JÁSZ-PLASZTIK KFT.

Megnevezés:

Információbiztonsági Szabályzat

Külső felek részére

Készítette: Kovács Zoltán

IT Csoportvezető

Ellenőrizte: Megyesi Béla

Belső Auditor

Jóváhagyta: ifj. Kasza Lajos

Műszaki és Kereskedelmi Igazgató

Jóváhagyás dátuma: 2021.05.01

Ellenőrzés: Évente

TARTALOMJEGYZÉK

CÉLJA

Meghatározni azokat az információbiztonsági előírásokat, amelyeket a külső feleknek be kell tartaniuk a Jász-Plasztik Kft. információi és/vagy informatikai eszközei (pl. Személyi számítógépek, munkaállomások és mobil eszközök) használatakor.

Külső félnek minősül bármely harmadik fél, amely szerződéses kapcsolat alapján nyújt szolgáltatásokat a Jász-Plasztik Kft. részére. E meghatározás nem terjed ki a Jász-Plasztik Kft. leányvállalataira.
Ezen szabályzat a külső felek menedzsmentjére, alkalmazottjaira és az érintett alvállalkozókra irányul.

Az információbiztonsági szabályzat védi az információk bizalmasságát, integritását és elérhetőségét, valamint a megrendelő és minden olyan természetes és jogi személy jogait és érdekeit, akik üzleti kapcsolatot tartanak fenn a megrendelő féllel és/vagy munkát végeznek részére.

ALAP KÖVETELMÉNYEK

A jelen dokumentum hatálya alá tartozó valamennyi külső félnek be kell tartania az alábbi követelményeket.

Szervezeti követelmények:

Figyelembe kell vennie az adott vállalatnak a megrendelő félhez nem tartozó informatikai eszközöknek a Jász-Plasztik Kft. telephelyeire vagy biztonságos területeire történő behozatalára vonatkozó szabályait.

A megrendelő félhez tartozó szoftverek vagy adatok felhasználása olyan informatikai rendszereken vagy tárolóeszközökön, amelyeket sem a megrendelő fél, sem a szállító nem hagyott jóvá, nem megengedett.

A Jász-Plasztik Kft.-hez tartozó szoftverek és adatok felhasználása olyan fájlszolgáltatásokon vagy internetes felhőszolgáltatásokon, amelyeket a megrendelő nem hagyott jóvá, nem megengedett.

Az adatok harmadik felek részére történő továbbítása csak a megrendelő adattulajdonosának írásbeli jóváhagyásával engedélyezett.

Be kell tartani a megrendelő által a személyes adatok használatára, tárolására és bármilyen feldolgozására vonatkozó előírásokat.

A vállalkozó munkavállalóit a vállalatvezetésüknek kötelezniük kell a titoktartásra, a vállalkozó és a megrendelő közötti titoktartási megállapodással összhangban. A megrendelő fél bármikor megvizsgálhatja ezeket a megállapodásokat.

Ha a megrendelő adatait mobil rendszereken vagy informatikai eszközökön tárolják, azokat hardver vagy szoftver segítségével titkosítani kell.

Külföldi utazás előtt be kell tartani a biztonsági használatára (pl. Titkosítás) vonatkozó országspecifikus előírásokat.

A szerződés megszűnése után a megrendelő adatait át kell adni és törölni kell a szállító eszközein és adathordozóin. A jogszabályi előírásokat (pl. Megőrzési időszakok) be kell tartani.

Az emberi erőforrások biztonsága

A már nem szükséges felhasználói azonosítót vagy a hozzáférési engedélyt, amelyre már nincs szükség a megrendelő adataihoz való hozzáféréshez, haladéktalanul jelenteni kell a megrendelő félnek és a felelős egységeknek (pl. A megrendelő rendszergazdája), hogy a megfelelő blokkolás/törlés megtörténhessen.

A már nem szükséges azonosító adathordozókat (például intelligens kártyákat, SecurID kártyákat) azonnal vissza kell küldeni a megrendelő félnek.

A kiosztott eszközöket (pl. Laptopokat), adatokat és adathordozókat vissza kell juttatni a megrendelő félnek, amikor már nincs rájuk szükség, vagy a megbízás végén.

A hitelesítéshez használt informatikai eszközök vagy adathordozók elvesztését azonnal jelenteni kell a megrendelő felelős egységének.

Fizikai és környezeti biztonság

Azokat az informatikai eszközöket, amelyek a megrendelő adatait tárolják vagy dolgozzák fel, úgy kell használni, hogy az illetéktelen személyek ne férhessenek hozzá az adatok megtekintéséhez vagy eléréséhez. Különös figyelmet kell fordítani a mobil eszközök használatára.

A bizalmas és titkos dokumentumokat nem szabad felügyelet nélkül hagyni az illetéktelen megtekintés megakadályozása érdekében.

Médiakezelés

Az adathordozókat (pl. CD-k, DVD-k, USB-meghajtók, merevlemezek) biztosítani kell az elvesztés, megsemmisülés és keveredés, valamint az illetéktelen felek hozzáférése ellen.

A már nem szükséges adathordozókat biztonságos körülmények között ártalmatlanítani kell.

Információcsere

A bizalmas vagy titkos információkról folytatott minden megbeszélés során, beleértve a telefonhívásokat és a webes vagy videokonferenciákat, biztosítani kell, hogy ezeket ne hallhassák le engedély nélkül.

A faxszámokat és e-mail címeket az aktuális kommunikációs könyvtárakból kell venni, vagy kérni kell a címzettől, hogy megakadályozzák az adatok helytelen továbbítását.

Az IT -eszközök és adathordozók szállításakor a megrendelő üzem határain túl, be kell tartani az adott csoporttársaság előírásait és működési megállapodásait.

Az e-mail küldőjeként a szerző felelős a tartalomért és a terjesztésért. Lánclevelek létrehozása és küldése nem megengedett.

Információbiztonsági incidensek kezelése

A megrendelő fél adatait vagy rendszereit érintő információbiztonsági eseményeket (pl. Sebezhetőségek, az információbiztonsági rendelet megsértése) azonnal jelenteni kell a felelős egységnek.

A megrendelő fél informatikai rendszereit érintő gyanított sebezhetőségeket és gyenge pontokat jelenteni kell a felelős egységnek. A sérülékenységek és gyenge pontok tesztelését (pl. Penetrációs teszt) csak a felelős egység végezheti el.

A bizalmas vagy titkos információk elvesztésének feltételezett gyanúját haladéktalanul jelenteni kell a felelős egységnek.

Megfelelőség
A megfelelőségmenedzsmentnek, amely betartja a jogi és szervezeti követelményeket (beleértve az erőforrás-kezelést, a belső kontrollrendszert, az IT-folytonosság-kezelést és az információvédelmet), a szállítónak kell végrehajtania a megrendelő fél összes információját, hardverét és szoftverét lefedve.

A megfeleléskezelésnek a következő szempontokat kell tartalmaznia:

A kockázatok korai felismerése
Meg kell határozni az informatikai rendszereket és adatokat érintő kockázatok és potenciális fenyegetések korai felismerésének folyamatát. Megelőző intézkedéseket és intézkedéseket kell tenni az észlelt kockázatok csökkentése érdekében.

Szellemi tulajdonjogok / Licenckezelés
A szellemi tulajdonhoz fűződő jogokat (pl. A szoftverek, dokumentumok és egyéb képanyagok szerzői jogait, a tervezetekhez fűződő jogokat, védjegyeket, szabadalmakat és forráskód -licenceket) be kell tartani.

Engedély nélküli szoftver (kalózmásolat) használata nem megengedett.

A licencszoftverre a szerzői jogi védelem törvényi rendelkezései vonatkoznak (pl. A szoftver reprodukálása, kivéve a biztonsági mentés és archiválás célját, a szerzői jog megsértését jelenti). E rendelkezések megsértése büntetőintézkedésekhez, valamint jogsértési és kártérítési követelésekhez vezethet.

A licencszoftvert csak a megbeszélt célra szabad használni, és kizárólag a meglévő rendelkezéseknek és a gyártóval kötött licencszerződéseknek megfelelően.

Adatvédelem
Be kell tartani a vonatkozó nemzeti adatvédelmi törvényeket és előírásokat.

A szállító cég vezetése kötelezi a vállalkozókat, hogy tartsák be az adatvédelemre vonatkozó jogszabályi követelményeket.

Szerződéses megfelelés
A beszállító informatikai szervezetének meg kell felelnie a megrendelő szerződéses követelményeinek. Intézkedéseket kell végrehajtani annak biztosítására, hogy a beszállítók saját szervezeti szabályzatát felülvizsgálják és frissítsék az aktuális szerződéses követelményeknek megfelelően.

Irányelvek és rendeletek
A szállítónak irányelveket és előírásokat kell biztosítania alkalmazottai számára annak biztosítása érdekében, hogy a megrendelő megfeleljen a követelményeknek, és megfelelően kezelje az információkat, hardvereket és szoftvereket.

Szabálysértések és végrehajtás
Az információbiztonsági irányelvek megsértését egyénileg kell követni a vonatkozó működési, szerződéses és jogi előírások vagy megállapodások szerint, és megfelelően szankcionálni kell.

Titoktartás

Titoktartási megállapodások

A Cég információbiztonságával kapcsolatos védelmet, azok harmadik fél felé történő továbbításának megakadályozását a partnerekkel történő megállapodások, szerződések, illetve a dolgozók munkaszerződése és munkaköri leírása tartalmazza. A szükséges elvárásokat és követelményeket a titoktartásra vonatkozóan a vállalat vezetősége határozza meg és a szerződést, megállapodást aláírók számára.

Bármely, csoporthoz nem tartozó ügyfél adatait nem szabad a megadott informatikai eszközökön feldolgozni.

Az informatikai eszközök és a megrendelő adatainak a szállító alkalmazottai általi használatához a megrendelő kifejezett hozzájárulása szükséges. A megrendelő fél bármikor jogosult megtiltani a hozzáférést / felhasználást (pl. Visszaélés esetén).

Külső partnerekkel történő titoktartás

Minden külső partnerrel történő szerződés része a titoktartási nyilatkozat, illetve ennek hiányában erről külön dokumentáció gondoskodik.

Speciális / egyéni titoktartási megállapodást kell készíteni az érintett Üzleti terület vezetőjének, ha a folyamat/cél érzékeny adatokat érint.

Külső munkatársak vagy szerződéses felek csak abban az esetben kaphatnak hozzáférési jogot a Cég adataihoz, amennyiben titoktartási nyilatkozatot írnak alá.

A titoktartási követelmények szerepeltetése a szerződésekben, illetve az egyedi megállapodások aláíratása és lefűzése az adott Üzleti terület vezetőjének feladata és hatásköre.

A felek különösen, de nem kizárólagosan az alábbi adatokat tekintik Bizalmas Információknak:
- JÁSZ–PLASZTIK Kft. partnereivel, alvállalkozóival, beszállítóival és munkavállalóival kapcsolatos adatok;
- JÁSZ–PLASZTIK Kft. termékeivel, gyártási módszereivel és folyamataival, üzleti tevékenységével, áraival, bevételével kapcsolatos adatok;
- JÁSZ–PLASZTIK Kft. jövőbeli tervei, azzal kapcsolatos adatok és információk.

A Titoktartásra kötelezett kötelezettséget vállal arra, hogy üzleti titkot, bizalmas információt nem tesz hozzáférhetővé harmadik személy számára, azt kizárólag a szerződésben, pályázati kiírásban előirányzott

cél érdekében, az együttműködéshez szükséges mértékben („need-to-know" alapon) használja fel, és megtesz minden, ezen titoktartási megállapodás előírásainak megfelelő intézkedést, az adatkezelés bizalmas jellegének biztosítására.

A Titoktartásra kötelezett kötelezettséget vállal a bizalmasan kezelendő információk biztonságos megőrzésére. Az együttműködés befejeztével az írásos információkat, ill. a titoktartási kötelezettség tárgyát képező információkat, dokumentumokat teljes egészében vissza kell szolgáltatni, ill. át kell adni a Jász-Plasztik Kft. részére, vagy a megegyezés alapján meg kell semmisíteni.

Megsértés következményei

1. A titoktartási kötelezettség megsértése súlyos szerződésszegésnek minősül; a Titoktartásra kötelezett teljeskörűen felel a Jász-Plasztik Kft.-nél ebből eredően keletkezett károk megtérítéséért. A Jász-Plasztik Kft. fenntartja továbbá a jogot, hogy ebben az esetben azonnali hatállyal felmondja a szerződést, ill. megszüntesse az együttműködést, illetve a pályázót a pályázati eljárásból kizárja.

2. A Titoktartásra kötelezett a munkavállalói, teljesítési segédei és alvállalkozói magatartásáért teljes felelősséggel tartozik.

3. A Jász-Plasztik Kft. kifejezetten felhívja a Titoktartásra kötelezett figyelmét, hogy a Jász-Plasztik Kft. a polgári jogi igényeinek érvényesítése mellett azonnali büntetőfeljelentéssel él abban az esetben, amennyiben a titoktartási kötelezettség be nem tartása büntetőjogi tényállást is megvalósít.

Alkalmazandó jogszabályok

Az üzleti titok és a know-how fogalmát, az üzleti titokhoz fűződő jog tartalmát, valamint az üzleti titokhoz fűződő jog megsértésének szankcióit az üzleti titok védelméről szóló **2018. évi LIV. törvény** határozza meg. Az ebben a törvényben nem szabályozott kérdésekre a Polgári Törvénykönyvről szóló 2013. évi V. törvény előírásait kell kisegítő jelleggel alkalmazni.

Külső partnerek kockázat azonosítása

A Cég az információs vagyon megvédése érdekében, amennyiben abban külső partnerek vesznek részt, azonosítja a külső partner által elérhető, hozzáférhető információkat, vagyon elemeket és ezek alapján megfelelő intézkedéssel és megállapodással rögzíti a szükséges védelmet és annak kezelését.

Külső partnerekkel kapcsolatos szerződéskötést megelőzően az Informatikai vezető kockázatelemzés alapján utasítja el, vagy dönt a megállapodás megkötéséről.

Kommunikáció a megrendelőkkel/partnerekkel

A megrendelők/partnerek jogosultak, a Céggel való együttműködéssel kapcsolatos témában, a számukra egyedi formában megadott teljes körű tájékoztatásra.

Külső kommunikáció

A külső kommunikációjának szervezése általában a Titkárság feladat- és hatáskörébe tartozik.

A Cég külső kommunikációs tevékenységeinek végzése során igazodik a „247/2014. (X. 1.) Korm. rendelet a Nemzeti Kommunikációs Hivatalról és a kormányzati kommunikációs beszerzések központosított közbeszerzési rendszeréről című jogszabályban leírtakhoz.

Kommunikáció az ellenőrző hatóságokkal

A Cég jelenleg hatályos Működési Szabályzatának megfelelően a Cégvezető végzi a hatósági ellenőrzések koordinációját.

Televíziós felvétel lebonyolítása, illetve fénykép készítése

A Cég területén csak a Cégvezető tudtával lehet bármilyen (kép-, hang-, stb.) felvételt, illetve fényképet készíteni. A forgatási engedélyt általánosságban a Titkárság adja ki.

Személyiségi jogok kezelése

A televíziós felvételek és egyéb képi anyag rögzítésekor a személyiségi jogokat betartani szükséges és erre a felvételt készítő személy(ek) figyelmét is fel kell hívni.

További követelmények a Jász-Plasztik Kft. hálózatához hozzáféréssel rendelkező külső felek részére

Meghatározás

A következő követelményeket kell betartania minden, az alábbi kategóriákba tartozó külső partnernek:

• Távoli hozzáféréssel (pl. Cisco AnyConnect) vagy más VPN-megoldásokkal csatlakoznak a Jász-Plasztik Kft. rendszeréhez.
• Közvetlenül a Jász-Plasztik Kft. vállalati gerincéhez (LAN) csatlakozik

Követelmények
Belső szervezet
A beszállítók csak a számukra felelős szervezeti egységen (a megrendelő üzleti osztályán) keresztül kérhetik vagy kezdeményezhetik a hardver és szoftver beszerzését és telepítését.

A mellékelt hardverek és szoftverek használatára az Jász-Plasztik Kft. IBSZ előírásai vonatkoznak.

Csak a Jász-Plasztik Kft. Informatikai Csoport tagjai nyithatják fel az informatikai eszközt, módosíthatják a hardvert (pl. Merevlemezek és memóriamodulok telepítése/eltávolítása), és manuálisan módosíthatják a biztonsági beállításokat (pl. Böngészőbeállítások).

A programok használata vagy későbbi módosítása csak a felelős egységek engedélyével megengedett.

A Jász-Plasztik Kft.-hez nem tartozó más ügyfelek adatait nem szabad feldolgozni a megadott informatikai eszközökön.

Az IT -eszközök és a megrendelő adatainak a szállító alkalmazottai általi használata a megrendelő kifejezett hozzájárulását igényli. A megrendelő fél bármikor jogosult megtiltani a hozzáférést/használatot (pl. Visszaélés esetén).

Fizikai és környezeti biztonság
A mellékelt eszközöket megfelelően kell kezelni, és védeni kell az elvesztéstől vagy az illetéktelen módosítástól. A készülék védelmére vonatkozó gyártó előírásait be kell tartani.

A megrendelő által biztosított eszközöket (például laptopokat, mobiltelefonokat) csak jóváhagyás után lehet a megrendelő területén kívül vinni.

Védelem a rosszindulatú és mobil kódok ellen
Azokat az informatikai eszközöket és adattároló eszközöket, amelyek gyanúja szerint rosszindulatú programokkal fertőzöttek, nem szabad tovább használni. A Jász-Plasztik Kft. Informatikai Csoportját haladéktalanul tájékoztatni kell.

Hozzáférés-szabályozás

Felhasználói kötelezettségek

A következő követelményeket minden felhasználónak be kell tartania:

• A Jász-Plasztik Kft. hálózatához történő hozzáférés a 3. fél hálózati hozzáféréskezelő űrlap kitöltésével és annak pozitív elbírálása után lehetséges.
• Más személy felhasználói azonosítójának vagy fiókjának használata nem megengedett.
• Az azonosító adathordozók (pl. Intelligens kártyák, SecurID kártyák) átadása másnak nem megengedett.
• A személyes használatra kijelölt felhasználói azonosító jelszavait vagy PIN-kódjait ("személyhez kapcsolódó felhasználói azonosító") nem szabad megosztani vagy nyilvánosságra hozni.
• Kerülni kell a nyilvántartás vezetését (pl. Papíron, mobil eszközökön vagy fájlokban), kivéve, ha ezeket biztonságos módszernek tekintik.
• A jelszavakat vagy a PIN -kódokat azonnal meg kell változtatni, ha bármilyen jel utal arra, hogy azok sérültek vagy ismertté váltak.
• Az ideiglenes jelszavakat (pl. Új fiókok esetén) meg kell változtatni az első bejelentkezéskor
• A jelszót vagy a PIN -kódokat először, majd legalább évente meg kell változtatni. A változási időköz nem vonatkozik a PIN -kódokra.
• A jelszavak kémkedése nem megengedett.
• A jelszavakat legalább bizalmasnak kell minősíteni.
• Ha a jelszavakat írásban kell tárolni, azokat a munkavállalónak lezárt borítékban kell tárolnia egy megfelelő helyen, amely védett az illetéktelen hozzáférés ellen és a jelszó megváltoztatásakor minden alkalommal frissíteni kell. A lezárt borítékot a megfelelő alkalmazottnak alá kell írnia. A boríték felbontására jogosult személyeket név szerint fel kell tüntetni. Kivételes esetekben (pl. Betegség esetén) szükség lehet a tárolt jelszó használatára. Ezt a "kétfős szabály" szerint kell megtenni. Minden nyitást dokumentálni kell, és jelenteni kell a munkavállalónak. Minden nyitás után a munkavállalónak haladéktalanul meg kell változtatnia a jelszót, és újra letétbe kell helyeznie.
• Amikor kilép a rendszerből a folyamatban lévő működés közben (pl. Szünet, értekezlet), a felhasználónak aktiválnia kell a rendszerzárat (pl. Jelszóval védett képernyővédőt).

Hálózat és hozzáférés szabályozás

A hálózati szolgáltatások használatára vonatkozó irányelv:

A megrendelő által biztosított informatikai eszközt csak a vállalaton kívüli hálózatokhoz (kivéve mobil kommunikációs hálózat) kell csatlakoztatni (pl. Hotspot, privát WLAN) a hálózattal való kapcsolat létrehozása érdekében. Közvetlen szörfözés stb. Nem engedélyezett (kivéve mobil kommunikációs hálózatokhoz csatlakoztatott okostelefonokat és táblagépeket).

Ha már nincs rá szükség, a kapcsolatot le kell bontani.

További követelmények azon külső felek részére, akik nem rendelkeznek közvetlen hozzáféréssel a Jász-Plasztik Kft. belső hálózatához.

Meghatározás

A követelményeket minden szállítónak be kell tartania, amely az alábbi kategóriák valamelyikébe tartozik:

• A szállító nem rendelkezik közvetlen hozzáféréssel a Jász-Plasztik Kft. hálózatához
• Nem kapcsolódik bármilyen VPN megoldás segítségével
• A szállító adatokat cserél a Jász-Plasztik Kft.-vel

Ezek a külső felek saját cégeik telephelyén találhatók, és kötelesek betartani saját társaságuk előírásait.

Követelmények

Belső szervezet

A Jász-Plasztik Kft. adatait el kell különíteni a harmadik felek adataitól (pl. A jogkezelés útján), és különösen a szállító más ügyfeleinek adataitól. Más harmadik felek nem férhetnek hozzá (pl. Titkosítással megvalósítható).

A Jász-Plasztik Kft. általi besorolást hozzá kell rendelni a szállító osztályozási rendszereihez annak biztosítása érdekében, hogy az összes szükséges biztonsági intézkedést teljesítsék.

A szállítónak a feladatai körében kapott előírások információbiztonsági követelményeit hozzá kell rendelnie a beszállítói saját vállalat megfelelő biztonsági intézkedéseihez.

Csak azoknak az alkalmazottaknak kell hozzáférniük a megrendelő félhez tartozó adatokhoz, akiknek erre szükségük van.

Felelősségek

Ezt a szabályozást minden szállítónak be kell tartania a jelen dokumentum hatálya szerint.

E szabálytól a biztonsági szintet csökkentő eltérések csak ideiglenesen, a felelős egységgel és a megrendelő féllel folytatott konzultációt követően megengedettek.

Érvényesség

Ez az információbiztonsági szabályozás a közzétételt követően azonnal érvényes.

Változási regiszter

Változtatott fejezet	Oldalszám	Változás dátuma	Változtatást végezte	Megjegyzés

Harmadik fél hálózati hozzáférési kérelem űrlapja

Ez az űrlap azoknak a szállítóknak vagy tanácsadóknak szól, akik szerződéssel vagy vásárlási megbízással rendelkeznek a Jász-Plasztik Kft.-vel és akiknek ideiglenes hálózati és/vagy hálózati rendszerekhez/alkalmazásokhoz való hozzáférésre van szükségük.

Vezetékné	Keresztné	Beosztása	Cég
Üzleti e-mail címe:	Mobil telefonszáma:	Vezetékes	
Szerződés kezdete:	Szerződés vége:	Jász-Plasztik Kft. részéről engedélyező/kapcsolattartó:	
◯ Hálózat & Email fiók ◯ Csak hálózati hozzáférés ◯ Hálózati drive megosztás (hálózaton belül) ◯ Távoli hozzáférés			
VPN / Távoli hozzáférés – Az elérendő szerverek listája (ip cím) és az elérni kívánt szolgáltatások listája (port)			
A hozzáférés kérelem indoklása:			

MINDEN SZÁLLÍTÓ ÉS TANÁCSADÓ, AKI IDEIGLENES HOZZÁFÉRÉST KAP A JÁSZ-PLASZTIK KFT. HÁLÓZATAIHOZ, RENDSZEREIHEZ ÉS/VAGY ADATAIHOZ, KÖTELES BETARTANI A JÁSZ-PLASZTIK KFT. CÉGES RENDSZEREK, NYILVÁNTARTÁSOK ÉS INFORMÁCIÓK BIZTONSÁGÁNAK ÉS TITKOSSÁGÁNAK FENNTARTÁSÁT. MINDEN ELADÓ/TANÁCSADÓ VÁLLALJA, HOGY BETARTJA AZ ALÁBBI SZABÁLYOKAT:

1. Tilos a Jász-Plasztik Kft. által tárolt adatok jogosulatlan felhasználása vagy elérése.

2. A kérelem alapján biztosított hozzáférés csak a Jász-Plasztik Kft. programjaival kapcsolatos munkákra vonatkozik.

3. A hozzáférés csak a fent említett időszakra szól, és automatikusan le lesz tiltva. A hozzáférés nem újul meg automatikusan. A hozzáférés csak egy évig biztosított. Évente meg kell újítani.

4. A szállítóknak/tanácsadóknak gondoskodniuk kell a fiók- és jelszóbiztonságról - tilos a fiókadatok és jelszavak bárki számára történő közzététele.

5. Az eladók/tanácsadók nem használhatják más személy bejelentkezési azonosítóját és jelszavát a Jász-Plasztik Kft. bármelyik elektronikus rendszerének eléréséhez.

6. A szállítók/tanácsadók távoli munkaállomásainak modern vírus- és kártevő -ellenőrző segédprogramokat kell használniuk.

7. A szállítóknak/tanácsadóknak szigorúan bizalmasan kell bizalmas információkat tárolniuk, és csak a Jász-Plasztik Kft.-vel kötött szerződésében meghatározott üzleti célokból férhetnek hozzá az információkhoz.

8. A szállítók/tanácsadók nyilvánosságra nem hozhatják, másolhatják (elektronikus vagy más módon), nem adhatják ki, nem adhatják el, nem kölcsönözhetik, nem tekinthetik át, nem módosíthatják vagy semmisíthetik meg az adatokat, kivéve, ha azt a Jász-Plasztik Kft. megfelelő tisztségviselője írásban megfelelően engedélyezte.

10. A szállítóknak/tanácsadóknak jelenteniük kell a Jász-Plasztik Kft. IT Osztályának a megállapodás minden olyan megsértését, amelyről ő tud, gyanítja, vagy okkal feltételezi, hogy történt, függetlenül attól, hogy a jogsértést az említett eladó/tanácsadó okozta -e. vagy más eladó/tanácsadó vagy más személy/szervezet.

Elolvastam és megértettem a fent felsorolt szabályokat, és vállalom, hogy betartom azokat. Fenntartom a rám bízott Jász-Plasztik Kft. nyilvántartások és információk biztonságát és titkosságát a fenti szabályok és az itt hivatkozott irányelvek szerint. Ha okkal feltételezhető, hogy megsértésre kerültek a Jász-Plasztik Kft. Információbiztonsági szabályai, tudomásul veszem, hogy hozzáférésemet, fiókjaimat és a fiókom tartalmát felügyelet és vizsgálat alá vonhatja az arra jogosult személyzet és azokat azonnal visszavonják. Tudomásul veszem, hogy a be nem tartás az alkalmazandó szerződés felmondását, valamint a szerződésben és a jogszabályokban elérhető egyéb szankciókat vonhatja maga után.

Vevő/Tanácsadó Aláírása: ……. Dátum: ……

Harmadik fél biztonsági kockázatértékelési kérdőíve

Cég Neve:

Cég webcíme:

Kapcsolattartó személy, aki elvégzi az értékelést :

Email Cím:

Telefonszám:

Válassza ki a megfelelő választ a Válasz oszlop legördülő menüjéből, és adjon meg egy rövid leírást a Megjegyzések részben.

	Információbiztonsági értékelési kérdések	Válasz	Megjegyzések	JP Megjegyzések/Kérdések	Harmadik fél válasza a JP megjegyzéseire/kérdéseire
	Szervezeti információbiztonság				
1	Ha a cége bizonyítani tudja a biztonságra vonatkozó auditokat (például ISO27001 vagy TISAX), és Ön bizonyítékot is szolgáltat róluk, akkor nem kell kitöltenie ezt a kérdőívet. Kérjük, igazolja a tanúsítást.				
2	Van e a szervezeténél olyan személy aki az információbiztonsági feladatokkal foglalkozik?				
3	Végeznek e háttérellenőrzést azon alkalmazottaik részére, akik hozzáférhetnek az adatainkhoz és kezelik azokat?				
4	Van e a szervezetének írásos információbiztonsági szabályzata?				
4,1	Ha a 4.0 igen, kérjük, adjon részünkre egy másolatot, ha megengedett, ha nem, kérjük, adja meg a címlapot és a tartalomjegyzéket, amikor válaszol erre az értékelésre.				
5	Rendelkezik e a szervezete írásos jelszó házirenddel, amely részletezi a jelszavak szükséges szerkezetét?				
5,1	Hogyan ellenőrizi a jelszavak erősségét?				
6	Minden személy részt vesz e információbiztonsági képzésen?				
	Általános biztonság				
7	Van e telepítve antivírus szoftver a szervezete szerverein?				
8	Van e telepítve antivírus szoftver a szervezete munkaállomásain?				
9	A rendszer- és biztonsági javításokat rutinszerűen alkalmazzák e a munkaállomásokra?				
10	A rendszer- és biztonsági javításokat rutinszerűen alkalmazzák e a szerverekre?				
11	A rendszer- és biztonsági javításokat tesztelik e az éles környezetben való bevezetés előtt?				
12	Rendelkeznek e az alkalmazottak egyedi bejelentkezési azonosítóval az adatok eléréséhez?				
13	Rendelkezik -e a szervezete biztonsági intézkedésekkel az adatvédelem érdekében?				
13,1	Ha igen, kérjük, írja le a megjegyzések rovatban				
14	Korlátozzák e a hozzáférést érzékeny adatokat tartalmazó rendszerekhez?				
14,1	Ha igen, milyen szabályozások vannak jelenleg a hozzáférés korlátozására?				
15	Korlátozott e az adatfeldolgozó berendezéseikhez (szerverekhez és hálózati eszközökhöz) való fizikai hozzáférés?				
15,1	Ha igen, milyen ellenőrzések vannak jelenleg érvényben?				
16	Létezik -e folyamat az informatikai eszközök és adathordozók biztonságos ártalmatlanítására?				
16,1	Ha igen, kérjük, írja le a megjegyzések rovatban				

17	A hálózat határait védi e tűzfal?				
18	Rendszeresen végeznek e hálózati sebezhetőségi vizsgálatot?				
19	Behatolásjelző rendszereket (IDS) vagy a behatolásmegelőző rendszereket (IPS) használ e a szervezete?				
19,1	Ha igen, kérjük, írja le a megjegyzések rovatban				
20	Kötelesek e az alkalmazottak VPN-t használni, amikor a szervezet rendszereit távoli helyről szeretnék elérni?				
21	Engedélyezett a vezeték nélküli hozzáférés a szervezetén belül?				
21,1	Ha igen, kérjük, írja le a megjegyzés rovatban, hogyan védett?				
	Rendszerbiztonság				
22	A számítógépes rendszerek (kiszolgálók) biztonsági mentése rendszeres ütemterv szerint történik?				
23	Ellenőrzik a biztonsági mentési és helyreállítási folyamatokat?				
24	A szervezete tárol biztonsági mentéseket a szervet telephelyin kívül?				
25	Titkosítja a szervezete a biztonsági mentéseit?				
26	A szervezeténél van kiszervezett adattárolás?				
26,1	Ha igen, kinek adják ki az adatokat?				
27	Szabályozva van a rendszergazdai jogosultságokhoz való hozzáférés?				
28	A kiszolgálók úgy vannak konfigurálva, hogy rögzítsék, ki férhet hozzá a rendszerhez, és milyen változtatásokat hajtottak végre?				
28,1	Ha nem, akkor biztonsági rés esetén hogyan határozza meg, hogy ki fért hozzá a rendszerhez, és milyen változtatásokat hajtott végre?				
29	Az érzékeny adatok megfelelően védettek és az adatkommunikáció titkosítva van? Például támogatja a szoftver az SSL titkosítást?				
	Üzletfolytonosság / katasztrófa utáni helyreállítás				
30	Van -e a szervezetének katasztrófa utáni helyreállítási terve az adatfeldolgozó létesítményekkel kapcsolatban?				
30,1	Van -e a szervezetének üzleti folytonossági terve?				
31	A számítógéptermek védettek e tűz és árvíz ellen?				
32	Van e a szervezetének "forró" helyreállítási helyszine?				
	Az incidensre adott válasz				
33	Ha a GDPR adatait érintő információbiztonsági jogsértés történt, értesítik a NAIH -t a jogsértésről?				
33,1	Ha igen, mennyi idő múlva értesítik a NAIH -t?				
34	Rendelkezik -e a szervezete hivatalos incidens-elhárítási tervvel?				
35	Tapasztalt -e a szervezete információ biztonsági megsértést az elmúlt három -öt évben?				
35,1	Ha igen, kérjük, dokumentálja, milyen információk vesztek el a megjegyzések rovatban?				
35,2	Ha igen, kérjük, dokumentálja a megjegyzések rovatban, hogyan és milyen gyorsan értesítették az ügyfeleket.				
	Külső tárhelyszolgáltatás / harmadik fél				
36	Fogja e adatainkat tárhelyszolgáltatónál tárolni?				
36,1	Ha igen, kérjük, adja meg a tárhelyszolgáltatás nevét, és hogy ISO27001 tanúsítvánnyal rendelkeznek e?				
37	Kérjük, sorolja fel azokat a harmadik feleket, amelyeket az Ön vállalkozása használ az adataink és tanúsítványaik tárolására.				
38	Rendszeresen felülvizsgálja a harmadik feleket, akik hozzáférnek az adatainkhoz? Milyen gyakran?				