intézkedések további fejlesztéséhez.

6. A Katasztrófa Vészhelyzeti Terv tesztelése

A Katasztrófa Vészhelyzeti Terv rendszeres tesztelése elengedhetetlen annak érdekében, hogy a vészhelyzeti reagálási képességek naprakészek és működőképesek legyenek.

A tesztelés célja, hogy a Bizottsági tagok és az érintett munkavállalók megfelelő ismeretekkel rendelkezzenek a folyamatokról, valamint a terv hatékonyságának értékelése és szükséges módosításainak elvégzése.

A Katasztrófavédelmi Bizottság vezetője felel a Katasztrófa Vészhelyzeti Terv rendszeres teszteléséért. A tesztelést évente egy alkalommal kötelezően, vagy ha az Egyetem működésében olyan alapvető változás, átszervezés, kulcsfontosságú eszközbeszerzés, eszköz csere következik be, amely a Katasztrófa Vészhelyzeti Terv azonnali tesztelését igényli, a Bizottság vezetője dönt a tesztelés elrendeléséről, és kijelöli:

- a tesztelés végrehajtásának időpontját és helyszínét,
- a tesztben résztvevők körét,
- a teszt módszerét és alkalmazott módszertanát:
  Egy fiktív katasztrófa helyzetet szimulálva a résztvevők szóban kifejtik feladatukat a Katasztrófaterv lépéseinek során:
  - IT Katasztrófa azonosítása
  - Incidens korlátozása, azonnali kárelhárítás
  - Incidens megszüntetése, rendszerek helyreállítása
  - Működés visszaállítása

- Utólagos elemzés és jelentés

A Katasztrófa Vészhelyzeti Terv teszteléséről minden esetben jegyzőkönyvet kell készíteni, amely tartalmazza a következő információkat:

- a tesztelés időpontja és résztvevői
- a tesztelt vészhelyzet típusa és forgatókönyve,
- az eredmények összefoglalása,
- a javasolt fejlesztések és azok végrehajtásának határideje.

Jelen utasítás 2024. év 11 hó 01 napján lép hatályba.

Jelen utasítás a helyben szokásos módon, valamint egyetem honlapján kerül közzétételre.

Sárospatak, 2024.11.01

Prof. Dr. Kéri Szabolcs

rektor

Tokaj-Hegyalja Egyetem 2. Sárospatak

Vincze Csaba

kancellár

1. melléklet

Informatikai szervezet elérhetőségei

Informatikai biztonsági esemény vagy incidens észlelését a felhasználók kötelesek azonnal jelenteni az Egyetem Informatika szervezetének az alábbi elérhetőségeken:

Informatika szervezet központi e-mail cím: it@unithe.hu

Informatika szervezet központi telefonszáma: +36 20 745 2741

Bajusz Gábor – informatikai vezető

Tel.: +36 30 994 4562

e-mail: bajusz.gabor@unithe.hu

Tóth Péter – Szerver- és hálózatüzemeltetési informatikai vezető-helyettes

Tel.: + 36 20 745 2727

E-mail: toth.peter@unithe.hu

Tóth Dávid - informatikus

Tel.: +36 20 745 2743

E-mail: toth.david@unithe.hu

Szatmári László – informatikus

(Grand Tokaj Zrt-vel kapcsolatos ügyekért felelős)

Tel.: + 36 70 430 9936

E-mail: szatmari.laszlo@unithe.hu

2. melléklet

Incidens **bejelentő lap**

Bejelentő	neve:	
	szervezeti egysége:	
	beosztása:	
Bejelentés időpontja:		
Incidens észlelésének időpontja:		
Az incidens rövid leírása:		
Bejelentő aláírása:		
Az incidens oka (informatika tölti ki):		
A hibaelhárítás leírása (informatika tölti ki):		
A hiba következményei és az abból levonható következtetések (informatika tölti ki):		

Kelt: Sárospatak, 202.....

.....

Informatikus aláírása

3. melléklet

Szerverhelyiség Hozzáférési Engedélyek

A dokumentum célja, hogy meghatározza az Egyetem Sárospatak Eötvös út 5. szám alatti épületének földszintjén található szerverhelyiségéhez való hozzáférés szabályait és eljárásait, ezzel biztosítva a helyiség, valamint az ott tárolt eszközök és adatok biztonságát.

1. Szerverhelyiség védelme
   A szerverszoba ajtaját folyamatosan zárva kell tartani. A szerverszobába csak az informatika szervezet 2. pontban rögzített tagjai, illetve az informatikai vezető, vagy helyettese által erre feljogosított, karbantartást végző dolgozó, külső beszállító, szerződött szolgáltató léphet be a mellékletben található Belépési/Kilépési Napló aláírásával és a Vendég Belépési Szabályok elfogadásával.
   Mások számára a belépés TILOS!

2. Szerverhelyiségbe belépésre jogosultak
   Szerverszoba kulccsal az informatikai szervezet alábbi dolgozói rendelkeznek, a pótkulcs pedig lezárt dobozban a portászolgálatnál került elhelyezésre.
   - Bajusz Gábor
   - Tóth Péter
   - Tóth Dávid

3. Vendég hozzáférés:
   Külső beszállítók és szerződött szolgáltatók ideiglenes hozzáférést kaphatnak a jelen dokumentumban rögzített Belépési/Kilépési Napló aláírásával és a Belépési Szabályok elfogadásával.
   A belépésre jogosult dolgozók kötelesek állandó felügyeletet biztosítani a vendég belépő számára, illetve kötelesek a Vendég Belépési Szabályok betartását ellenőrizni.

Sárospatak,.....

Vincze Csaba

kancellár

Szerverhelyiség

Belépési/Kilépési Napló

Dátum: .....
(A belépés napja)

Időpont (Belépés): .....
(A pontos idő, amikor az illető belépett a szerverhelyiségbe.)

Időpont (Kilépés): .....
(A pontos idő, amikor az illető elhagyta a szerverhelyiségét.)

Vendég Belépő Neve: .....
(Vendég Belépő teljes neve.)

Vendég Belépő Szervezete: .....
(Vendég Belépő szervezete, akinek az alkalmazásában eljár.)

Belépés célja: .....

.....

.....
(Rövid leírás a belépés céljáról pl. karbantartás, ellenőrzés, szállítás.)

Kísérő neve: .....
(A szerverszobába belépésre engedélyezett kísérő személy neve.)

Megjegyzések: .....

.....

.....
(Bármilyen egyéb releváns információ, például rendkívüli események vagy problémák.)

Szerverhelyiség Belépési Szabályait elolvastam, tudomásul vettem és magamra nézve kötelezőnek tekintem: ..... Vendég Belépő aláírása	..... Kísérő aláírása

Tokaj-Hegyalja Egyetem - Szerverhelyiség

Vendég Belépési Szabályok

Belépési Feltételek

- A vendég belépőnek igazolnia kell magát, illetve a szervezetet, akinek az alkalmazásában eljár.
- A vendég belépési kérelmét előzetesen jóvá kell hagynia az Egyetem IT vezetőjének vagy helyettesének.
- A belépési naplóban rögzíteni kell a vendég adatait, a belépés időpontját és célját.
- A vendég kizárólag a kísérő jelenlétében tartózkodhat a szerverhelyiségben.
- A belépő csak az általa elvégzendő tevékenység időtartamára léphet be a helyiségbe.

Magatartási Szabályok

- Tilos bármilyen étel, ital vagy más anyag bevitele a szerverhelyiségbe.
- A vendég kizárólag az engedélyezett tevékenységeket végezheti, és csak az engedélyezett területeken tartózkodhat.
- A vendégnek a távozáskor alá kell írnia a belépési naplót, megadva a kilépés időpontját.

Biztonsági Előírások

- Tilos bármilyen hálózati vagy hardvereszközt módosítani, csatlakoztatni vagy leválasztani, kivéve, ha azt a kísérő belső munkatárs engedélyezte.
- A vendég nem férhet hozzá semmilyen adatforráshoz vagy szoftverhez, kivéve, ha ezt előzetesen az az Egyetem IT vezetője vagy helyettese engedélyezte.
- A vendég a belépési napló aláírásával titoktartási kötelezettséget vállal, amelyben kijelenti, hogy az itt szerzett információkat nem adja át harmadik félnek.