Adatbiztonság

I_Site

A Toyota Material Handling tisztában van vele, hogy az I_Site rendszer megvásárlásával az ügyfelek bizonyos adatokat adnak át a cégnek, és ezeket az adatokat biztonságosan kell kezelni.
A dokumentum ismerteti a Toyota Material Handling általános biztonsági jellemzőit, valamint I_Site flottakezelő rendszerünk biztonsági és egyéb jellemzőit.

TOYOTA
MATERIAL HANDLING

BEVEZETÉS ÉS ISMERTETŐ

Az I_Site rendszerrel fokozható a termelékenység, a biztonság, a környezetvédelem, valamint csökkenthetők a működési költségek. Az I_Site segítségével a flottában lévő gépek csatlakoztathatók a Toyota Material Handling háttérirodai rendszereihez, amit a gépekbe épített telematikai egységek tesznek lehetővé.

A gépadatok birtokában nyomon követhetők és javíthatók a logisztikai műveletek, például a biztonság, az energiafogyasztás és a szerviz. A gépadatok a webes portálon és a mobilalkalmazáson keresztül érhetők el, az olyan információk, mint a gépek kihasználtsági szintje, az akkumulátor töltöttségi állapota és számos egyéb tényező pedig megjelenik a webes portálon és a mobilalkalmazásban, hogy teljes áttekintést nyújthasson a targoncaflotta műveleteiről.

A Toyota Material Handling vállalatnál tisztában vagyunk vele, hogy ügyfelünk az I_Site kiválasztásával megbízott bennünket az Ön vállalatával (gépadatokkal) kapcsolatos információkkal, és hogy ezeket az információkat védeni kell a kiberfenyegetésektől, illetve egyéb jogosulatlan felhasználástól vagy hozzáféréstől. Elismerjük, hogy a magánélet védelmére és az adatvédelemre vonatkozó törvények és rendeletek bizonyos követelményeket támasztanak azzal kapcsolatban, hogy az Ön által ránk bízott adatokat hogyan kell biztonságban tartani.

Az egyre inkább összekapcsolt és összetett világban a biztonság ma még fontosabb, mint valaha, a minőség kulcsfontosságú eleme. A Toyota Material Handling vállalatnál arra törekszünk, hogy minden tevékenységünk minőségét biztosítsuk, ezért annak érdekében, hogy megkönnyítsük a biztonság terén való vállalásaik megértését, elkészítettük ezt, az I_Site rendszer biztonságával foglalkozó dokumentumot.

A kétségek elkerülése érdekében hangsúlyoznunk kell, hogy ez a dokumentum olyan tájékoztató dokumentum, amely általánosságban a Toyota Material Handling vállalat biztonsági funkcióit és különösen az I_Site biztonsági vonatkozásait próbálja ismertetni, és nem értelmezhető jogi tanácsként vagy egyéb üzleti tanácsként.

Az I_Site rendszert „Software-as-a-Service" vagy „SaaS" formában kínáljuk megvételre. Ezért nincs szükség az ügyfél-infrastruktúrával való interakcióra vagy integrációra. Emellett ez az elrendezés azt jelenti, hogy nem tudunk részletes információkat biztosítani az infrastruktúráról, például az I_Site-ról származó naplókat sem tudunk biztosítani. Továbbá nem engedélyezzük az I_Site biztosítására használt végpontok biztonsági réseinek ellenőrzését vagy hasonló tevékenységeket.

[1] Az ebben a dokumentumban használt nagybetűs kifejezések az I_Site Általános Szerződési Feltételeiben megadott jelentéssel bírnak.

ADATBIZTONSÁGÉRT FELELŐS RENDSZERÜNK („ISMS")

ÁLTALÁNOS

Az ISMS-ünk összhangban van az ISO 27001 szabványokkal, és az alábbi a)-f) pontban ismertetett biztonsági intézkedések köré alakítottuk ki. Amennyiben az ISO 27001 szabvánnyal való részletes megfeleltetésre kíváncsi, tekintse meg az 1. függeléket. A biztonsági intézkedéseket kockázatértékelések, végrehajtás és felülvizsgálat révén kezelik és folyamatosan javítják.

- A jogosulatlan felhasználók nem férhetnek hozzá a személyes adatokhoz a hozzáférés-vezérlés révén.
- A hozzáférés-ellenőrzés révén, és egy vállalkozás számára szükséges ismeret alapján biztosítjuk, hogy az adatok felhasználására jogosult személyek csak a releváns adatokhoz férjenek hozzá, és az adatok nem olvashatók, másolhatók, módosíthatók, illetve nem távolíthatók el engedély nélkül a feldolgozás során.
- Az átvitelvezérlés révén biztosítjuk, hogy az adatok elektronikus továbbítás vagy szállítás közben engedély nélkül nem olvashatók, másolhatók, módosíthatók vagy távolíthatók el.
- A bemeneti ellenőrzés, a hozzáférés-vezérlés, a biztonságos fejlesztési gyakorlatok, a rosszindulatú programok elleni funkciók, a naplók áttekintése és a sebezhetőségi tesztek segítségével fel tudjuk mérni és meg tudjuk állapítani, hogy a személyes adatok bevitelre kerültek-e az adatfeldolgozó rendszerekbe, módosították-e vagy eltávolították azokat, és ha igen, ki.
- A szolgáltatásokra és infrastruktúrára vonatkozó adminisztratív és IT-biztonsági (rendelkezésre állási) ellenőrzések kombinációjával biztosítjuk, hogy az adatok védve legyenek a véletlen megsemmisítéstől és elveszéstől.
- A biztonságos fejlesztéssel, logikai és fizikai elkülönítéssel szavatoljuk, hogy az eltérő célokra gyűjtött adatok feldolgozása elkülönítve történjen.

Ahol kell, titkosítást vagy pszeudonim eljárásokat, törlés és adatminimalizáló műveleteket alkalmazunk.

SZERVEZETI BIZTONSÁG INTÉZKEDÉSEK

ÁLTALÁNOS

A szervezet stratégiai és operatív irányítási fórumaiban való részvétel révén egy kijelölt információbiztonsági és IT-kockázatkezelő felügyeli az ISMS kezelését, az információbiztonsági irányítást és az IT-biztonságot.

Az adatvédelmi törvényeknek és rendeleteknek való megfelelést a célzott információbiztonsági és az adatvédelmi munkacsoportot alkotó jogtanácsosi kollégák felügyelik.

A mobileszközök használatát és a távoli hozzáférést az elfogadható használatra vonatkozó szabályok szabályozzák.

EMBERI ERŐFORRÁSOK

Foglalkoztatás előtt: Dolgozóink és tanácsadóink betanítási folyamatának része a Toyota Material Handling ISMS és a titoktartási megállapodások szerepalapú ismertetése.

Foglalkoztatás közben: Minden foglalkoztatási és tanácsadói szerződésre a vállalat magatartási kódexének (amely általános ellátási kötelezettségről rendelkezik a vállalati adatok és információs eszközök kezelése során, valamint az adatokhoz való hozzáférés általános üzleti-know-alap elvéről) és az információbiztonsági irányelveknek való megfelelés vonatkozik. A vállalat adataihoz hozzáféréssel rendelkező minden alkalmazottnak és tanácsadónak részt kell vennie az információbiztonsággal és a kapcsolódó témákkal kapcsolatos rendszeres figyelemfelkeltő és oktató képzéseken. Létezik egy formális és közölt fegyelmi eljárás, amely a szabályzataink be nem tartásának eseteivel foglalkozik.

Elbocsátás vagy a foglalkoztatás megváltozása: Elbocsátás vagy a foglalkoztatás megváltozása esetén a dolgozók és a tanácsadók eligazításban részesülnek, hozzáférési jogaikat visszavonják, a náluk lévő eszközöket pedig le kell adniuk.

MŰSZAKI BIZTONSÁGI INTÉZKEDÉSEK ÉS ESZKÖZKEZELÉS

Bizalmasságánál fogva valamennyi adatot négy kategóriába osztunk fel, vagyis vannak nyilvános, belső, bizalmas és szigorúan bizalmas adatok, amelyeket ennek megfelelő elnevezéssel látunk el.

Minden információs eszközt, mint például az alkalmazások, szolgáltatások, kiszolgálók, számítógépek, mobileszközöket és hálózati eszközök regisztrálnak, és olyan kijelölt tulajdonossal rendelkeznek, aki egy eszköz teljes életciklusa során tisztában van az információs eszközhöz kapcsolódó felelősségekkel és elfogadható használattal.

A mobileszközök használatát és a távoli hozzáférést a hozzáférés-vezérlés (például többtényezős hitelesítés), a titkosítás és a hozzáférési szabályok korlátozása szabályozza. A cserélhető adathordozók engedélyezett használata az információk osztályozásán alapul, míg a cserélhető adathordozók biztonságos leselejtezése a FIPS 800-88 szabvány szerint történik.

Az információkhoz való hozzáférés szerepköralapú, és csak szigorú üzleti szükségességgel biztosított. A felhasználói hozzáférés minden biztosítását egy ITIL kéréskezelési folyamat kezeli, beleértve az erőforrás-kezelő vagy az információeszköz-kezelő általi hozzáférés jóváhagyását.

A biztonságos bejelentkezési eljárások biztosítása érdekében minden belső infrastruktúrában az Active Directory felé a hitelesítés, hitelesítés és számlázás (AAA) funkciót használjuk. A titkos hitelesítési információkat biztonságos módon tároljuk, és biztonságos módon tájékoztatjuk róluk a munkatársakat. A hozzáférési értékeléseket legalább évente elvégzik.

FIZIKAI, KÖRNYEZETI ÉS MŰVELETI BIZTONSÁG

A jogosulatlan hozzáférés, az információ- vagy információfeldolgozó létesítményeink sérülése vagy zavarai elkerülése érdekében olyan adatközpontokat használunk, amelyek:

- ISO 9001:2015 tanúsítással rendelkeznek,
- ISO 14001:2004 tanúsítással rendelkeznek, és
- ISO 27001:2013 tanúsítással rendelkeznek.

Emellett az alábbi kritériumok alapján állapítjuk meg az adatközpont kapacitását:

- A létesítményeket úgy tervezték és helyezték el, hogy védelmet nyújtsanak a természeti katasztrófák, balesetek és rosszindulatú támadások ellen.
- A létesítmények célja, hogy megvédjék az információfeldolgozást, az átviteli vonalakat, a szállítási és rakodási területeket a véletlen károsodástól, a fennakadásoktól és a fizikai beavatkozástól.
- Az információfeldolgozó berendezéseket és az átviteli vonalakat olyan intézkedések védik az áramkimaradástól, mint a redundáns tápellátási segédeszköz használata, a dedikált, folyamatosan működő szünetmentes tápegység, valamint a (rendszeresen karbantartott és tesztelt) generátorok által biztosított vészhelyzeti áramtámogatás, beleértve a vészhelyzeti üzemanyag-ellátást is.
- Tűzérzékelési és -elnyomó képesség, beleértve a folyamatos megfigyelést és tesztelést.
- A hőmérséklet és a páratartalom HVAC-szabályozása, beleértve a folyamatos megfigyelést és tesztelést.
- A biztonsági határ érvényesítése, a meghatározott és felügyelt belépési pontokra (beleértve a szomszédos irodahelyiségeket és egyéb létesítményeket) korlátozott fizikai hozzáférés, valamint a kéttényezős hitelesítéssel megoldott tartozó fizikai hozzáférés.
- Fizikai és logikai elkülönítés a közös elhelyezésű ügyfelek között.
- Az év minden napján folyamatos felügyelet, SOC által.
- A hozzáféréssel rendelkező entitások legalább negyedéves felülvizsgálata.
- A fizikai és környezetvédelmi, valamint a kapcsolódó fizikai és környezetvédelmi ellenőrzések végrehajtásának megkönnyítése érdekében meghatározott, dokumentált és elosztott eljárások, beleértve a rendszeres képzést az érintett személyzet számára.
- A Toyota Material Handling eszközei, adathordozói vagy információi nem kerülnek az adatközponton kívülre a Toyota Material Handling előzetes engedélye nélkül. Az áthaladó eszközök bizalmas adatait és integritását titkosítással és hasonló megoldásokkal biztosítjuk
- A NIST SP 800-88 szerint megtisztított, biztonságos hulladékkezelés helyszíni vagy mobil megsemmisítési szolgáltatásokkal.

Üzemeltetési eljárások és felelősségek: Az információfeldolgozó létesítményeink biztonságos működésének biztosítása érdekében a szervizdokumentációért egy erre a célra kijelölt szerviztulajdonos felel. Számos információbiztonsági ellenőrzőpont van számos olyan változtatási folyamatban, amelyen minden szervezeti változásnak vagy üzleti folyamatváltozásnak át kell haladnia. A működési változások ITIL-alapú változáskezelési folyamaton haladnak át. Szolgáltatásaink nyomon követése és megfigyelése a jövőbeli kapacitásigények figyelembe vételével történik. A fejlesztési, tesztelési és működési környezet elkülönül a jogosulatlan hozzáférés és az üzemeltetési környezet megváltoztatása kockázatainak csökkentése érdekében.

Rosszindulatú programok elleni védelem: Annak érdekében, hogy megvédjük magunkat és ügyfeleinket a rosszindulatú programok fenyegetésével szemben, szolgáltatásainkra számos rosszindulatú program elleni követelmény vonatkozik, amelyeket adminisztratív és technikai ellenőrzések ellenőriznek és érvényesítenek. Rosszindulatú programok elleni funkciókat, a rosszindulatú programok eseményeinek naplózását és felügyeletét, valamint ITIL-alapú incidenskezelési folyamatot használunk.

Biztonsági mentés: Az adatvesztés elkerülése érdekében szolgáltatásonként dokumentáljuk és érvényesítjük a követelményeket. A biztonsági mentés állapotának rendszeres áttekintése a szolgáltatás jóváhagyott helyreállítási szabályzatának megfelelően történik.

Naplók és felügyelet: Informatikai környezetünket a hét minden napján, napi 24 órában felügyeljük. A naplók tárolása UTC időbélyegzővel, legalább 3 hónapos központi óraszinkronizálási szolgáltatással történik, és védve vannak az illetéktelen beavatkozás és jogosulatlan hozzáférés ellen. Az eseménynaplók rögzítik a felhasználó hozzáférését, a kivételeket, a hibákat, és szükség esetén a egyéb felhasználói tevékenységeket is. Az események kategorizálása előre meghatározott súlyossági szintek szerint történik, és kezelésük az ITIL-alapú incidenskezelési folyamaton keresztül zajlik.

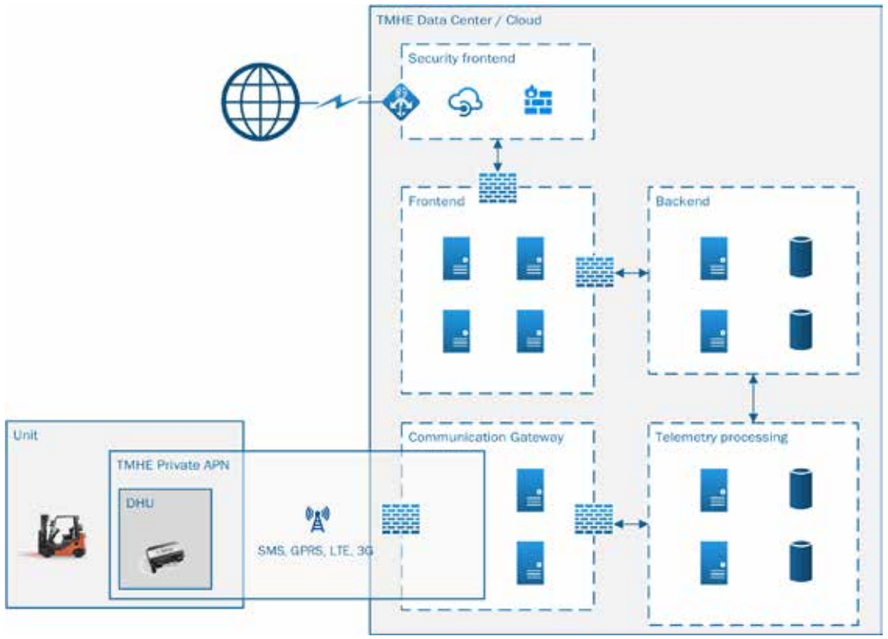
Operációs rendszerek kezelése: A szolgáltatások, alkalmazások és operációs rendszerek folyamatosan frissülnek a legújabb biztonsági javításokkal és kiadásokkal. A technikai biztonsági réseket egy kockázatkezelési folyamat követi nyomon. A szoftver telepítése csak a privilegizált hozzáféréssel rendelkező felhasználók számára engedélyezett. Külső és belső infrastruktúránkat rendszeresen átvizsgáljuk a műszaki biztonsági rések szempontjából.

Az információs rendszerek ellenőrzésének szempontjai: Az ellenőrzési tevékenységek operációs rendszerekre gyakorolt hatásának minimalizálása érdekében az infrastruktúra rendszeres felülvizsgálatát a rendelkezésre állás, a kapacitás és a biztonsági kockázatok alapján végzik. A rendszeres felülvizsgálatokat az IT szolgáltatásmenedzsment tartalmazza, és úgy tervezték őket, hogy ne befolyásolják az üzleti folyamatokat.

KOMMUNIKÁCIÓ BIZTONSÁG

Hálózati biztonság kezelése: Információeszközeink, többek között az Ön, ügyfeleink, a vállalat hálózatai és támogató információfeldolgozó létesítményei titkosságának, integritásának és rendelkezésre állásának védelme érdekében a Toyota Material Handling hálózatai alapos biztonsági, hálózati szegregációs és mért műszaki hálózati biztonsági képességekkel rendelkeznek.

Az alábbi képen az I_Site biztonságkezelésének elvi áttekintése látható.



Az információátadásra kereskedelmi szerződések, titoktartási megállapodások és adott esetben adatfeldolgozási megállapodások vonatkoznak. Az ilyen megállapodások életciklus-alapú nyomon követés és felülvizsgálat tárgyát képezik.

FORRÁSTERVEZÉS

Annak biztosítása érdekében, hogy az információbiztonság az információs rendszerek szerves részét képezze teljes életciklusuk során, a következő ellenőrzéseket és követelményeket kell alkalmazni.

Általános biztonsági követelmények: A nyilvános hálózatokon keresztül továbbított információkat biztosítani kell. A szolgáltatások interfészeire vonatkozó szabványoknak megfelelő védelemmel kell rendelkezniük a nem teljes átvitel, a hibás útvonaltervezés, a jogosulatlan üzenetmódosítás, a jogosulatlan felfedés, a jogosulatlan üzenetmásolás vagy visszajátszás kezeléséhez.

A nyilvános interfésszel rendelkező valamennyi szolgáltatás esetében a jóváhagyási folyamat során a biztonsági rések műszaki ellenőrzését ellenőrző elemként kell figyelembe venni, és az életciklus többi részében a rendszeres általános műszaki sebezhetőségi vizsgálatok részét képezik.

A fejlesztési és támogatási folyamatok biztonsága: A biztonsággal, rendelkezésre állással, rugalmassággal és katasztrófákra való felkészültséggel kapcsolatos tervezési, fejlesztési és támogatási követelményeket projektvezetési, elfogadási tesztelési, változáskezelési, architektúrára és architektúrára felülvizsgálati folyamataink tartalmazzák. A vonatkozó követelmények olyan területekre terjednek ki, mint például a veszteséggel, megsemmisítéssel, hamisítással, jogosulatlan hozzáféréssel és jogosulatlan kiadással szemben védett információk. Figyelembe veszik a szabályozási követelményeket, mint például a beépített adatvédelem, az érintett jogai, valamint a titkosítás vagy az anonimizálás alkalmazása. A tesztadatok és a gyártási adatok között szigorú elkülönítést biztosítunk.

Szállítói szolgáltatás kezelése: A szolgáltatásainkat kezelő minden partner köteles betartani a Toyota Material Handling irányelveit, és a partnerrel kötött kereskedelmi megállapodás életciklusának részeként figyelemmel kísérjük őket. Az információbiztonság és a szolgáltatásnyújtás megállapodás szerinti szintjének fenntartása a beszállítói megállapodásokkal összhangban a partnerek által nyújtott szolgáltatások módosítása az életciklus-felülvizsgálat, a változások ellenőrzése és a kockázatkezelés függvénye.
Az utasításoknak megfelelő tárolás és használat közben az adatok nem sérülnek.
Tűz és nyitott cellák esetén fennáll a hidrogén-fluorsav és a szén-monoxid kibocsátásának lehetősége.

ÜZLETMENET-FOLYTONOSSÁG, MEGFELELŐSÉG ÉS ESEMÉNYKEZELÉS

Az információbiztonsági események kezelése: A biztonsági események kezelésének következetes és hatékony megközelítése érdekében, beleértve a biztonsági eseményekről és hiányosságokról szóló kommunikációt, a következő követelmények alkalmazandók. Minden eseményt, beleértve a személyes adatok Toyota Material Handlingnál való megsértését is, az ITIL alapú eseménykezelési folyamatok szerint kezelnek, ahol az eszközök az esemény eredetétől függenek. Az eseménykezelési folyamatok közé tartozik a rangsorolás, a kategorizálás, a mérés, a jelentés, az eszkaláció, az értesítés és kezelés. Az eseménykezelés folyamatos fejlesztése minden folyamat integrált részét képezi.

Minden alkalmazott és tanácsadó köteles jelenteni az ügyfélszolgálatnak minden kockázatot, hiányosságot vagy biztonsági eseményt. A személyes adatok megsértésének kezelésére vonatkozó folyamat magában foglalja az adatvédelmi munkacsoport felé való eszkalációt.

Az információbiztonság folytonossága: Az adatbiztonság folyamatosságát általános üzleti folyamatirányítási rendszerünkben szavatolja. A követelmények között szerepel, hogy a szolgáltatásokat hogyan tervezik a kedvezőtlen helyzetek kezelésére válság vagy katasztrófa esetén. Eljárásokat és ellenőrzéseket dolgoztunk ki, hogy biztosítsák az információbiztonság szükséges szintű folyamatosságát kedvezőtlen körülmények között, beleértve a redundanciával kapcsolatos képességeket, valamint ezen folyamatok rendszeres felülvizsgálatát és tesztelését.

I_Site biztonsági keretrendszerünk fontos része annak, hogy hogyan biztosítjuk az Általános Adatvédelmi Rendelet 32. cikkének megfelelő műszaki és szervezeti biztonsági intézkedéseket.

A Toyota Material Handling termékei és szolgáltatásai biztonságának folyamatos javítása, valamint a törvényi, rendeleti és szerződéses kötelezettségek teljesítésének biztosítása érdekében az ISMS-ünk rendszeres (legalább éves és szükség esetén gyakoribb) felülvizsgálat tárgyát képezi. A szükséges változtatások azonosítása érdekében folyamatosan figyelemmel kísérjük a rendelkezésre álló technológia, jogszabályi és szabályozási követelmények, valamint az ügyfelek igényeinek korszerű fejlesztését. A kijelölt szervizfelelősök feladata annak biztosítása, hogy a kvalitatív biztonságot szabályzataink és eljárásaink szerint vezessük be.

Toyota Material Handling Európában

Teljes lefedettség
A Toyota Material Handling hálózata Európa több mint 30 országára kiterjed, és 5000-nél is több mobil szervizszakembert foglalkoztat.

Mindig helyben – globális támogatással
Bárhol is legyen Európában, mi széles körű lefedettségünknek köszönhetően mindig helyben elérhetők vagyunk, ám egy nemzetközi szervezet stabilitásával és támogatásával a hátunk mögött.

Európai gyártmány
Az általunk értékesített targoncák több mint 95%-a saját európai gyárainkban (Svédországban, Franciaországban és Olaszországban) készül, valamennyi a TPS minőségi szabványainak megfelelően. Több mint 3000 fős gyártási csapatot alkalmazunk Európában, és 300-nál is több európai beszállítóval dolgozunk.

Európai termelésünk mintegy 15%-át exportáljuk a világ más részeibe.