INFORMÁCIÓBIZTONSÁGI ÉS ÜZLETMENET-FOLYTONOSSÁGI KÖVETELMÉNYEK

A beszerzési eljárásban nyertes vállalkozás (továbbiakban: **Partner)** az MVM NET Zrt.-vel kötött szerződés (továbbiakban: **Szerződés**) alapján, illetve azzal összefüggésben végzett tevékenysége során köteles a jelen mellékletben foglalt szabályokat betartani. A jelen mellékletben foglalt bármely követelmény olyan esetben és mértékben alkalmazandó, amennyiben a Szerződés tárgya szerinti termék vagy szolgáltatás kapcsán releváns.

Bevezetés

A Partnerekkel történő szerződéses kapcsolatok során, az elektronikus hírközlési és információs technológia jellegéből fakadóan, valamint egyéb fenyegetettségekkel összefüggésben a Megrendelő MVM NET Zrt. (továbbiakban: **MVM NET**) és ügyfelei olyan biztonsági kockázatoknak lehetnek kitéve, amelyek szándékos vagy véletlen biztonsági incidensekhez vezethetnek és befolyásolhatják az elektronikus hírközlési szolgáltatási szintek teljesülését. A biztonsági kockázatok elkerülése, illetve mérséklése érdekében az MVM NET speciális biztonsági követelményeket alkalmaz beszállítóira és kiszervezett tevékenységet ellátó Vállalkozóira, hogy az alábbiakban megfogalmazott céljai teljesüljenek.

Az MVM NET Zrt., a nemzetközileg elismert, legjobb gyakorlatokon alapuló ISO/IEC 27001 szabvány követelményei alapján kialakított információbiztonság irányítási rendszert, valamint ISO 22301 üzletmenet-folytonosság irányítási rendszert vezetett be és tart fenn abból a célból, hogy a Társaság működése és szolgáltatása során:

- biztosítsa, hogy a Társaság, mint létfontosságú rendszer üzemeltető és alapvető szolgáltatásokat nyújtó vállalat megfeleljen a vonatkozó törvényi előírásoknak és rendeleteknek (ideértve, de nem kizárólag: 2013. évi L. törvény, 41/2015. (VII. 15.) BM rendelet);
- biztosítsa a Társaság által kezelt, feldolgozott, továbbított, valamint tárolt adatok kockázattal arányos védelmét (bizalmasságát, sértetlenségét és rendelkezésre állását) a felmerülő veszélyforrások ellen a 2013. évi L. törvény szerinti és az ISO/IEC 27001 szabványi előírások alapján. Függetlenül ezen információ, adat származási helyétől, forrásától, jellegétől (személyesen kapott, telefon/fax, e-mail, levél, hozzáférés engedélyezés alapú), megjelenési formájától (eredeti/másolat, szóbeli/papíralapú/elektronikus, kivonatolt/átfogalmazott/teljes);
- megfelelő eszközökkel, készségekkel, erőforrásokkal és folyamatokkal biztosítsa, hogy szolgáltatásai mindig működőképesek maradjanak, betartva az ügyfelek felé vállalt és elfogadott minimális szolgáltatási szintet;
- biztosítsa, hogy szolgáltatásai az előre meghatározott és elfogadott minimális helyreállítási időn belül helyreállhassanak akár egy súlyos biztonsági incidens esetén is.

1. Biztonságirányítás és kockázatkezelés

1.1. Információbiztonsági szabályzat

1.1.1. A Partnernek teljes mértékben meg kell értenie az MVM NET biztonsági céljait, meg kell ismernie a lefektetett biztonsági szabályait és integrálnia kell ezeket saját biztonságirányítási rendszerébe.

1.1.2. A Partnernek olyan információbiztonsági szabályzattal kell rendelkeznie, amely biztosítja termékei és szolgáltatásai biztonságát, ellenálló képességét, valamint összhangban áll az MVM NET magas szintű biztonsági elvárásaival.

1.1.3. A Partnernek bizonyítania kell, hogy rendelkezik megfelelő belső információbiztonsági szabályzattal, amely biztosítja termékei és szolgáltatásai, valamint a szolgáltatás biztosításához esetlegesen átadott üzleti titok adatok biztonságát és ellenálló képességét, ezért vállalja, hogy ezen dokumentumot, vagy ennek vonatkozó részeit és szükség szerint az alátámasztást szolgáló evidenciákat elemzés céljából, az MVM NET kérésére bemutatja.

1.1.4. A Partner, a jelen melléklet aláírásával igazolja, hogy megértette és betartja az MVM NET által meghatározott biztonsági követelményeket.

1.2. Kockázatkezelés

1.2.1. A biztonsági követelményeket az MVM NET, az általa elvégzett és meghatározott kockázatértékelések eredményei alapján határozza meg. Az MVM NET rendszereit és / vagy a Partner elektronikus hírközlési szektorban jelenlévő termékeit vagy szolgáltatásait érintő esetleges tesztek / gyakorlatok vagy események alapján feltárt kockázatok alapján jogosult változtatni a biztonsági követelményeken, amely változtatásokról a Partnert tájékoztatja. A frissített biztonsági követelményeket ezután a Partner haladéktalanul végrehajtja, majd ennek befejezését követően a teljesített intézkedésekről tájékoztatja a Megrendelőt.

1.2.2. A Partnernek és alvállalkozóinak, illetve egyéb közreműködőinek a Szerződésben foglalt kötelezettségeinek teljesítésével összefüggésben a megadott szempontok szerint Beszállítói Önértékelést kell végrehajtania. Az ennek során megadott adatokat az MVM NET a Szerződés hatálya alatt kezelheti.

1.2.3. A Partner, - anélkül, hogy ezért külön díjat vagy költséget számolna fel - vállalja, hogy az MVM NET számára jogszabályban, valamint szerződésben előírt kötelezettségei teljesítésében együttműködik.

1.3. Biztonsági szerepkörök és felelősségek

1.3.1. A félreértések és a visszaélések elkerülése érdekében a Partner köteles a szerződésben és jelen mellékletben foglalt szerepköröket és felelősségeket figyelembe véve kialakítani működési folyamatait.

1.3.2. A Partner szervezetében egy, a szerződésben általa kijelölt személynek elszámoltathatónak kell lennie a szerződés teljes időtartama alatt, annak biztosítása érdekében, hogy:

- a Partner a biztonsági kockázatokat és követelményeket teljes mértékben megértse;
- megfelelő biztonságtechnikai eljárások legyenek érvényben, és az MVM NET-tel – mindkét fél által megfelelőnek elfogadott megállapodás szülessen a maradványkockázat minimálisan elfogadható szintjéről,
- a Partnernél megfelelő folyamatokat alkalmazzanak a biztonsági kockázatok kezelésére, melynek eredményét kommunikálják az MVM NET felé;

- a Partner megfelelő támogatást nyújtson az MVM NET-nek a szerződésben meghatározott módon és szolgáltatási szinteken;
- a Partner a szerződéses feltételeket tiszteletben tartsa.

1.4. Ellátási lánc biztonsága

1.4.1. A Partnernek információkat kell szolgáltatnia azokról a meglévő és / vagy leendő alvállalkozóiról, egyéb közreműködőiről, amelyek termékeket vagy szolgáltatásokat nyújtanak az MVM NET részére.

1.4.2. Ezeket az információkat az MVM NET kockázatértékelése során felhasználja (lásd: 1.2.1. és 1.2.2. pont) és figyelembe veszi a biztonsági követelmények meghatározásakor.

1.4.3. A Partner köteles jelen szabályzatban meghatározott követelményeket az alvállalkozói szerződés részeként az MVM NET-nek nyújtott szolgáltatás tekintetében valamennyi, a szerződés teljesítésében érintett alvállalkozójától, illetve egyéb közreműködőjétől megkövetelni (pl. külső IT szolgáltató).

1.4.4. A Partner kizárólagosan elszámoltatható az alvállalkozó(i) illetve egyéb közreműködői által végrehajtott összes tevékenységért. Ezen elszámolás kiterjed arra, hogy felelős az alvállalkozói, egyéb közreműködői tevékenységéért annak érdekében, hogy az MVM NET által megkövetelt biztonsági követelmények teljesüljenek, a védelmi intézkedések hatékonyan működjenek.

2. Emberi erőforrások biztonsága

2.1. Átvilágítás

2.1.1. A Partnernek – kérésre – igazolnia kell, hogy alkalmazottai / megbízottai / alvállalkozói vagy egyéb közreműködői a megfelelő tapasztalattal rendelkeznek a biztonsági kockázatok kezelésében.

2.1.2. A termékek vagy rendszerek rosszindulatú vagy szándékos módosításának elkerülése céljából az MVM NET kérésére, összhangban az adatvédelmi és egyéb vonatkozó jogszabályi előírásokkal, és kizárólag ezen jogszabályi előírások által megengedett esetekben, a Partner köteles:

- a munkaerőfelvételt megelőzően és az alkalmazás során előre meghatározott időszakonként ellenőrizni az alkalmazottai által bemutatott erkölcsi bizonyítványokat annak igazolására, hogy ezen személyek nem szerepelnek bűnügyi nyilvántartásokban,
- az ellenőrzések végrehajtásának tényéről és a munkavállalói megfelelőségéről jelentést tenni az MVM NET részére.

2.1.3. Kérésre a Partner a Szerződés tartalmának végrehajtásában résztvevő személyek szakmai önéletrajzát – ezen személyek előzetes jóváhagyásának birtokában – megismerés céljára megküldi az MVM NET részére. Az önéletrajzokat a Szerződés hatályának lejártát követően helyreállíthatatlanul törölni kell a Megrendelő rendszereiből.

2.2. Biztonsági ismeretek és képzések

2.1.4. A Partner alkalmazottainak dokumentált és bizonyított módon, megfelelő képzést kell kapniuk az MVM NET által meghatározott biztonsági követelmények megismerésére.

2.1.5. Az MVM NET kérésére a Partnernek rendelkezésre kell állnia a szükséges, információbiztonsági és üzletmenet-folytonossági témákban képzett személyzettel.

2.1.6. A Partner kötelezettsége, hogy alkalmazottainak és alvállalkozóinak/egyéb közreműködőinek körében valamennyi természetes személynek rendszeres, legalább évente ismétlődő képzést tartson, illetve szervezzen annak érdekében, hogy ezen személyek naprakészek tudjanak maradni a fejlett technológiai környezetben folyamatosan változó biztonsági fenyegetettségek és gyakorlatok területén.

2.1.7. Partner köteles gondoskodni arról, hogy alkalmazottai megfelelő biztonsági és műszaki ismeretekkel, készségekkel és képesítéssel rendelkezzenek, azért, hogy elkerüljék a termékek vagy rendszerek véletlen módosítását. Ugyanezen célból Partnernek megfelelő változás menedzsment folyamattal és dokumentációval kell rendelkeznie. A kellő gondosság bizonyítékaival kapcsolatos konzultáció céljából Partnernek az MVM NET rendelkezésre kell állnia.

2.3. Személyzeti változások

2.3.1 A Partner vagy alvállalkozója, illetve egyéb közreműködője köteles valamennyi olyan munkavállalójával és minden olyan általa alkalmazott vagy megbízott személlyel, aki hozzáférést kap az MVM NET rendszereihez, bizalmas információkhoz vagy az ügyfelek üzleti vagy személyes adataihoz, titoktartási nyilatkozatot aláíratni. Ezen személyek valamennyien kötelesek közvetlenül az MVM NET által alkalmazott titoktartási nyilatkozatot is aláírni. A Partnernek be kell tartania a Szerződésben meghatározott titoktartásra és a személyes adatok védelmére vonatkozó záradékokat.

2.3.2 A Szerződés teljesítésében résztvevő személyek körében bekövetkező változást az MVM NET felé haladéktalanul be kell jelenteni a fentebb meghatározott személyi követelmények teljesítéséről szóló bizonyítékok párhuzamos megküldése mellett.

2.3.3 A szolgáltatás körébe tartozó személyzet esetleges cseréjéről az MVM NET-el egyeztetni kell, összeférhetetlenség esetén az MVM NET jogosult a változást elutasítani.

2.3.4 A Partnernek meg kell határoznia a dokumentált feladat- és tudásátadás folyamatát, melyet a helyettesítendő alkalmazottak között végre kell hajtania. Ennek bizonyítékát az MVM NET kérésére be kell mutatnia.

2.3.5 A Partnernek késlekedés nélkül, időzítetten vissza kell vonnia az MVM NET információs rendszereihez való hozzáférési jogot a felmentett személyzet körében. Amennyiben ez nem a Partner hatásköre, akkor haladéktalanul jeleznie kell a jogosultság visszavonási kérését az MVM NET felé.

2.3.6 Partner köteles az MVM NET által kiírt beszerzési pályázat kapcsán elkerülni az összeférhetetlenséget és annak minden olyan látszatát, amely a pályázat elbírálására vonatkozó döntés helytelen befolyásolására tett kísérlet benyomását keltheti. A Partner köteles ajánlata benyújtásával egyidejűleg az MVMNET-BSz-106-NY-09 Összeférhetetlenségi és titoktartási nyilatkozat (partnerek/ajánlattevők) az MVM NET rendelkezésére bocsátani, és amennyiben bármely összeférhetetlenség esete utóbb bekövetkezik, arról haladéktalanul értesíteni az MVM NET-et.

3. Rendszerek és létesítmények biztonsága

3.1. Fizikai és környezeti biztonság

3.1.1. A Partnernek megfelelő biztonsági folyamatokkal kell rendelkeznie, amelyek biztosítják termékei és/vagy rendszerei fizikai biztonságát és megakadályozzák a fizikai létesítményekhez és infrastruktúrához való illetéktelen hozzáférést, ideértve, de nem kizárólag:

- a gyártási vagy szolgáltatási helyszínek, létesítmények biztosításának eljárásait;

- eljárásokat a tároló helyiségek, irattárak biztonságára;
- az üzemeltetési létesítmények biztosításának eljárásait;
- a berendezések, bizalmas küldemények, adathordozók csomagolásának és szállításának biztonságára vonatkozó eljárásokat.

3.1.2. A fizikai biztonsági folyamatok hatékony működtetéséről szóló bizonyítékokat elemzés céljából, kérésre meg kell osztani az MVM NET-el.

3.1.3. A biztonsági folyamatokat a Partnernek figyelemmel kell kísérnie és szükség szerint fejlesztenie kell.

3.1.4. A Partnernek rendszeresen mérnie és értékelnie kell a biztonsági folyamatok hatékonyságát és szükség esetén felül kell vizsgálni azokat, különösen az MVM NET rendszereit és / vagy a Partner elektronikus hírközlési ágazatban jelenlévő hasonló termékeit vagy szolgáltatásait érintő incidenseket, vagy teszteket továbbá gyakorlatokat követően.

3.2. Hálózatokhoz és információs rendszerekhez történő hozzáférések ellenőrzése

3.2.1. A Partnernek speciális logikai hozzáférés-ellenőrzéssel kell rendelkeznie, amelyek biztosítják termékei vagy rendszerei biztonságát és megakadályozzák a hálózataihoz és információs rendszereihez való illetéktelen hozzáférést: ideértve, de nem kizárólag:

- felhasználó azonosítás és hitelesítés, naplózás;
- egyedi azonosítók;
- felelősségek különválasztása;
- privilégium alapú hozzáférési csoportok.

3.2.2. Az MVM NET rendszerei vonatkozásában a logikai hozzáférés-ellenőrzések bizonyítékait elemzés céljából meg kell osztani az MVM NET-el, legalább éves rendszerességgel, (értelmezhető formában).

3.2.3. A Partnernek rendszeresen értékelnie kell a biztonsági folyamatok hatékonyságát és szükség esetén felül kell vizsgálni, különösen teszteket / gyakorlatokat vagy az MVM NET rendszereit és / vagy a Partner elektronikus hírközlési ágazatban jelen lévő hasonló termékeit vagy szolgáltatásait érintő események után.

3.2.4. Az érzékeny hálózatokhoz és információs rendszerekhez való hozzáférést a Partner azon alkalmazottjaira, alvállalkozóira és egyéb közreműködőire kell korlátozni, akiknek a Szerződés teljesítése érdekében elengedhetetlen a hozzáférés biztosítása.

3.2.5. Kizárólagosan az MVM NET által meghatározott követelményeknek megfelelő eszköz csatlakoztatható az MVM NET érzékeny hálózataihoz és információs rendszereihez.

3.2.6. A Partnernek rendszeresen, de legalább évente, dokumentáltan felül kell vizsgálnia a hálózatok és információs rendszerek hozzáférési listáit, egyénenként ellenőrizve a felhasználók jogait és kiváltságaival.

3.2.7. A Partnernek rendszeresen, de legalább évente, dokumentáltan ellenőriznie kell a tevékenységnaplót annak érdekében, hogy felismerje a rendellenes viselkedést. Ezt az ellenőrzést harmadik félnek kell elvégeznie (pl. független minőségellenőr a Partner szervezeten belül).

3.2.8. A Partnernek ki kell alakítania és alkalmaznia kell azokat a rendszereket, amelyek észlelik és rögzítik a módosítási kísérleteket, illetéktelen hozzáféréseket vagy károkozást.

3.3. Hálózati és információs rendszerek integritása

3.3.1. A Partnernek rendszeresen, de legalább évente, dokumentáltan ellenőriznie kell a termék vagy a rendszer integritását megfelelő sérülékenység vizsgálattal és teszteléssel, mielőtt az integrálódna az MVM NET infrastruktúrájába.

3.3.2. A tesztelési / sérülékenység vizsgálati eljárásokat és eredményeket, a meghozott intézkedéseket, elemzés céljából meg kell osztani a szolgáltatóval.

3.3.3. Kockázatos vagy illetéktelenül módosított elemek találata esetén a Partnernek megfelelő intézkedéseket kell végrehajtania annak cseréjére, biztosítva a szolgáltatás folytonosságát és a korábbi elvárt biztonsági szintet.

4. Üzemeltetés biztonság

4.1. Üzemeltetési eljárások

4.1.1. A szerződés részeként a Partnernek meg kell egyeznie az MVM NET-el egy olyan szolgáltatási szintről (SLA), amely mérhető módon meghatározza, hogy a Partner milyen szolgáltatásokat nyújt. Ez magában foglalja:

- a szolgáltatás minimális szintjét, amelyet az MVM NET elfogad;
- a maradványkockázatok minimális szintjét (miután a védelmi intézkedések megvalósultak), amelyet az MVM NET elfogad;
- biztonságorientált kulcsfontosságú teljesítménymutatókat (KPI), amelyek alapján az MVM NET értékeli a Partner teljesítményét.

4.1.2. A Partner teljesítménye az MVM NET részéről rendszeresen értékelésre kerül, amelynek során az MVM NET hivatkozik a szerződéses SLA-ra.

4.1.3. A Partnernek meg kell adnia minden olyan támogató adatot, nyilvántartást vagy jelentést, amely megkönnyíti a termék vagy szolgáltatás teljesítményének értékelését. Ezenkívül a Partnernek meg kell osztania az MVM NET-el az adatok, a nyilvántartások vagy a jelentések teljes megértéséhez szükséges tudást.

4.2. Változáskezelés

4.2.1. A Partnernek változáskezelési folyamatokat kell fenntartania. Különböző folyamatok valósíthatók meg a szükséges változtatások típusa alapján, például, de nem kizárólagosan:

- újonnan felfedezett biztonsági rés, amely további biztonsági intézkedések alkalmazásához vezet;
- szoftver frissítés;
- hardvercsere;
- naprakész adatbázisú vírusirtó.

4.2.2. A változáskezelési folyamatnak tartalmaznia kell a pontos és hatékony tesztelést (lásd: 7. pont). A Partnernek tesztelnie kell minden szoftver vagy hardver változását, mielőtt integrálódna az éles környezetbe. A Partnernek bizonyítékokat kell szolgáltatni az MVM NET felé a végrehajtott tesztelésekről.

4.2.3. A változás megindításának és a többletköltségek kifizetésének felelősségét a szerződésben kell meghatározni.

4.2.4. A Partnernek felelősséget kell vállalnia az alábbiakkal kapcsolatos változásokért:

- bármely általa kezdeményezett változásokért;
- a szerződésben elfogadott egyéb változtatásokért (pl. frissítésekért);

- az általa okozott eltérésekért a szolgáltatási szintekben;
- újonnan felfedezett biztonsági résekért a saját termékében vagy rendszerében.

4.2.5. Biztonsági incidensek bekövetkezését követően a Partnernek korrekciós intézkedéseket kell hoznia, ezekről tájékoztatást kell nyújtson a Megrendelő felé.

4.3. Szerződéses kapcsolat megszűnése

4.3.1. Amennyiben a szerződéses kapcsolat még a megállapodás lejárta előtt véget érne a Partnernek meg kell határoznia és meg kell egyeznie az MVM NET-el egy átmeneti tervben, amely biztosítja a biztonság kezelését, amíg az átadás – az MVM NET-nek vagy egy általa meghatározott másik jogi személynek – befejeződik.

4.3.2. A Partnernek át kell adnia a termékkel vagy szolgáltatással kapcsolatos összes dokumentumot, eljárást, konfigurációt, nyilvántartást stb., amelyek szükségesek a szolgáltatás zavartalan folytatásának biztosításához az MVM NET számára.

4.3.3. A Partnernek vissza kell adnia vagy helyreállíthatatlanul meg kell semmisítenie az MVM NET adatait tartalmazó összes fájlt, rekordot, dokumentumot.

4.3.4. Felek megállapodása alapján a fenti 4.3.1 - 4.3.3 pontokban rögzített átadást haladéktalanul, de legkésőbb a szerződéses kapcsolat megszűnését követő 8 napon belül végre kell hajtani.

4.3.5. Abban az esetben, ha a Felek bizonyos információk megőrzéséről egyeztetnek, a Partnernek az egyeztetést követően haladéktalanul, de legkésőbb annak befejezését követő 8 napon belül végre kell hajtania az adatok titkosságának és védelmének biztosítását garantáló biztonsági intézkedéseket.

4.4. Beszállított termékek és szolgáltatások kezelése

4.4.1. A Partnernek fent kell tartania a változáskezelési folyamatokat (pl. szoftverfrissítés, hardvercsere stb.) (Lásd 4.2.pont).

4.4.2. A Partnernek mérlegelnie kell azt az időkeretet, amelyen belül termékei vagy rendszerei várhatóan elavulnak (életciklus vége), erről köteles tájékoztatni az MVM NET-et.

4.4.3. A Partnernek rendszeresen ellenőriznie kell termékeit és rendszereit az elavulás korai jeleinek észlelése érdekében.

4.4.4. A Partnernek ki kell dolgoznia és végre kell hajtania egy csere- vagy frissítési tervet, figyelembe véve a kompatibilis termékek, pótalkatrészek és kompatibilis frissítések elérhetőségét a meglévő infrastruktúrával az MVM NET szolgáltatások folyamatosságának biztosítása érdekében.

4.4.5. A Partnernek bizonyítékot kell szolgáltatnia arról, hogy hatékony logisztikai funkcióval rendelkezik az alkatrészei, termékei és rendszerei nyilvántartásának kezelésében, és ésszerű időn belül biztosítja azok rendelkezésre állását vagy megfelelő helyettesítő alkotóelemek elérhetőségét.

4.4.6. A Partnernek garantálnia kell a kritikus alkatrészek, termékek vagy rendszerek cseréjét vagy frissítését az MVM NET-tel kötött szerződésben megállapított határidőn belül, hogy elkerülje az MVM NET-tel szembeni szolgáltatás szintek megsértését (lásd: 6.3 fejezet).

4.4.7. A Partnernek értesítenie kell az MVM NET-et, amikor a termék frissítése elérhető.

4.4.8. Cseréhez vagy frissítéshez a Partnernek támogatást kell nyújtania.

4.4.9. A szerződés részeként mindkét félnek meg kell állapodnia arról a minimális időtartamról, amelyen belül a Partner támogatja a terméket.

4.5. Információk és adatok védelme

4.5.1. A Partner kizárólag arra a célra használhatja fel az MVM NET-től kapott információkat, amely célra azokat a Partner részére átadták, és kizárólag addig a mértékig, és annyi ideig ameddig a Szerződés teljesítéséhez szükséges.

4.5.2. A Partnernek haladéktalanul vissza kell adnia vagy helyreállíthatatlanul meg kell semmisítenie az MVM NET információit tartalmazó összes fájlt, rekordot, dokumentumot amennyiben a Szerződés teljesítéséhez már nem szükséges.

4.5.3. Amennyiben az MVM NET megbízásából a Partner személyes adatfeldolgozást hajt végre, úgy az Adatvédelmi és adatfeldolgozási szerződésben meghatározottak az irányadóak.

4.5.4. Amennyiben a Partner a szerződés teljesítésével összefüggésben az MVM NET adatait felhő szolgáltatás igénybevételével kívánja kezelni vagy tárolni, MVMhoz az MVM NET előzetes, írásbeli hozzájárulása szükséges.

4.5.5. Csak titkosított mobil eszközön és adattárolón tárolhatóak és szállíthatóak az MVM NET üzleti adatai.

5. Incidensek kezelése

5.1. Incidens kezelési eljárások

5.1.1. A Partnernek sürgősségi eljárást kell alkalmaznia az esetleges incidensek kezelésére és / vagy az MVM NET támogatására, rendkívüli események esetén. Az eljárás az események típusait, a felek szerepét és felelősségét, az eszkalációs folyamatot stb. tartalmazza.

5.1.2. A Partnernek rendelkeznie kell egy szolgáltatás-folytonossági tervvel (lásd 6.3. pont) és egy katasztrófa utáni helyreállítási tervvel (lásd 6.4. pont), hogy minimalizálja az MVM NET szolgáltatásainak rendelkezésre állásával kapcsolatos incidens hatását.

5.1.3. A Partnernek be kell tartania az SLA-ban meghatározott és az MVM NET-el egyeztetett átlagos javítási és helyreállítási időt.

5.1.4. A Partnernek értékelnie kell minden incidenskezelési esetet, és az MVM NET számára jelentést kell készítenie róla (lásd: 5.2. pont).

5.1.5. Ha az incidenskezelési eljárás fejlesztése szükséges, a Partnernek egyes fejlesztési tevékenységről (pl. jobb munkafolyamatok, új kapcsolattartási módok stb.) az MVM NET-el szükség szerint meg kell állapodni és azokat a Partnernek késlekedés nélkül meg kell valósítania (lásd 5.2. pont).

5.2. Incidensek jelentése és kommunikálása

5.2.1. A Partnernek folyamatokat kell fenntartania annak érdekében, hogy pontosan és időben jelentse az MVM NET-nek a termékeivel vagy szolgáltatásaival kapcsolatos biztonsági eseményeket, biztonsági incidenseket, továbbá az MVM NET-el kapcsolatos bármely adatbiztonsági incidenst, valamint a szerződésben meghatározott vagy törvény által előírt biztonsági követelmények megsértését.

- A Partnernek haladéktalanul, előzetes figyelmeztetést kell kiadnia, ha rendellenességet, gyanús eseményt vagy körülményt észlel, vagy mulasztás gyanúja áll fenn.
- A Partnernek be kell jelentenie az MVM NET infrastruktúrájában bekövetkezett incidenseket, mulasztásokat, feltételezett mulasztásokat vagy egyéb rendellenességeket.

5.2.2. A rendkívüli működés kapcsán a Partnernek küszöbértéket kell az MVM NET-el közösen meghatározni, hogy a Partner csak az indokolt riasztásokat jelentse azok kritikussága alapján.

5.2.3. A Partnernek jelentenie kell az MVM NET felé minden olyan eseményt, amely termékeivel vagy szolgáltatásaival az elektronikus hírközlési ágazatban bekövetkezett (vagyis más szolgáltatókat érintett), abban az esetben, ha ugyanazon termékekre és szolgáltatásokra az MVM NET-tel is szerződött.

5.2.4. Világos eszkalációs folyamatot kell kialakítani a Partner és az MVM NET között a jól meghatározott és hatékony kommunikációs folyamat biztosítása érdekében. Az 5.2.1 és 5.2.3 pontokban meghatározott eseményeket a lehető legrövidebb időn belül a következők szerint kell jelenteni:

- szerződés szerinti kapcsolattartó részére;
- Biztonsági Irányítási Terület (BIT) részére: bit@MVMnet.hu
- Hálózatfelügyeleti osztály (NOC) részére: noc@MVMnet.hu

5.2.5. A Bekövetkezett incidensek esetén a Partnernek ki kell vizsgálnia, illetve támogatnia kell az MVM NET-et az esetleges vizsgálatban, vagy fel kell kérnie egy harmadik felet a kivizsgálás folyamán, hogy megtalálják a kiváltó okokat. Erről a szerződésben vagy ennek hiányában eseti alapon is meg lehet állapodni.

5.2.6. Ha szükséges, a további események elkerülése érdekében az MVM NET-el meg kell állapodni a korrekciós intézkedésekről, amelyeket a Partner hajt végre, és melynek eredményét az MVM NET ellenőrizheti.

6. Üzletmenet-folytonosság irányítás

6.1. Szolgáltatások folytonossági stratégiája és folytonossági tervei

6.1.1. A Partnernek eszközökkel, készségekkel, erőforrásokkal vagy folyamatokkal kell biztosítania, hogy az MVM NET szolgáltatásai mindig működőképesek maradjanak, betartva az SLA-ban meghatározott és az MVM NET által elfogadott minimális szolgáltatási szintet. Ilyenek lehetnek (nem kizárólag):

- pótalkatrészek;
- biztonsági mentés;
- helyettesítő személyzet a kritikus funkciók fenntartásának biztosítása érdekében.

6.1.2. A Partnernek teljeskörű dokumentációt kell szolgáltatnia az üzletmenet-folytonossági folyamatokról. A Partnernek rendelkeznie kell a szolgáltatás folytonosságát biztosító tervvel, különösen, de nem kizárólag az áramellátás esetleges meghibásodására.

6.1.3. A Partner üzletmenet-folytonossági tervének figyelembe kell vennie az alvállalkozók/egyéb közreműködők függőségét.

6.1.4. A Partnernek a bekövetkező és a múltbeli incidensek, valamint korábbi tapasztalatok, adott szektorban megtörtént események alapján, illetve legalább éves rendszerességgel felül kell vizsgálnia a szolgáltatás folytonossági tervét és szükség esetén módosítania kell.

6.2. Katasztrófa utáni helyreállítási képességek

6.2.1. A Partner eszközökkel, készségekkel, erőforrásokkal vagy folyamatokkal biztosítja, hogy az MVM NET szolgáltatásai az SLA-ban meghatározott minimális helyreállítási időn belül helyreállhassanak egy súlyos incidensből. Ilyenek lehetnek többek között:

- pótalkatrészek;

- biztonsági mentés;
- helyettesítő személyzet a kritikus funkciók fenntartásának biztosítása érdekében.

6.2.2. A Partner helyreállítási tervében figyelembe kell venni az alvállalkozók / egyéb közreműködők függőségét.

6.2.3. A Partnernek a bekövetkező és a múltbeli incidensek, valamint korábbi tapasztalatok, adott szektorban megtörtént események alapján, és legalább éves rendszerességgel felül kell vizsgálnia a szolgáltatás helyreállítási tervét, és szükség esetén módosítania kell.

6.2.4. Az MVM NET kérésére a Partner közös gyakorlaton vesz részt az MVM NET-el, hogy felkészüljenek az esetleges rendkívüli helyzetekre (például: viharok, katasztrófa események, a kritikus hálózati berendezések meghibásodásai stb.).

7. Figyelemmel kísérés, felülvizsgálatok és tesztelés

7.1. Figyelemmel kísérési és naplózási szabályok

7.1.1. A Partnernek folyamatosan figyelnie kell minden olyan rendellenes tevékenységet, amely az MVM NET hálózatának és rendszerének elérhetőségével vagy integritásával kapcsolatos problémákat jelezhet.

7.1.2. Az esetleges rendellenességeket a Partnernek ki kell vizsgálnia.

7.1.3. Az esetleges rendellenességeket haladéktalanul jelenteni kell az MVM NET-nek (lásd 5.2. pont).

7.2. Hálózati és információs rendszerek tesztelése

7.2.1. A termék vagy szolgáltatás minőségét és biztonságát a Partnernek a szerződésben meghatározott előírások alapján kell értékelnie, mielőtt az integrálódna az MVM NET rendszerébe. Néhány elfogadási kritériumot az MVM NET beállíthat és a termék vagy berendezés elutasítható, ha az nem felel meg az MVM NET szerződésben egyértelműen meghatározott elvárásainak. A folyamat új komponensekre, javításokra és frissítésekre is érvényes.

7.2.2. A Partnernek gondoskodnia kell a rendszeres, pontos és hatékony tesztelésről, és biztosítania kell, hogy a termékek és szolgáltatások a megfelelő módon működjenek:

- a tesztelést a termék / szolgáltatás teljes életciklusa mentén kell elvégezni: a fejlesztési fázistól kezdve, a meglévő hálózathoz való integráció előtt és után, valamint bármilyen javítás vagy frissítés végrehajtásakor;
- a tesztelést megfelelő konfigurációval kell elvégezni - tesztkörnyezetben, ha lehetséges, az éles környezet konfigurációit (vagy helyettesítését) szimulálva;
- a tesztelést iterációkkal kell elvégezni, hogy a Partner szükség esetén javításokat hajthasson végre;
- többféle tesztet kell végrehajtani, beleértve, de nem kizárólag, az ismert sérülékenységek vizsgálatát, behatolási teszteket, forráskód-elemzéseket stb.

7.2.3. A tesztelést a Partner, az MVM NET, egy harmadik fél és / vagy egy közreműködő szervezet végezheti el (az MVM NET és a Partner tesztelőivel együttesen). A tesztelésért felelős felekről, a tesztelés gyakoriságáról a szerződésben kell megállapodni.

7.2.4. A tesztelési terveket és módszereket rendszeresen felül kell vizsgálni a technológiai változások, a frissítések és a múltbeli incidensek alapján.

7.2.5. A Partnernek átfogó vizsgálati jelentést kell megosztania az MVM NET-el, amely tartalmazza a vizsgálati eljárásokat, az azonosított sebezhetőségeket, a szükséges

mérséklő intézkedéseket és egyértelmű eszkalációs folyamatot, a további problémák esetére.

7.3. Biztonság értékelés

7.3.1. A szerződéses kapcsolatot megelőzően a Partnernek dokumentációt kell benyújtania az MVM NET részére a termékek, szolgáltatások és rendszerek ismert, lehetséges sérülékenységeiről, valamint azok kritikusságáról és bekövetkezési valószínűségéről.

7.3.2. A Partnernek olyan folyamatot kell bevezetnie és működtetnie, amely haladéktalanul értesíti az MVM NET-et az újonnan felfedezett és kihasználható biztonsági résekről (lásd: 5.2. pont).

7.3.3. A Partnernek figyelembe kell vennie a fenyegetések alakulását, és rendszeresen felül kell vizsgálnia az ipari biztonsági figyelmeztetéseket / szabványokat az esetleges új sérülékenységek felmérése érdekében.

7.4. Megfelelés figyelemmel kísérése

7.4.1. Rendszeres egyeztetéseket kell szervezni a Partner és az MVM NET között, hogy értékeljék a Partner teljesítményét a biztonsági követelmények alkalmazásával kapcsolatban.

7.4.2. A Partnernek biztosítania kell, hogy a biztonsági kockázatokat kezeljék, és a követelményeket a szerződésben megállapodottak szerint teljesítsék. A feleknek meg kell állapodniuk a biztonsági követelmények teljesülését összefoglaló jelentés hatásköréről, módszertanáról és gyakoriságáról. Ennek többféle megoldása lehetséges, például:

- A Partner a szolgáltatás részeként jelentheti a biztonsági állapotot, kockázatokat, sérülékenységeket és eseményeket.
- A Partner rendszeres független felülvizsgálatot kérhet szolgáltatási vagy gyártási folyamatairól, létesítményeiről és az eredményekről, valamint az azonosított korrekciós intézkedésekről jelentést küld az MVM NET részére. Figyelembe vehető, hogy ez az intézkedés költségekkel járhat az Partner számára, ezért külön megállapodás alapján, eseti jelleggel alkalmazzák.
- Az MVM NET hozzáférési és felülvizsgálati joggal (pl. csak betekintés) rendelkezhet a Partner szolgáltatásaival vagy gyártási folyamataival kapcsolatban, beleértve a berendezéseket, szoftvereket, információkat, nyilvántartásokat, adatokat vagy az MVMhoz kapcsolódó személyeket. Ezen hozzáférés, illetve felülvizsgálat kapcsán - szükség esetén, és az MVM NET előzetes írásbeli felhatalmazása alapján - harmadik fél is eljárhat az MVM NET nevében.
- Külső független fél általi tanúsítással bizonyosság szerezhető (pl. ISO 27001).

7.4.3. A Partner Szerződésben vállalt kötelezettségeinek teljesítését igazoló dokumentum (SAP TIG) nem írható alá a biztonsági követelmények teljesülését összefoglaló jelentés MVM NET általi elfogadása nélkül.