Információbiztonsági Szabályzat

Változatok jegyzéke

Verzió	Kiadás dátuma	Kiadás indoka	Készítette	Jóváhagyó
1.0	2023. 06. 01.	ISO 27001 megfelelés	Gill & Murry Kft,	Dr. Matula Evelin

Tartalomjegyzék

1. Bevezetés

1.1 A szabályzat célja

Az Információbiztonsági Szabályzat (a továbbiakban: Szabályzat, vagy IBSZ) célja a Büttner Kft. (továbbiakban Büttner Kft. vagy Szervezet) információbiztonsági követelményeinek és környezetének meghatározása, ami leírja az elvárt védelmi intézkedések és azok dokumentálásának és felügyeletének feladatait. A szabályzat a Büttner Kft. által tárolt, feldolgozott és továbbított adatok kezelésének, valamint az informatikai rendszerek működésének, üzemeltetésének és információbiztonságának általános elveit és részletes szabályozását tartalmazza, továbbá a szükséges szerepköröket, felelősségeket határozza meg. Az IBSZ rögzíti a tevékenységek elvégzésének folyamatát, módját, gyakoriságát, előírva a felelősségeket és a dokumentálási kötelezettségeket.
A Szervezet a kezelt adatok és információk védelme érdekében MSZ ISO 27001:2014 követelményszabvány szerinti Információbiztonsági Irányítási Rendszert (továbbiakban: IBIR) tervezett meg, vezetett be, működtet és rendszeresen felülvizsgál a rendszer folyamatos fejlesztése érdekében.

Az Információ Biztonsági Szabályzat és a kapcsolódó dokumentáció elérhető a Büttner Kft. központi szerverén: IBIR mappa

1.2 A szabályzat személyi hatálya

Az IBSZ-ben meghatározott információbiztonsági és IT üzemeltetési szabályok személyi hatálya kiterjed a Büttner Kft. munkavállalóira, IT rendszereihez hozzáféréssel rendelkező valamennyi felhasználójára és üzemeltetőjére (a továbbiakban: Felhasználó), tekintet nélkül arra, hogy az adott személy vagy szervezet munkaviszonyban, megbízási szerződéses vagy egyéb jogviszonyban áll a Büttner Kft.-vel.

1.3 A szabályzat tárgyi hatálya

Az IBSZ tárgyi hatálya szerszámlapok megmunkálása és CAD – Cam tervezése a szervezet informatikai rendszerében, a tárgyi hatály kiterjed minden olyan hardverre és szoftverre, alkalmazásra, adatbázisra, adathordozóra (annak típusától függetlenül), valamint egyéb informatikai és infokommunikációs eszközállományra (a továbbiakban: vagyontárgy), amely a Büttner Kft. adatvagyonát kezeli, feldolgozza vagy tárolja. Továbbá a Büttner Kft.-val szerződéses kapcsolatban lévő ügyfelek a Büttner Kft. részére adatkezelésre, feldolgozásra, gyártás előkészítésre átadott az ügyfelek tulajdonát képező adatokra, a felek között fennálló szerződésben rögzített mértékben.
Az IBSZ hatálya kiterjed a nem digitális adatkezelésre (pl. papír alapú, szóbeli közlés) is.

1.4 A szabályzat területi hatálya

A Büttner Kft. mindenkori székhelye és telephelyei:

- 7500 Nagyatád, Taranyi úti Ipartelep 2744 hrsz.,
- 7636 Pécs, Időjós út 7/F

1.5 Az IBSZ felülvizsgálata

Az információbiztonsági tevékenységek megfelelő hatékonyságának biztosítása érdekében az Információbiztonsági felelős irányításával a Büttner Kft. minden évben az információbiztonsági átvizsgálás keretében tekinti át és értékeli az Információbiztonsági Irányítási Rendszer működését és annak hatékonyságát.
Az információbiztonsági átvizsgálás alkalmával az IBSZ és mellékletei is felülvizsgálatra, aktualizálásra kerülnek, az Információbiztonsági felelős gondoskodik róla, hogy a szükséges változtatások átvezetésre kerüljenek.
Az IBSZ-t az éves átvizsgáláson kívül is felül kell vizsgálnia az Információbiztonsági felelősnek, ha:

- új, az információbiztonságot érintő törvények vagy szabályozók lépnek hatályba,
- jelentős szervezeti változások esetén,
- olyan új információbiztonsági fenyegetések merülnek fel, melyeket korábban nem kezeltek,
- az IT rendszerek fejlesztésére, jelentős módosítására kerül sor.

2. Az Információbiztonsági Politika

A Büttner Kft. az IBIR bevezetésével egy időben kiadta az információbiztonságra vonatkozó politikáját. Az Információbiztonsági politikát az Ügyvezető fogadta el és adta ki. Az információbiztonsági politikát a közzétételt követően jelen szabályzat személyi hatálya alá tartozók számára folyamatosan elérhetővé kell tenni.

Az Információbiztonsági Politika elérhető a Büttner Kft. telephelyén, annak folyosóján kifüggesztve, valamint a Büttner Kft. weboldalán kell közzétenni.
A politika editálható verzióját a szervezet központi szerverén az IBIR mappában kell tárolni. Az információbiztonsági politika hatályos verziója nyilvánosan is elérhetővé kell tenni a Szervezet weboldalán és a szervezet telephelyén olyan helyen, ahol a vendégek is hozzáférnek.

3. Fogalmak

A jelen szabályzatban használt fogalmakat az IBIR Törzsdokumentuma tartalmazza.

4. A Büttner Kft. környezete

A Büttner Kft. környezetének bemutatását az IBIR Törzsdokumentuma tartalmazza.

5. Információbiztonsági szabályozások

5.1 A vezetői elkötelezettség

Az ügyvezető elkötelezettségét személyes példamutatással (szabályozások betartása) és személyes felelősségvállalással demonstrálja.
A belső és külső szolgáltatói megállapodások figyelése, figyelembevétele és a bennük megfogalmazott paraméterek mérése a vezetői elkötelezettség egyik kinyilvánítási módja. Az információbiztonsági intézkedések megvalósításához szükséges erőforrások biztosítása, szintén a vezetői elkötelezettséggel összhangban történik.

5.2 Bizalmassági nyilatkozatok

A Büttner Kft. minden alkalmazottjával és a bizalmassági kérdésben érintett egyéb érdekelt féllel bizalmassági nyilatkozatot (BSZ01_Bizalmassági nyilatkozat) kell kitöltetni, melynek aláírásával vállalja, hogy megértette a jelen biztonsági szabályzatban foglaltak rá vonatkozó részeit és a megismert információkkal nem él vissza.
Az információbiztonsági szabályok betartásával és betartatásával kapcsolatban a IBIR/BSZ01 mappában részletezett bizalmassági nyilatkozatot írnak alá az érdekelt felek, melyet a humán dokumentumok között tárolnak.

6. Az információbiztonság szervezete

6.1 Az információbiztonság belső szervezete

6.1.1 Felelősségi körök

A Büttner Kft. információbiztonsági tevékenységét az Információbiztonsági felelős vezeti és dönt valamennyi információbiztonságot érintő kérdésről, az IBIR részét képző szabályzatról.

Az Információbiztonsági felelős szerepkört a Társaság kiszervezte és külső szakértőt bízott meg a feladatkör ellátására arra az időre, míg szervezeten belül a megfelelő kompetenciát kialakítják.

6.1.2 A feladatkörök szétválasztása

A Büttner Kft. belső szervezeti folyamataiban definiált szerep és feladatköröket oly módon kell meghatározni és dokumentálni, hogy a véletlen vagy szándékos szervezeti vagyonelemek elleni támadás kockázata minimalizálható legyen.

- Az engedélyezési folyamatokban az igénylő, engedélyező és végrehajtó szerepköröket külön kell választani,
- Kifejezetten figyelni kell az egyedi fejlesztéseknél a fejlesztői és a tesztelői munkakörök és jogosultságok elkülönítésére.

6.1.3 Az információbiztonság a projektirányításban

A Szervezet a vevői megrendelések és szolgáltatások vagy a szolgálatáson belül indított projektek keretében a szerződéskötés során (pl. titoktartási nyilatkozat) kezeli az információbiztonsági elvárásokat.

Minden 5 000 000 millió forintot meghaladó nem az alaptevékenységgel kapcsolatos projekt indításakor, konzultálni kell az Információbiztonsági felelőssel, szükség szerint meg kell határozni azon, a projekttel kapcsolatos információbiztonsági elvárásokat, melyek eltérnek a jelen szabályzat elvárásitól. A projektekben az Információbiztonsági felelős szúrópróbaszerűen ellenőrizheti az elvárások betartását.

6.1.4 Kapcsolattartás hatóságokkal, érdekelt felekkel

Hatósági kapcsolattartásra és egyéb információbiztonsági csoportokkal, szakmai csoportokkal, vagy más specializálódott biztonsági fórumokkal és szakmai egyesületekkel való kapcsolattartársa kijelölt személy az információbiztonsági felelős, aki a partnerek információbiztonsági szakértőivel is kapcsolatot tart fenn.

6.2 A mobil eszköz és a távmunka

6.2.1 A mobil eszköz használata és védelme

A Büttner Kft. a mobil eszközöket munkavégzés céljából bocsátja a munkavállaló rendelkezésére. Ha a munkavállaló munkavégzéséhez szükséges a mobilitás, a mobil informatikai eszköz biztosításáról az Ügyvezető dönt. A mobil eszköz használatának engedélyezésével a szervezet egyben hozzájárul a mobil eszköz telephelyen kívüli használatához. Az eszközöket kizárólag a Büttner Kft. alkalmazottja vagy szerződéses partnere használhatja, az eszközök harmadik fél számára nem adhatóak át.
A mobil eszközöknek a Büttner Kft. telephelyén kívüli használata esetén az eszköz használatából, elvesztéséből adódó, bármilyen adatszivárgás vagy adatvesztés következménye a felhasználót terheli.
A Büttner Kft. által biztosított notebookokon, egyéb mobil eszközön, magán célú felhasználás nem engedélyezett, kivétel ez alól a Büttner Kft. által biztosított mobiltelefon. A mobil eszközön való munkavégzés alkalmával a felhasználó felelős az eszköz rendeltetésszerű használatáért, valamint a „váll feletti betekintéses” adatszivárgás megelőzéséért.

6.2.1.1 Mobiltelefon szabályok

A nem a Büttner Kft. által biztosított IT eszközök, mobiltelefonok használata szervezeti adatok elérésére, kezelésére (pl. email,) esetében alapértelmezetten tiltott. Amennyiben a munkavégzéshez szükséges, Információbiztonsági felelős dokumentált jóváhagyásával, kizárólag az e-mail és a MSTeams alkalmazások használhatók.
A felhasználó felelőssége, hogy gondoskodjon a Büttner Kft. adatvagyonának védelméről, a mobil eszközökön automatikus zárolás, biometrikus azonosítás beállítása szükséges.

6.2.2 A távoli bejelentkezés

A Büttner Kft. rendszereinek távoli menedzsment hozzáférése, megfelelő titkosítással bíró adatkapcsolattal, külső hálózatból is engedélyezett. Minden egyéb hozzáférési kísérlet incidensnek minősül és logikai védelmi intézkedésekkel is megakadályozható az üzemeltetők részéről.
Speciális hálózati szolgáltatásokkal (pl. VPN kapcsolat kettős authentikációval) az intranet, a szervezet fizikai hálózatán kívülre is meghosszabbítható, ezáltal a munkahelyen kívüli munkavégzés megvalósítható. Ezen megoldások önerős megvalósítása nem megengedett, kizárólag a Büttner Kft. távoli elérési szolgáltatásai vehetők igénybe.

A távoli bejelentkezést kizárólag a Büttner Kft. tulajdonát képző és a vagyonleltárban szereplő eszközökről, lehet megvalósítani. A Biztonsági vezető egyedi eseteben, dokumentáltan engedélyezheti az eltérést a fent meghatározott elvárások alól, amennyiben a távoli bejelentkezésre használni kívánt IT eszköz megfelel a jelen IBSZ által támasztott biztonsági kritériumoknak, az igénylő vállalja, hogy az IBSZ által támasztott követelményeket a saját eszközén is betartja.

A felhasználók távoli hozzáférésének engedélyezésekor is a legkisebb jogosultság, legkevesebb hozzáférés elvét kell követni.

7. Az emberi erőforrás biztonságával kapcsolatos kérdések

A munkáltatói jogokat az Ügyvezető gyakorolja. A felvételi és elbocsátási folyamatok lebonyolításáért az HR vezető a felelős.

7.1 Az alkalmazás előtti feladatok

A Büttner Kft. szervezetében a munkaerő-felvételt az HR-csoport egy tagja bonyolítja le, szükség szerint elvégzi, vagy elvégezteti a jelentkező előzetes háttérellenőrzését.

A munkaerő-felvétel folyamata:

- A munkaerő felvételéről az Ügyvezető dönt.
- A döntést követően az HR csoport elkészíti a munkakörrel kapcsolatos elvárásokat és ezek alapján az meghirdetésre kerül az álláshirdetés.
- Az álláshirdetést a pozíciótól függően a Büttner Kft. a honlapján, a Facebook oldalán, álláskereső portálon, fejvadász cégen keresztül vagy egyéb médiafelületen teszi közzé.
- A jelölt vagy a fejvadász cég képviselője e-mailben elküldi önéletrajzot a munka@buttner.hu vagy a vezetoseg@buttner.hu e-mail címére a pozíció bizalmasságának megfelelően.
  Amennyiben a beérkező email az info@buttner.hu vagy a titkarsag@buttner.hu email címre érkezik, a fiókot kezelő késedelem nélkül továbbítja a beérkezett önéletrajzot a munka@buttner.hu email címre. A továbbítást követően az elküldött elemek közül és a fogadó postafiókból is törli a beérkezett önéletrajzot tartalmazó emailt-.
- A toborzási folyamatba bevont vállalkozó vállalja, hogy a toborzási folyamat során tájékoztatja a jelölteket a Büttner Kft. adatkezelési tájékoztatójába foglaltakról.

- A jelölt kiválasztásáról és alkalmazásról az Ügyvezető dönt.
- A jelölteknek az alkalmazást megelőzően szükség szerint szakirányú végzettséget igazoló dokumentumot kell bemutatni. A bemutatott dokumentumok azonosítóit, a Büttner Kft. a munkavállaló HR dokumentumai között tárolhatja.
- A Büttner Kft. minden munkavállalója a munkaszerződés részeként titoktartási nyilatkozatot (BSZ04 Titoktartási nyilatkozat) kell aláírjon.

7.2 Az alkalmazás alatti tennivalók

A Büttner Kft. minden felhasználójától elvárja, hogy a jelen szabályozásban foglaltakat és az egyéb szervezeti szabályozások információbiztonsági előírásait betartsa és mind a kollégákkal mind a szerződött partnerekkel betartassa.

A munkavállalók az alkalmazásuk során:

- az első munkanapjukon megismerik a Büttner Kft. belső szabályait és a kommunikációs rendet,
- megismerik a Büttner Kft. IBIR rendszerét és rájuk vonatkozó elvárásokat,
- megismerik az Információbiztonsági oktatás anyagát,
- az oktatási naplóban aláírásukkal igazolják az ismeretek elsajátítását.

7.2.1 Az információbiztonsági tréning

A Büttner Kft. kiemelt figyelmet fordít az információbiztonság oktatására. Évente egyszer információbiztonsági tudatosító tréninget tart az alkalmazottak számára. Az információbiztonsági oktatások megszervezése és lebonyolítása az HR csoport feladata, a tréning tematikájának összeállítás és a tréning megtartásáért a Információbiztonsági felkelős a számonkérhető.
Az információbiztonsági tréningen való részvételről dokumentált információkat kell tárolni (BSZ05 mappa).
Az oktatást követően a résztvevőknek aláírásukkal igazolniuk kell részvételüket és az adott oktatáson elhangzottak megismerését.
Az információbiztonsági képzésen megszerzett tudás mindennapi használatát az Információbiztonsági felelős év közben több alkalommal is ellenőrizheti.

7.2.2 A fegyelmi eljárás

Az IBSZ előírásainak szándékos és tudatos megsértése esetén a munkavállaló vagy szerződéses partner szankcionálható. A szankciókat az Ügyvezető határozza meg. A jegyzőkönyveket a BSZ06 mappában kell tárolni.
A Büttner Kft., ügyvezetői döntés alapján jogosult kizárni a felhasználói körből az IBSZ-t súlyosan megsértőket.

7.3 A munkakör változása vagy a munkaviszony megszűnése

A dolgozó munkaviszonyának megszüntetése vagy megszűnése esetén a felhasználói, az üzemeltetői és kiemelt jogosultságokat, a tevékenységet lehetővé tevő belépési kódokat és a fizikai belépésre jogosító eszközöket és a hozzáférést azonnal vissza kell vonni.
A munkavállaló köteles az általa használt, a Büttner Kft. tulajdonát képző összes vagyontárgyat hiánytalanul leadni az utolsó munkában töltött napon.
Az átadás-átvételt és a jogosultságok megszüntetésének igazolására a Büttner Kft. papíralapú dokumentumot (Kilépő adatlap) használ.
Amennyiben a volt dolgozó, a tevékenységeket szerződéses partnerként végzi a továbbiakban, akkor a szerződés megkötése után, Ügyvezetői jóváhagyással új, partneri hozzáférés biztosítható számára, az ott részletezett szabályok alapján.

7.3.1 A kiléptetési folyamat

- A munkaviszony megszűnéséről / megszüntetéséről vagy elfogadásáról az Ügyvezető dönt.
- A döntést követően a HR vezető / IT vezető lebonyolítja le az eszközök átadás-átvételét.
- Az Ügyvezető dönt a felhasználó elektronikus levelezésének átirányításáról és az ügyfelek értesítésének szükségességéről.
- Az IT csoport egy tagja az utolsó munkába töltött napon, de legkésőbb 24órán beül megszünteti a felhasználói jogosultságokat.

A munkaviszony megszűnésével/megszüntetésével kapcsolatos feladatok ellenőrzéséért az HR vezető a felelős.

8. A vagyonelemek menedzsmentje

8.1 Felelősség az információvagyonért

8.1.1 Vagyonleltár

Az IBSZ tárgyi hatálya alá tartozó vagyonelemekről leltárt kell készíteni, beleértve fizikai és az adatvagyon elemeket is.
A szervezet hardware, szoftver leltárát folyamatosan napra készen a B2MS rendszerben kell tartani, az eszközök vásárlását és selejtezését követően. Az eszközök jelölése, azonosítása service tag, vagy sorozatszám alapján történik. Az IT eszközöket a felhasználók részére történt átadást követően a B2MS rendszerben kell felhasználó nevére rögzíteni. A nyilvántartásban szereplő eszközök felelőse az a felhasználó akinek a nevén nyilvántartja a szervezet az adott eszközt. A Home Office használatra kiadott eszközöket papír alapú átadás-átvétel dokumentummal kell rögzíteni. A Büttner Kft. szoftverelemeinek és adatvagyonának leltárát a BSZ10 mappában kell tárolni.

8.1.2 A vagyonelemek tulajdonjoga

A Büttner Kft. IT rendszereiben tárolt minden szervezet specifikus adat (és annak minden felhasználási joga) a Büttner Kft. tulajdonát képezi. Ugyanezen rendszerek konfigurációs adatai és beállításai (minden olyan konfigurációs komponens, ami a vásárolt rendszerben található állapottól eltér), a Büttner Kft. tulajdonát képezi. Felhasználásuk a munkafeladatok ellátásához szükséges módon és mértékben, a legkisebb jogosultság elve szerint engedélyezett, ezektől eltérni a Szervezet Ügyvezetőjének írásbeli engedélyével lehetséges.

8.1.3 A vagyonelemek elfogadható használatának szabályai

A Büttner Kft. vagyonleltárában szereplő vagyonelemek rendeltetésszerű használatáért a felhasználója a felelős, az alábbiak szerint:

- A használat során be kell tartani az eszközök használati utasításában foglalt követelményeket.
- Az eszközöket tisztán, üzemképes állapotban, fizikai sérülésektől védve kell használni.
- A felhasználó felelőssége, hogy az észlelt működési rendellenességeket az Ügyvezetőnek haladéktalanul jelentse.
- Tilos a számítógépeket és a perifériákat az IT üzemeltetésben nem résztvevő munkavállalóknak:
    - elmozdítani,
    - burkolatukat megbontani,
    - összeköttetéseiket megváltoztatni,
    - nem üzemszerűen használni.

A Büttner Kft. informatikai eszközeit használók számára kifejezetten tilos olyan adatot (beleértve a video, hang, és képanyagot) tartani a számítógépen, amelyik adatszerzői jogának tulajdonosa nem a számítógép felhasználója, vagy bármilyen módon törvénybe ütközik. Minden olyan kárért, amely a jogszerűtlenül használt programból, adatból származik, a munkavállaló a felelős.

8.2 Az információvagyon osztályozása

Az információs vagyonelemek osztályba sorolása, adatvagyon osztályozásának felülvizsgálata az Információbiztonsági felelős a feladata. A vagyonelemek szabályzat szerinti kezelését az Információbiztonsági felelős szúrópróbaszerűen ellenőrizheti.

A Büttner Kft. az alábbi információosztályokat vezeti be:

Publikus:
Ebbe a kategóriába tartoznak Ügyvezetői jóváhagyás alapján azok az adatok és információk, melyek korlátozás nélkül terjeszthetők harmadik fél számára. Ide tartoznak például a Büttner Kft. saját weboldalán és a közösségi médiában közzétett információk és az állashirdetések a közzététel időpontjától.

Belső használatú:

Minden olyan dokumentum – függetlenül annak keletkezési helyétől és hordozójától – ami kizárólag a Büttner Kft. munkavállalói és szerződéses partnerei számára – a szerződése által meghatározott szintig – hozzáférhetők. A Belső használatú kategóriába tartozó adatok és információk harmadik fél számára, csak az Ügyvezető engedélyével, megfelelő titoktartási nyilatkozat aláírását követően, vagy az adatokat a Büttner Kft. részére átadó megrendelő kifejezett kérésére adhatóak ki.

Titkos:
Az Ügyvezető által Titkosnak nyilvánított dokumentum, adat vagy információ.

8.2.1 Az információvagyon jelölése

Publikus:
A Büttner Kft. Ügyvezetője által Publikusnak minősített adatok tárolásának helyét a Szervezet központi szerverén kell kialakítani. A Publikus dokumentumokat a felhasználók a szervezet által üzemeltetett B2MS rendszerben érhetik el. A Publikus dokumentumokat és információkat a web bármely szegmensébe történő feltöltésekor/publikálásakor már nem kell külön jelöléssel ellátni.

Belső használatú:
A Belső használatú dokumentumokat nem kell külön jelöléssel ellátni. A külön jelöléssel el nem látott és a Büttner Kft. által kezelt bármely dokumentumot, Belső használatúnak kell tekinteni. Az adatokhoz felhasználói azonosítást követően, a legkisebb jogosultság elve alapján férhetnek hozzá a felhasználók.

Titkos:
A Titkos minősítésű, digitális dokumentumok esetén a tárolás a Büttner Kft. fájlszerverén, a Management által meghatározott mappákban történik. A mappák nevében szerepelnie kell a „Titkos” karaktersornak .
A papír alapú dokumentumok esetén minden oldalon, vagy a fedlapon, vagy a dokumentumokat tároló mappák külső felületén fel kell tüntetni a „Titkos” jelölést.

8.3 Adathordozók kezelése

8.3.1 A szállítható információhordozók kezelése és szállítása

A Büttner Kft. adatvagyon leltárában szereplő elemeket lehetőleg titkosított formában kell szállítható adathordozón tárolni.
A Windows operációs rendszer alapú hordozható eszközök titkosítására a rendszerbe épített BitLocker alkalmazást kell használni.
Az Apple OS operációs rendszer alapú eszközök titkosítása, az Apple beépített FileVault megoldásával történik vagy ezzel egyenértű titkosítási megoldással.
Mind a Bitlocker mind pedig a FileVault esetében, az egyedi kód alapú titkosítási paramétert kell választani és minden eszköz mesterkulcsát a BSZ-33 mappában kell tárolni, jelszóval védett fájlban.

A Büttner Kft. informatikai rendszerében belső használatú vagy ügyfél adatot, kizárólag nyilvántartott, jelölt, titkosított adathordozók használhatók, beleértve a külső mobil merevlemez-tárolókat és az USB-tárolókat is.
Az üzemeltetési feladatok ellátásához szükséges nyilvántartott, titkosítás nélküli USB-s tárolók használata (pl.: image telepítés), ezen eszközökön belső használatú vagy ügyfél adat tárolása tilos.

8.3.2 Nyilvántartott adathordozók kezelése

- A Büttner Kft. azon munkavállalói részére, akiknek a feladat ellátásához szükséges titkosított USB drive-ot biztosít. Eseti jelleggel, szükség esetén az IT vezetőnél igényelhető és a feladat elvégzését és az adatok törlését követően neki adják vissza az eszközt.
- Az USB-s drive-on csak a munkavégzéshez feltétlenül szükséges adatokat, a szükséges ideig lehet tárolni, különös tekintettel az ügyfelek adataira (pl. migráció).
- Minden felhasználó köteles a részére átadott drive-ot a felügyelete alatt tartani, és egyben tudomásul venni, hogy a drive elvesztéséből adódó információbiztonsági incidensek következményei Őt terhelik.
- A felhasználók tudomásul veszik, hogy a drive-on saját tulajdonú adatot nem tárolhatnak vagy kezelhetnek.

8.3.3 Nem a Büttner Kft. tulajdonában lévő (külsős) adathordozók kezelése

Amennyiben a Büttner Kft. egy vendége vagy üzleti partnere egy USB adathordozón kíván adatot átadni a Büttner Kft. részére az adatátadás csak az IT üzemeltetés bevonásával a következő feltételekkel valósulhat meg:

- A külső adathordozót a Büttner Kft. által biztosított IT eszközhöz, nem a szervezet tulajdonában lévő adathordozón, csatlakoztatás után minden esetben vírusellenőrzést kell indítani, a telepített vírusvédelmi megoldásával.
- Amennyiben a vírusellenőrzés nem talált fertőzést vagy gyanús állományt a Külsős adathordozóról a szükséges adatok a Büttner Kft. informatikai rendszerébe másolhatóak.
- Amennyiben a vírusellenőrzés során fertőzés kerül beazonosításra, vagy a rendszer gyanús állományt talál az adathordozón, az adathordozót azonnal el kell távolítani a Büttner Kft. informatikai rendszeréből. Az adatok NEM használhatók és kezelhetők a Büttner Kft. informatikai rendszerében.

8.3.4 Az adathordozók megsemmisítése

Használatból kivont eszközök:
A használatból kivont berendezéseket értékesíteni, csak az adathordozón található adatok megfelelő törlését, visszaállíthatatlan törlési megoldás alkalmazása után lehetséges.
A nem továbbértékesített eszközök esetében az adathordozókat el kell távolítani az eszközből és fizikai roncsolással meg kell semmisíteni.

A Büttner Kft. az adathordozójuktól megfosztott berendezéseket a vonatkozó hulladékgazdálkodási és környezetvédelmi szabályok betartása mellett selejtezi le és távolítja el.

A használatból kivont adathordozókat a megsemmisítésig zárt szekrényben, az aktív állapotban alkalmazott fizikai védelemmel megegyező módon kell védeni. Az Ügyvezető gondoskodik kell a kor technikai színvonalának megfelelő, legbiztonságosabbnak tekinthető módon történő megsemmisítéséről.

9. A hozzáférés szabályozása

9.1 Működési követelmények a hozzáférés szabályozására

Minden olyan informatikai rendszer esetében, ami a Büttner Kft. működéséhez szükséges, illetőleg bármilyen védett információt tartalmaz, a legkisebb jogosultság elve mentén meg kell határozni és dokumentálni a hozzáférésre jogosultak körét. Hozzáférés kezdeményezésekor a jogosultságot ellenőrizni kell. Az informatikai rendszerhez tartozó módosítást és a védett adatok lekérdezését lehetővé tevő hozzáférésre kizárólag egy másik, jóváhagyott IT rendszer vagy egy feljogosított felhasználó lehet jogosult.
A kiosztott jogosultságokat a Büttner Kft. az adatvagyon leltár kiegészítéseként kell tárolni
A jogosultságkezelési listát az Információbiztonsági felelős évente egyszer felül kell vizsgálja.

9.2 A jogosultság beállítása

A felhasználók jogosultsága határozza meg, hogy a felhasználó, a fejlesztő, a rendszergazda milyen műveleteket hajthat végre az egyes alkalmazások, szolgáltatások használatakor. A Büttner Kft. hálózatához érvényes jogosultság, illetve azonosító és jelszó nélkül senki nem kapcsolódhat.

9.2.1 A jogosultság igénylésének folyamata

A felhasználók jogosultságait, csoporttagságát szerepkörök alapján, munkába álláskor automatikusan kapják meg, egyedi hozzáférés igénylés alapértelmezetten nincs. Abban az esetben, ha egyedi hozzáférésre lenne szükség, a munkavállaló a B2MS rendszerben írt hibajegyeben jelezheti ezt és Információbiztonsági felelősi jóváhagyás után kerülhet beállításra. A beállítást az IT üzemeltetési csoportnak kell elvégeznie.

A felhasználók csoporttagságát és az egyedi hozzáférési igényeket az adott adatvagyon elem adatgazdája vagy az ügyvezető vagy az Információbiztonsági vezető hagyja jóvá.

9.2.2 A jogosultság megszüntetése

A munkaviszonynak a Büttner Kft.-n belüli megváltozása (feladatkör váltás), illetve a munkaviszony megszűnése/megszüntetése információbiztonsági szempontból hasonlóan kezelt kategóriák. Az áthelyezett munkatárs munkaállomásán tárolt adatainak és elektronikus leveleinek (e-mail) átvihetőségéről az Ügyvezető dönt.

A Büttner Kft.-n belül áthelyezett felhasználó a személyéhez kapcsolódó hozzáférésein kívül (pl. e-mail cím) semmilyen korábbi – az informatikai alkalmazások, rendszerek eléréséhez kapott – hozzáférési jogot nem vihet magával az új feladatkörébe.
A munkaviszony megszűnéséről/megszüntetéséről hozott döntést követően az IT üzemeltetési csoport egy munkatársa a felhasználói jogokat a jogviszony utolsó munkában töltött napján kell visszavonja.

- A hozzáférési jogokat minden rendszerből vissza kell vonni.
- Az informatikai jogosultságokon kívül, a visszavonásra kerülő vagy átalakítandó hozzáférési jogok közé tartoznak a fizikai vagy logikai hozzáférések, azonosítók, beléptető kártyák, kulcsok, előfizetések. Különös figyelemmel kell lenni a hozzáférést biztosító jelszavak visszavonására, illetve megváltoztatására.

A munkakör átadási folyamat részeként, indokolt esetben rendelkezni kell:

- automatikus e-mail üzenet kiküldéséről, amely azt tartalmazza, hogy a postaláda tulajdonosa a leveit nem olvassa és a beérkezett üzenet automatikusan törlésre került.
- a munkafeladatokkal összefüggő levelek a továbbiakban mely e-mail címre legyenek elküldve.

9.2.3 A privilegizált felhasználói jogosultságok kezelése

A Büttner Kft. informatikai üzemeltetését saját hatáskörben végzi. Az adminisztrátori tevékenységgel végzett munkafolyamatok naplózásra kerülnek, legalább az alábbiak szerint:

- belépés
- kilépés
- módosítások

A nem adminisztrációval foglalkozó felhasználók nem kaphatnak hozzáférést az adminisztratív rendszerszoftverekhez vagy segédprogramokhoz.
A munkaállomásokon a felhasználók amennyiben a munkafeladataik elvégzéséhez szükséges, lokális rendszergazdai jogosultsággal rendelkezhetnek. A szervezetben minden kiemelt jogosultságú felhasználó magasan képzett IT szakember, információbiztonsági ismeretekkel, ennek megfelelően tisztában vannak az üzemeltetés megfelelő szabályaival és kockázataival.
A Büttner Kft. eszközeit használó felhasználók, minden esetben a felhasználás megkezdése előtt kötelesek aláírni a rendszergazdai jogosultságból származó kockázatok kezelésére szóló nyilatkozatot, a BSZ07 minta alapján.

Az Ügyvezető tisztában van az üzemeltetés kockázataival, amit a kockázatértékelés során értékel, szükség szerint kockázatcsökkentő intézkedéseket rendel el.

Kiemelt vagy adminisztratív fiókot csak a rendszerek, adatbázisok és alkalmazások kezeléséért felelős felhasználók kaphatnak.

Adminisztrátori fiókok esetén törekedni kell az egyedi felhasználónevek használatára.

9.2.4 A technikai felhasználók kezelése

Azokban az esetekben, ha a szervezet által fejlesztett vagy üzemeltett rendszerek közötti kommunikációt egy felhasználó nevében kell végrehajtani:

- kifejezetten tiltott az informatikai rendszer általános adminisztrátori felhasználó adatait használni erre a célra,
- minden rendszerhez külön technikai felhasználót kell létrehozni,
- a technikai felhasználókról nyilvántartást kell vezetni a BSZ20 dokumentumban,
- a technikai felhasználókhoz tartozó jelszavakat a lehelő legkisebb körben kell publikálni és a hozzáférést a kockázatokkal arányosan kell védeni. A jelszavak tárolását a Büttner Kft. a központi szerveren egy védett dokumentumban vagy titkosított módon védett jelszó kezelő rendszerben kell megvalósítani.
- a jelszavakat csak abban az eseten kell megváltoztatni, ha egy olyan kolléga távozik a szervezettől, aki ismerte a hozzáférési adatokat vagy lehetősége volt azok megváltoztatására.

9.3 A felhasználói felelősség

A Büttner Kft. rendszereinek felhasználója, munkaköri felelőssége az adatok bizalmas kezelése. A Büttner Kft. rendszereit a felhasználó csak munkakörének keretei között, erőforrás-kímélő módon, a kezelési utasításoknak megfelelően használhatja. Köteles a rendelkezésére bocsátott egyedi azonosítók biztonságát és bizalmasságát megőrizni. Harmadik fél számára tilos a biztonsági azonosítók átadása.

9.4 A hozzáférési és jelszókezelési politika

A jelszóválasztásnál minden felhasználónak figyelembe kell vennie jelen szabályzat jelszavakkal kapcsolatos biztonsági elvárásait. A felhasználóktól meg kell követelni, hogy a jelszavak kiválasztásában és használatában a jó biztonsági gyakorlatot kövessék, lehetőség szerint többfaktoros authentikációt kell alkalmazni a hozzáférések biztosításához.
A rendszerekhez történő hozzáférést központosítani kell, amennyiben lehetséges minden rendszert össze kell kötnie a központi autentikációt ellátó rendszerrel.
Kezdeti jelszavak küldése SMS-ben, telefonon vagy one-time-secret megoldással történik. A kezdeti jelszavak megváltoztatását a rendszerekben lehetőség szerint ki kell kényszeríteni.
Az olyan kiemelt jogokkal bíró segédprogramok használata esetén, melyek képesek lehetnek arra, hogy felülírják a rendszer- és alkalmazásszintű védelmi intézkedéseket, korlátozni kell, és szoros felügyelet alatt kell tartani.

9.4.1 A jelszókezelés komplexitása

A Büttner Kft. a munkaállomások és szerverek jelszókomplexitásának követelményeit az BSZ-35 mappában

9.4.2 Az operációs rendszerhez való hozzáférés

Az operációs rendszerekben a felhasználók kizárólag egyedi azonosítás után végezhetnek munkát.

9.4.3 Levelezés biztonsága

A Büttner Kft. informatikai rendszerében olyan központi beállításokat kell alkalmazni, hogy a levelezés webböngészőn keresztüli elérése (webmail) vagy ezzel egyenértékű felhasználás esetén a fiókhoz kizárólag kétfaktoros authentikáció után lehessen hozzáférni.

10. A titkosítási eljárások és a titkosító kulcsok kezelése

A Büttner Kft. rendszereibe távolról történő, módosítási jogosultságot is lehetővé tevő bejelentkezés csak titkosított kommunikációval (pl. SSH, SSL, IPsec) engedélyezett.
A hozzáférési jogosultságok elbírálását végző komponensek bármely rendszer esetében a felhasználói jelszavakat csak titkosítva tárolhatják.
A szervezeti jelszavak kezelése jelszóval védett fájlban történik.

10.1 Jelszavak központi tárolása kezelése

A Büttner Kft. informatikai rendszerinek üzemeltetésével kapcsolatosan használt jelszavak tárolására jelszó széfet kell alkalmazni. A jelszó széf hozzáférését kontrolálni kell és a hozzáférést minden alkalommal felül kell vizsgálni, amit egy adminisztrátori jogosultsággal rendelkező kolléga távozik a szervezettől. A jelszó széf adatbázisát a szervezeten belül az erre a célra kijelölt központi szerver vagy adattárón (NAS) kell tárolni.
Az informatikai rendszerekhez tartozó Adminisztrátori jelszavakról papír alapú másolatot kell tárolni az Büttner Kft. titkársági zárt szekrényben.

11. A fizikai és környezeti biztonság

11.1 Biztonsági zónák, területek

11.1.1 Fizikai biztonsági zónák

A Büttner Kft. adatvagyonának kezelése, feldolgozása a Szervezet székhelyen valósul meg.

A Székhely területei adatbiztonsági szempontból az alábbi zónákra vannak osztva.

- Irodai zóna
- Szerver szoba zóna
- Gyártási területi zóna
- Irattár zóna
- vezetői szoba zóna

11.1.2 A területekre vonatkozó fizikai előírások

11.1.2.1 Valamennyi területre érvényes szabályok

A telephelyen elvárás, hogy az épület, az épület elektromos hálózata, valamint túlfeszültség- és villámvédelme elégítse ki a mindenkor hatályos kommunális lakó-, irodaépületekre és gyártási területre vonatkozó szabványokat.

11.1.2.2 Az irodai zónára vonatkozó további védelmi intézkedések

Belépési szabályok

A felhasználók munkaidőben, a Büttner Kft. alkalmazottai időbeli korlátozás nélkül, szabadon léphetnek be az irodahelyiségekbe.
A belépéshez a portaszolgálaton azonosítani kell a belépő munkavállalót. A munkavállalót az élő erős őrzést biztosító biztonsági szolgálat egy munkatársa végzi el. A telephelyet a 22.00 – 06 .00 között zárva kell tartani és a telepített riasztórendszert élesíteni szükséges. A vagyonőr távozásakor meg kell győződjen róla, hogy a telepített videokamera rendszer üzemel.

A nem munkavállalók, illetve a belépésre jogosultak listájában nem nyilvántartott személyek, a társaságtelephelyére csak a portán történt regisztrációt követően léphetnek be. A 6 hónapnál régebbi adatokat tartalmazó belépők nyilvántartását évente egy alkalommal automatizált módon kell törölni.

Tartózkodási szabályok
Az alvállalkozók, a beszállítók és partnerek munkaidőn belül és kívül kizárólag munkavállaló által kísérve, felügyelve tartózkodhatnak.

Adatkezelési szabályok
Az irodai helyiségekben kezelhetők belső használatú, személyes és titkos adatok is.

11.1.2.3 Szerver szoba

A szerverszoba ajtaját fizikai behatolás védelemmel kell ellátni. A helyiségbe való belépéseket nyilván kell tartani. A szerverszobába állandó belépésre jogosultak az IT csoport tagjai.
A szerver szobába belépő vendégekről nyilvántartás kell vezetni, melyet az adott helységben kell tárolni. Az szerver szobák tűzvédelméről és a megfelelő elektronikus tüzet is oltani képes oltóberendezésekről gondoskodni kell.
A szerverszoba védelmét hőmérséklet és vízérzékelővel kell megvalósítani, amely az előre beállított határérték elérésekor riasztást küld az IT rendszer üzemeltetési csoportjának.
A szerverek áramellátását az üzleti igényeknek megfelelően szünetmenet áramforrásokkal kell ellátni.

Tartózkodási szabályok
Alapértelmezetten állandó tartózkodásra nem használható a helység

Adatkezelési szabályok
Az helyiségekben kezelhetők és tárolhatók belső használatú, személyes és titkos adatok is.

11.1.2.4 Irattár Zóna

Az irattár zóna határát (ajtaját) fizikai behatolás védelemmel kell ellátni. A helyiségbe való belépéseket nyilván kell tartani. Az irattára folyamatosan zárva kell tartani csak a benntartózkodás idejére lehet az ajót nyitva tartani.
Az irattár tűzvédelméről és a megfelelő oltóberendezésekről gondoskodni kell.
Az irattárba minden belepéséről nyilvántartás kell vezetni, melyet az adott helységben kell tárolni.
Az iratárba engedélyezett belépők és helyettesítőikről nyilvántartást kell vezetni.

Tartózkodási szabályok
Alapértelmezetten állandó tartózkodásra nem használható a helység.

Adatkezelési szabályok
Az helyiségekben kezelhetők és tárolhatók belső használatú, személyes és titkos adatok is.

11.1.2.5 Vezetői szoba zóna

Az vezetői szobák határát (ajtaját) fizikai behatolás védelemmel kell ellátni. A helyiségbe való belépéseket nyilván kell tartani. A vezetői szobák ajtaját csak akkor lehet nyitva tartani, ha egy oda kulccsal rendelkező kolléga a szobában tartózkodik. Az utolsó távozáskor a szobát be kell zárni.
A vezető szobák tűzvédelméről és a megfelelő oltóberendezésekről gondoskodni kell.

Tartózkodási szabályok
A helységekben a kijelölt a helységhez kulccsal rendelkező személyek tartózkodhatnak. A kulccsal nem rendelkező munkavállaló és vendégek felügyelet nélkül nem tartózkodhatnak a helységben se

Adatkezelési szabályok
Az helyiségekben kezelhetők és tárolhatók belső használatú, személyes és titkos adatok is.

11.1.2.6 Gyártási területi zóna

A gyártási területlenre a belépést a Büttner Kft. határvédelmével kell megvalósítani. A portaszolgálaton belépő munkavállalók jogosultak a gyártói területre történő belepésre. A vendégeket információbiztonsági és munkavédelmi szerpontiok miatt is folyamatosan kísérni kell. nyilván kell tartani.

Tartózkodási szabályok

Munkavállalók a munkabeosztásnak megfelelő időben tartózkodhatnak az adott gyártói területen. Az alvállalkozók, a beszállítók és partnerek munkaidőn belül és kívül kizárólag munkavállaló által kísérve, felügyelve tartózkodhatnak.

Adatkezelési szabályok
Az helyiségekben csak a gyártási folyamathoz szükséges belső használatú és akár titkos adatok kezelhetők, de ott nem tárolhatók.

11.2 Eszköz biztonság

11.2.1 Az eszközök elhelyezése, védelme

A Büttner Kft. iroda helységeiben alkalmazott munkaállomások és notebookon védelme nem kíván az általános eszközhasználat elvárásokon felül különleges védelmet.
A gyártó területen elhelyezett informatikai eszközök esetében úgy kell kialakítani a tárolás helyet, hogy a gyártás következtében az eszköz fizikai, hő és tűzvédelme megvalósítható legyen.
Azoknál az hálózati eszközüknél melyek védelme aránytalan költséget jelentene a meghibásodás esetére azonnali csereeszközt kell raktáron tartani.
A notebookok fizikai védelméért a felhasználó, a szerverek fizikai védelméért az IT vezető a felelős. Az eszközöket használat során folyamatos felügyelet alatt kell tartani és védeni a külső fizikai károsodástól és a lopástól.

11.2.2 Támogató közművek, szolgáltatások

A Büttner Kft. telephelyén redundáns internetkapcsolatot kell kialakítani. Az elektromos ellátás biztosítása érdekében a kockázatkezelés alapján a megfelelő helyekre szünetmenetes áramforrásokat kell telepíteni az esetleges áramszünetek kivédése érdekében.

11.2.3 Kábelbiztonság

A Büttner Kft. telephelyén, saját erős vagy gyengeáramú hálózattal. A Büttner Kft. irodai zónában, illetve minden munkatársa és alvállalkozója a Home office tevékenység során úgy kell kialakítsa az elektromos hálózati csatlakozást, hogy balesetmentesen és az eszközök védelmének megfelelő módon kapcsolódjanak az elektromos és az informatikai hálózathoz.
A Gyártási zónában kifejezett figyelmet kell fordítani mind az erős áramú mind a gyenge áramú hálózat megfelelő hő és tűzvédelmi kialakítására.

11.2.4 Eszközkarbantartás

A Büttner Kft. az informatikai rendszerének kialakításánál törekedett arra, hogy elsősorban helyi eszközökkel valósítsa meg a informatika rendszerét. Ennek megfelelően éves rendszerességgel

minden a szerver oldali eszköz és az azt üzemeltető infrastruktúrát évente egyszer karban kell tartani, bele értve a szünetmentes áramforrásokat és a hűtő fűtő berendezéseket.
A karbantartásokról dokumentált információt kell tárolni a szervezetben.

11.2.5 Eszközök (hw, sw) kivitele a telephelyről

A Büttner Kft. vagyonleltárában szereplő eszközök ki/be szállítását a B2MS rendszerben kell nyilvántartani.
A Büttner Kft. azzal, hogy notebookot, mobiltelefont vagy egyéb hordozható informatikai eszközt ad át a munkavállalói számára, egyidőben hozzájárul az eszközöknek a Büttner Kft. telephelyén kívüli használathoz is.

11.2.6 A telephelyen kívül használt eszközök biztonsági szabályai

A telephelyekről kivitt eszközök használata során bekövetkező károkért (anyagi kár, adatvesztés, adatszivárgás) az a felhasználó viseli a felelősséget, aki az eszközt átvette. A telephelyen kívüli használat során mindazon elvek és gyakorlat követendő, amelyeket az IBSZ egyes fejezetei leírnak, biztosítva az adatok és az eszköz védelmét.

11.2.7 Az eszközök biztonságos megsemmisítése vagy újra hasznosítása

A használt eszközök selejtezése esetén, a selejtezés megkezdéséig az IT vezető feladata gondoskodni az eszközök zárt, biztonságos elhelyezésről.

Az eszköz értékesítése előtt az IT csoport egy tagja - amennyiben lehetséges - visszaállítja a gyári, eredeti állapotot és az összes, szervezet tulajdonát képző, licencköteles terméket eltávolítja az eszközről és aktualizálja az vagyonleltárt.
Az eszköz megsemmisítésekor az eszközben található adathordozót fizikai roncsolással kell megrongálni vagy visszaállíthatatlanságot biztosító technikával törli.

A Büttner Kft. vagyonleltárában szereplő eszközök selejtezését a B2MS rendszerben kell nyomon követni.

11.2.8 A felügyelet nélkül hagyott berendezések és „tiszta asztal” politika

A felhasználóknak biztosítaniuk kell az őrizetlenül hagyott berendezések megfelelő védelmét. Az úgynevezett „tiszta asztal, tiszta képernyő” szabályokat kell alkalmazni. Az iratok és eltávolítható adathordozók tekintetében a „tiszta asztal”, míg az információfeldolgozó eszközök tekintetében a „tiszta képernyő” szabályzatát kell alkalmazni.
A munkakörnyezet felügyelet nélkül hagyása esetén, minden felhasználó köteles az informatikai eszközhöz való hozzáférést megakadályozni, az eszközt (a képernyőt) zárolni, oly módon, hogy a

hozzáférés csak jelszó ismételt megadását követően, vagy egyéb authentikációs módszer alkalmazása után váljon ismét lehetővé.
Az iroda napvégi elhagyásakor a munkaasztalon nyomtatott dokumentumot hagyni TILOS. Minden papír alapú üzleti dokumentumot zárt szekrényben kell elhelyezni.
A „tiszta asztal" politika betartását az Információbiztonsági felelős időszakosan ellenőrizheti.

A Büttner Kft. informatikai rendszereiben olyan rendszerbeállítást kell alkalmazni, amely minden irodai zónában használt informatikai eszközt automatikusan lezár a felhasználó 15 perces inaktivitása után. A gyártási terelteken használt informatikai eszközt esetében az automatikusan lezárást a felhasználó 45 perces inaktivitása után kell alkalmazni.
A beállítások alkalmazásáért az Informatikai vezető a felelős. A beállításokat az Információbiztonsági felelős rendszeresen ellenőrizheti.

12. Üzemeltetés

12.1 Üzemeltetési eljárások és felelősségek

12.1.1 Üzemeltetési eljárások

A Büttner Kft. informatikai rendszerének üzemeltetését a szervezet saját maga végzi a dokumentált üzemeltetési eljárásoknak megfelelően.
Az üzemeltetési eljárásrendet a Büttner Kft. központi szerverén a BSZ15 mappában tárolja. Az üzletmenet-folytonossági elvárásoknak megfelelően egy digitális példányt elérhetővé kell tenni akkor is, ha a Büttner Kft. által használt elsődleges üzemeltetési helyszín átmenetileg vagy folyamatosan nem elérhető.

12.1.2 Változáskezelési eljárások

12.1.2.1 Változtatási kérelmek benyújtása

Változtatási kérelmet (VK) a Büttner Kft. valamennyi felhasználója benyújthat a szervezet által üzemeltett ticketing rendszerben. Az IT üzemeltetési témájú változások véleményezését és jóváhagyását, elfogadását az IT vezető végzi (amennyiben a kérelem megfelel a jelen szabályzatban meghatározott biztonsági követelményeknek). Az elbíráláshoz szükség szerint kikérheti az Információbiztonsági felelős véleményét is.

12.1.3 Kapacitáskezelés

A Büttner Kft. Információbiztonsági felelős rendszeres időközönként, de évente minimum egy alkalommal, a vezetőségi átvizsgálásra való felkészülés alkalmával meg kell tervezze, és felül kell vizsgálja az üzletmenet folyamatos fenntartásához kapcsolódó külső és belső szolgáltatások kapacitásigényét.

A Büttner Kft. az informatikai erőforrások kapacitásának megtervezésekor erős túltervezést alkalmaz, hogy az eszközök és szolgáltatások tervezett életciklusa alatt a megfelelő kapacitás rendelkezésre álljon.

Kapacitáskezelés alá vont területek:

- Szerver tárkapacitás
- Szerver memória, processzor teljesítmény

A kapacitáskezelésről a Büttner Kft. dokumentált információkat tárol a IBIR/BSZ16 mappában.

12.2 Kártékony kódok elleni védelem

Lehetőség szerint minden szerver, valamint minden munkaállomás esetében, ahol a vírusfertőzés kockázata magas, központi menedzsmenttel ellátott védelmi rendszert (antivírus, kémprogram, tűzfal) kell telepíteni. A védelmi rendszerben a vírusadatbázis frissítésének sűrűségét minimálisan napi rendszerességűre kell beállítani.
A vírusvédelmi rendszer paraméterezésénél lehetőség szerint aktiválni kell a tűzfal-beállításokat azokon az eszközökön, ahol nincs külön telepített tűzfalmegoldás. Itt a Windows vagy az Mac OS rendszer beépített tűzfalát kell engedélyezni.
A vírusvédelmi rendszer beállításait az IBIR/BSZ17 mappában kell tárolni.

12.2.1 A vírus incidens kezelése

A vírusvédelmi rendszerben paraméterezni kell, hogy végponti vírus incidens esetén automatikus e-mail-üzenetet küldjön az IT üzemeltetési vezetőnek.
A vírus incidenseket a vírusvédelmi rendszerben naplózni kell, valamint minden esetben ki kell vizsgálni az incidens okát, és szükség esetén módosításokat kell eszközölni a vírusvédelmi rendszer paraméterein.
3 vagy több gépet érintő incidensről értesíteni kell az Információbiztonsági felelőst.

12.3 Biztonsági mentések és visszaállítás

12.3.1 Adatmentés, archiválás

A Büttner Kft. által alkalmazott informatikai rendszerek mentése a BSZ18_Mentési rend alapján kell végrehajtani.
A munkaállomásokon a szervezet adatvagyonát csak kezelni szabad a tárolást minden esetben a szervezet szerverein kell megvalósítani.

12.3.2 Az adatok visszaállítása

A mentésekről évente egyszer adatvisszaállítási tesztet kell végezni. Az adat-visszaállítási tesztekről jegyzőkönyvet kell felvenni és dokumentált információként tárolni kell. Az adat-visszaállítási jegyzőkönyveket a Büttner Kft. IBIR/BSZ19 mappában kell tárolni.
Az adat-visszaállítási tesztek végrehajtásáért az Információbiztonsági felelős a felelős.

12.3.3 Médiakezelés

A Büttner Kft. IT vezetője a felelős azért, hogy minden esetben a gyártói ajánlásoknak megfelelő médiumokat használjanak.
A lejárt szavatosságú adattárolók megsemmisítését jelen szabályzat vonatkozó rendelkezése szerint kell elvégezni.

12.4 Naplózás és megfigyelés, monitorozás

A Büttner Kft. a monitorozási feladatokat az adott rendszer naplózási funkciójával kell megvalósítani.
Az alkalmazott felhő alapú rendszerek mindegyike és saját üzemeltetésű rendszerei rendelkeznek központi felügyeleti rendszerrel.
A nyilvántartást minden vizsgálat alkalmával felül kell vizsgálni és az újonnan bevezetett rendszereket fel kell venni a havi ellenőrzési listába.
A naplózó eszközöket és a naplóinformációkat védeni kell a meghamisítástól és a jogosulatlan hozzáféréstől.
A rendszeradminisztrátori és rendszeroperátori tevékenységeket naplózni kell, a naplókat védeni kell, és rendszeresen át kell vizsgálni.
Az információfeldolgozó rendszerek óráit szinkronizálni kell egyetlen órajelforrással, mint viszonyítási alappal. A rögzített napló fájlokat minimálisan 30 napig de maximum a vonatkozó GDPR rendeletben meghatározott időtartamig szabad tárolni.

12.5 Az operatív szoftverek kontrollja

A Büttner Kft. üzembe állított rendszereire csak kellő körültekintéssel és a Büttner Kft. üzletfolytonosságát figyelembe véve lehetséges szoftvert vagy a felhő rendszerek esetében plug in-t telepíteni, a változáskezelési szabályoknak megfelelően.
Minden felhasználó, aki a munkaállomásán lokális rendszergazdai jogosultsággal rendelkezik tudomásul kell vegye, hogy felelősséggel tartoznak az általuk telepített szoftverek legális felhasználásáért. Egy szoftver kizárólag a következő feltételekkel:

- ha az üzleti környezetben is ingyenes licenccel rendelkezik vagy a Büttner Kft. megvásárolta a megfelelő licencet
- az IT üzemeltetési csoport írásban (email) vagy a ticketing rendszerben létrehozott hibajegyen hozzájárult az szoftver telepítéséhez.

A telepítés megkezdése előtt ellenőrizni kell, hogy az előző mentés sikeresen lefutott-e. Lehetőleg a mentést követő legközelebbi időpontban és munkaidőn kívül kell a telepítést elvégezni.

12.6 Műszaki sérülékenységi menedzsment

A Windows és Mac alapú rendszereket úgy kell konfigurálni, hogy minden internet eléréssel rendelkező eszköz automatikusan letöltse és telepítse a publikált frissítéseket (pl. patchek és fixek letöltése). Az internet eléréssel nem rendelkező eszközök esetében a IT üzemeltetési csoport

negyedévente minimum egy alkalommal megvizsgálja a kiadott frissítéseket és minimálisan a biztonsági besorolású frissítéseket ütemezetten telepíti.

12.6.1 Műszaki sérülékenységi menedzsment

A Büttner Kft. által fejlesztett rendszerek esetében évente minimálisan egy alkalommal sérülékenység vizsgálatot kell végezni. Minden feltárt sérülékenységet a prioritásának megfelelően javítani kell.

13. A kommunikáció biztonsága

13.1 Hálózatvédelmi intézkedések

Az összes hálózati eszköz és a tűzfal konfigurációját a Büttner Kft. központi szerverén a BSZ22_Konfiguracio mentes mappában mentett fájlok tartalmazzák.

Általános beállítások és irányelvek:

- Active Directory (AD) authentikált szolgáltatásokat internetre publikálni nem szabad.
- Az AD szolgáltatásait csak VPN-csatornán keresztül lehet elérni a szervezet hálózatán kívülről

Tűzfalon olyan webszűrés van, ami nem engedi meg:

- A hálózatban csak statikus IP címeket lehet alkalmazni, amennyiben technikai okokból nem lehet megvalósítani, akkor DHCP szervert csak úgy lehet alkalmazni, hogy az adott eszköz MAC cím alapján azonosítani kell a hálózatban.
- Amennyiben lehetséges minden hálózati szegmensben port security védelmet kell alkalmazni.

Tűzfalvédelmi beállítások:

- Csak az engedélyezett felhőszolgáltatások weboldali látogathatók a szervezet belső hálózatából.
- A fájlküldés és fájlfeltöltés csak az engedélyezett weboldalak és felhőszolgáltatások felé megengedett.

13.1.1 Hálózati szegmentálási elvárások

A Büttner Kft. informatikai rendszerében az üzleti igények alapján, szükségesség elve mentén kell megvalósítani a hálózatok szegmentálását. Új hálózat kialakítása a változáskezelési szabályok betartásával történik. A Büttner Kft. által kialakított zónák a tűzfal konfigurációs beállításaiban kerülnek nyilvántartásra és naprakészen tartásra.
Vezeték nélküli hálózati elérés mind az Office hálózathoz, mind a vendégek részére biztosított. A helyi hálózathoz történő távoli (VPN) kialakítani. A megosztott tartalmakhoz való hozzáféréseket rendszeres időközönként felül kell vizsgálni.

13.1.2 A rendszerfájlok biztonsága

A kiszolgáló informatikai rendszerek működését biztosító rendszerfájlokhoz a felhasználók csak olyan mértékben férhetnek hozzá, amit a szolgáltatás használata megkövetel.
A rendszerfájlok védelme, az üzembiztos konfiguráció megőrzése és helyreállíthatóságának biztosításáért a Büttner Kft. Kft IT vezetője a felelős.

13.2 Információátvitel

13.2.1 Kommunikáció a külső partnerekkel

A Büttner Kft. IBIR törzsdokumentumának 7.4 pontjában megfogalmazott elvárásai mellett a következő elvárásokat fogalmazza meg:

a) Minden partnerrel az együttműködés elején meg kell határozni az információbiztonságával kapcsolatos követelményeket.
b) A Titkárság vezető az IBSZ 15.3 pontjában megfogalmazott kritériumok alapján meghatározza a szállítók információbiztonsági besorolását.
c) Az Információbiztonsági felelős a vevők esetében felülvizsgálja, hogy az ISO 27001 elvárásán felül az új partnernek van-e egyedi követelménye.
d) Az Információbiztonsági felelős minimum évente egy alkalommal felülvizsgálja a partnerek részéről a Büttner Kft. felé támasztott információbiztonsági követelményeinek teljesülését.

13.3 Információátvitel

13.3.1 Kommunikáció – Adat átvétel és átadás ügyfelek és parterek részére

A Büttner Kft. a megosztott mappán keresztüli dokumentumcserét részesíti előnyben.

Partner által biztosított mappa esetében:
A partner által biztosított csatornához való hozzáférést biztonságos jelszó széfben kell tárolni, és csak a projektben részt vevő, a partner kiszolgáló kollégák férhetnek hozzá.

A Büttner Kft által biztosított megosztott mappa esetében:
A hozzáférés átadása során a mappa elérését, és a hozzáférési adatokat külön időpontban és lehetőleg külön csatornán kell eljuttatni a partner számára. Amennyiben lehetséges olyan műszaki megoldást kell alkalmazni, hogy a jelszót a első bejelentkezés alkalmával meg kelljen változtatni.

Amennyiben az ügyfél oldalon nem megvalósítható a Büttner Kft. által biztosított mappa használat akkor fel kell hívni az ügyfél figyelmét a publikus csatorna használatának kockázataira.
Amennyiben nem a preferált csatornákon érkezik az adat a vevőtől vagy a partnertől akkor az alábbi biztonsági megoldást kell javasolni a küldő féltől.

a) Email - Tömörítve jelszóval ellátva

b) USB kulcs - Tömörítve jelszóval ellátva vagy titkosított USB drive használatával

13.3.2 Kommunikáció – az alvállalkozói láccal

Amennyiben az üzleti adatot a Büttner Kft-nek tovább kell küldeni egy alvállalkozójának, úgy az vagy az előző pontban meghatározott megosztott mappákkal kell megoldani vagy ha emailen keresztül történik az adatátadás akkor azt minden esetben jelszóval védett formában kell továbbítani a alvállalkozó számára.

13.3.3 Titoktartási megállapodások

A Büttner Kft. minden olyan alkalmazottal és szerződéses partnerrel titoktartási megállapodást köt, aki (amely) Belső használatú vagy titkos biztonsági osztályba tartozó adatokat ismerhet meg, vagy kezel.

A Szolgáltató és fejlesztő partnerek szerződésének információbiztonsági melléklete tartalmazza a titoktartási elvárásokat.

13.3.4 Az elektronikus üzenetküldés követelményei (e-mail)

a) Az elektronikus levelezést biztosító eszközökről, elsősorban a szerverek fizikai és logikai védelméről folyamatosan gondoskodni kell (pl. nyomon kell követni a szoftverfrissítések megjelenését).
b) A Büttner Kft. levelezőrendszere a Büttner Kft. tevékenységéhez NEM kapcsolódó célokra (pl. magán hirdetések kiküldése) nem használható.
c) A Büttner Kft. elektronikus levelezési címjegyzéke a Büttner Kft.-n kívüli személynek, szervezetnek csak az Információbiztonsági felelős engedélyével adható ki.
d) Tilos az elektronikus üzenetek automatikus átirányítása, vagy másolat küldése a Büttner Kft.-n kívüli e-mail címekre (pl. Gmail, Freemail stb.).
e) A Büttner Kft. a munkavállalói számára egyedi engedélyezés alapján lehetőséget biztosít a levelezőrendszer webmail alapú távoli elérésére.

14. Az információs rendszerek beszerzési, fejlesztési követelményei

14.1 Az információs rendszerek biztonsági követelményei

Új rendszerek megvalósítása során a biztonsági követelményeket előzetesen meg kell határozni és az igényhez mellékelni kell.
A már működő rendszerek továbbfejlesztése, módosítása során a biztonsági követelmények nem változtathatók olyan irányba, hogy a rendszer biztonsági szintje csökkenjen.
Az új vagy módosított rendszer tervét az Informatikai vezető fogadja el, szükség esetén konzultál az Információbiztonsági felelőssel-el.

A Büttner Kft. informatikai rendszereiről naprakész topológiát készít és a BSZ_24_Topológia mappában dokumentálja, melyet legalább évente egy alkalommal felül kell vizsgálni. A felülvizsgálatért az Informatikai vezető a felelős.

14.2 Biztonság a fejlesztési és támogatási folyamatokban

A Büttner Kft. amennyiben külsős partnerrel végeztet fejlesztési feladatokat, minden esetben elvárja a szoftverfejlesztési technológiai nemzetközi sztenderdeket és a best practice-k követését. Figyelmet fordít az információbiztonság és a szoftverfejlesztés biztonságának egyensúlyára.
A fejlesztési folyamat során fókuszban tartja, hogy a fejlesztők és a tesztelő/telepítő természetes személyek lehetőleg elkülönüljenek.
A fejlesztések, tesztek, hibajavítások minőségéért a Fejlesztési vezető a felelős.

14.2.1 Szabályozás a biztonságos fejlesztésre

A Büttner Kft. fejlesztései során az agilis SDLC módszertant követi, a fejlesztésre vonatkozó részletes szabályokat a BSZ-34_Buttner_Biztonságos_Szoftverfejlesztesi Utmutato dokumentum tartalmazza.

14.2.2 Rendszerek változásfelügyeleti eljárásai

A Büttner Kft. a szoftverfejlesztések változáskezeléséhez a B2MS rendszerben rögzíti és követi a fejlesztési és hibakezelési feladatokat.

14.2.3 Az alkalmazások műszaki vizsgálata a működtető környezet változásai után

A Büttner Kft saját informatikai rendszereiben végzett változtatások után ellenőrzi az ott futó alkalmazásokat, hogy azok megfelelően működnek-e. A vizsgálatok és tesztek elvégzésért a Fejlesztési vezető a felelős.

14.2.4 Szoftvercsomagok változtatásainak korlátozása

A Büttner Kft. törekszik a rendszereiben és a fejlesztéseiben a változtatásokat optimalizálni és csak a szükséges mennyiségű szoftvercsomagot felhasználni vagy saját fejlesztésű rendszereinél kiadni.

14.2.5 Biztonságos rendszerek tervezési elvei

A Büttner Kft. a belső igényeket mentén fejleszti az informatikai és szoftver rendszereit a szoftver rendszerek fejlesztése során a BSZ-34_Buttner_Biztonságos_Szoftverfejlesztesi Utmutato dokumentum tartalmazza. Az egyéb informatikai rendszerek fejlesztése során figyelembe kell vennie sz ISO 27001 elvárásait és az Iparági sztenderdeket.

14.2.6 Biztonságos fejlesztési környezet

A Büttner Kft. informatikai rendszerében a fejlesztési feladatok megvalósításához külön fejlesztési környezetet kell megvalósítani. A fejlesztői környezeten felül a szoftverfejlesztéshez a szoftverkódot külön erre a feladatra optimalizált kódtárban kell tarolni. A fejlesztő feladata a fejlesztő rendszerben a kód alkalmazáshoz szükséges szintű dokumentálás (kommentelése). A fejlesztési környezet hozzáférési jogosultságainál minden esetben figyelembe kell venni a feladatkörök szétválasztásának elvárásait.

14.2.7 Kiszervezett fejlesztés

A Büttner Kft. alvállalkozók bevonása esetén a jelen szabályzatban meghatározott információbiztonsági, fejlesztési és változáskezelési elvárásokat meg kell követelje az alvállalkozótól.

14.2.8 A rendszer biztonsági tesztelése

A Büttner Kft. minden saját fejlesztésű rendszer esetén egyedi biztonsági tesztelési projekt lépést vezet be a kiadási folyamatba. Projektenként a megrendelő elvárásának megfelelően ettől eltérő biztonsági tesztelési folyamatok is alkalmazhatók.
A biztonsági tesztelés lépést a szervezet által alkalmazott projekt vezetési rendszerben dokumentálni kell.

A Büttner Kft. az éles környezeten évente minimálisan egy alkalommal biztonsági sérülékenységre utaló tesztet kell végrehajtáson.
A vizsgálat minimálisan a következő területekre kell, hogy kiterjedjen:

- Az éles környeztet védő tűzfal valamit a DMZ terület nyitott port vizsgálata mely során vizsgálandó, hogy szükség van-e a nyitott port további nyitvatartására.

14.2.9 A rendszer elfogadási tesztelése

A Büttner Kft. a verzió kiadásai során a miden kiadott verziót a fejlesztőnek a saját fejlesztési környezetében tesztelnie kell. A tesztelésről a B2MS rendszerben dokumentált információkat kell tarolni.
A fejlesztői tesztelést követően a fejlesztők a B2MS rendszerben kiosztják a tesztelési feladatokat a változásban érintett területek kollégái számára. A tesztelésben részt vevők a feladatban meghatározott idő intervallumon belül kötelesek a tesztelést elvégezni és visszajelzést küldeni a fejlesztőnek.
Amennyiben az összes tesztelő elfogadja a verziót és ismert biztonsági és funkcionális tesztelést követően az egyes programverziók elfogadási tesztelését az ügyfél vagy az ügyfél képviseletében az account menedzser végezi.

14.3 A tesztadatok védelme

A teszt rendszerben létre kell hozni az éles rendszer adat tömegének egy részleges nem teljes másolatát oly módon, hogy a benne szereplő személyes és cég specifikus adatok ne legyenek azonosíthatók. Új funkció kialakításakor minden esetben meg kell vizsgálni, hogy szükséges-e a teszt rendszerben előre teszt adatot generálni, vagy a tesztelés során létrejövő adatok elégségesek leszenek a tesztelések lebonyolításához. A tesztadatok menedzselésért, kialakításáért és anonimizálásáért a Fejlesztési vezető a felelős.

15. Szállítói kapcsolatok

15.1 A külső felekhez, partnerekhez kapcsolódó kockázatok azonosítása

A Büttner Kft. a szállító partnerekhez kapcsolódó kockázatok kezelését a partnerek minősítésével valósítja meg. A partnerekkel kötendő szerződések megkötésének folyamata közben a kell a partnereket minősíteni.

15.1.1 Külső felhasználókkal kapcsolatos információbiztonsági feladatok

Bármilyen rendszer esetében az első telepítés időszakán kívül, a partner hozzáférését eseti jelleggel az Ügyvezető engedélyezi.
Az igénylésnek tartalmaznia kell a külső felhasználó adatait, a hozzáférés indokát, módját, paramétereit és tervezett időtartamát. Engedély nélküli hozzáférés esetén az adott informatikai rendszer nem minősül IBSZ megfelelőnek.

15.2 Harmadik féllel kötött megállapodások biztonsági kérdései

Minden harmadik féllel kötött megállapodás esetén a megállapodásban rögzíteni kell az információbiztonsági kérdéseket és hivatkozni kell a jelen szabályzatban foglaltakra.

A jelen szabályzat kiadása előtt megkötött és még aktív megállapodások esetén a harmadik fél egyoldalú nyilatkozatban fogadja el a rá vonatkozó információbiztonsági elvárásokat.

15.3 Biztonsági előírások harmadik féllel kötött megállapodásokhoz

A Büttner Kft. a harmadik féllel történő együttműködések információbiztonsági követelményeit az alábbi csoportokra nézve határozza meg:

- Egyetemes szolgáltató, kereskedelmi Partnerre vonatkozó információbiztonsági elvárások
- Alvállalkozó – beszállító partner információbiztonsági elvárások
- Tanácsadó, IT szolgáltató vagy üzleti adatot feldolgozó partner vagy szoftverfejlesztő információbiztonsági elvárások

Minden csoporthoz egyedi információbiztonsági követelményrendszer került meghatározásra, a követelményeket a Büttner Kft. központi szerverén a BSZ25 mappa tartalmazza

A partnerrel a szerződés előkészítésének fázisában közölni kell az információbiztonsági követelményeket.
Az Információbiztonsági felelős az egy éven túli szerződési idővel rendelkező partnereket évente egyszer felülvizsgálja és értékeli az információbiztonsági követelmények teljesülését, és szükség esetén változtatási javaslatokat tesz.

15.4 Szállítói értékelés

A Tanácsadó, IT szolgáltató vagy üzleti adatot feldolgozó partner vagy szoftverfejlesztő kategóriába tartozó partnereket az Információbiztonsági felelős évente egyszer felülvizsgálja és a partnerekkel együtt értékeli a partnerek szerződésben vállalt kötelezettségeinek (SLA) teljesülését, szükség esetén változtatási javaslatokat tesz.
Az értékelésről dokumentált információkat kell tárolni a BSZ27 mappában.

16. Incidens- és problémakezelés

16.1 Információbiztonsági események jelentése

Az olyan események bekövetkeztekor, mikor a Büttner Kft. digitális adatvagyonának vagy az általa kezelt ügyfél adatvagyon bizalmassága, sértetlensége és rendelkezésre állása közvetlen veszélyben van, haladéktalanul értesíteni kell az Információbiztonsági felelőst az ibf@buttner.hu e-mail címen, annak akadályoztatása esetén az Ügyvezetőt.
Ilyen esetekben, a digitális adatvagyon védelme érdekében a Büttner Kft. informatikai szolgáltatásainak szintjét átmenetileg a kivizsgálás és a hibaelhárítás idejére korlátozható.
Minden olyan nem tervezett eseményt rögzíteni kell, amely a Büttner Kft. által használt adatokat kezelő alkalmazások rendelkezésre állására, az adatok bizalmasságára vagy integritására hatással volt.

Minden egyes incidens esetén fel kell jegyezni:

- az incidens észlelésének pontos időpontját,
- az incidens pontos leírását,
- az incidens megoldásáért felelős nevét,

Valamennyi incidens jegyzőkönyvben rögzíteni kell továbbá:

- az incidens elhárítása érdekében tett valamennyi erőfeszítést,
- az incidenshez kapcsolódó valamennyi végfelhasználói visszajelzést.

16.2 Probléma kezelés

Amennyiben egy incidens előfordulási gyakorisága vagy a szervezet folyamatira gyakorolt hatása nagy, illetve felmerül a felelősség kérdése is, úgy az Információbiztonsági felelős problémafeltárási

vizsgálatot rendelhet el. A vizsgálat folyamatáról és eredményéről jegyzőkönyvet kell készíteni. A jegyzőkönyvnek tartalmazni kell az probléma megelőzése érdekében javasolt intézkedéseket.

Minden egyes probléma esetén fel kell jegyezni:

- a kapcsolódó incidens vagy incidensek észlelésének pontos időpontjait,
- az incidensek pontos leírását,
- az incidensek elhárítása érdekében tett valamennyi erőfeszítést,
- az incidensekhez kapcsolódó valamennyi végfelhasználói visszajelzést.
- a probléma feltárt okát, ami az incidensekhez vezetett
- a javasolt megelőző lépéseket
- az Információbiztonsági felelős döntését
- az esetlegesen feljegyzett ismert hibát

16.3 Információbiztonsági gyengeségek jelentése

A szolgáltatások felhasználása közben tapasztalt biztonsági gyengeségek jelentése a ibf@buttner.hu címen történik - a rendszer működőképességének fenntarthatósága érdekében -, ami minden felhasználónak kötelessége. Ennek elmulasztása vagy a gyengeség kihasználása információbiztonsági eseménynek minősül.

17. A működésfolytonosság biztosítása

17.1 A működésfolytonosság információbiztonsági vetülete

A Büttner Kft. számára fontos a szerződésben vállalt szolgáltatásainak folyamatos, szerződés szerinti megvalósítása. Ennek érdekében az üzletfolytonossági elvárások mentén Üzletmenet folytonossági tervet készít és tart napra készen, valamin a Katasztrófa elhárítási tervek készít és dokumentál a Büttner Kft. központi szerverén, ami a BSZ29 könyvtárban található. A DRP tervet évente egy alkalommal felül kell vizsgálni.

A vészhelyzeti tervek felülvizsgálata az Információbiztonsági felelős feladata.

18. Megfelelőség

18.1.1 A jogszabályi megfelelőség

A Büttner Kft. Ügyvezetőjének felelőssége a biztonsági politikának, a szabványoknak, a műszaki előírásoknak, továbbá a mindenkori jogszabályoknak való megfelelőség biztosítása a nyújtott szolgáltatások vonatkozásában.
Az Ügyvezető értelemszerűen nem felel a felhasználók által elkövetett jogsértésekért (pl. jogosulatlan adatkezelés, szerzői jogokkal való visszaélés stb.), és hatósági megkeresés esetén a jogszabályban előírt adatokat az adott felhasználóval kapcsolatban kiadhatja.

18.1.2 Az alkalmazandó jogszabályok, követelmények gyűjteménye

a) 2011. évi CXII. tv. az információs önrendelkezési jogról és az információszabadságról.
b) 2012. évi I. tv. A munka törvénykönyvéről.
c) 1999. évi LXXVI. tv. a szerzői jogról.
d) 2005. évi CXXXIII. Törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól
e) EU 2016/679 számú Általános Adatvédelmi Rendelete

a) MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények.
b) ISO 27005 - Information technology — Security techniques — Information security risk management.
c) ISO 31000 - Risk management.

18.1.3 A szellemi jogok védelme

Az Ügyvezető felelőssége a szervezeten belül a szellemi tulajdonjogok és a szoftvertermékek tulajdonjogának védelme.
Tilos a Büttner Kft. infrastruktúrájában bármely illegális szoftver használata vagy azok visszafejtése.
A Büttner Kft. fejlesztésre szerződött munkavállalói és partnerei a Büttner Kft. megbízásából vagy érdekkörében fejlesztett szoftverkódhoz kapcsolódó értékesítési és felhasználási jogát minden esetben átruházzák a Büttner Kft-re a szerzői jogát minden fejlesztő a szoftverkód alkalmazásáig vagy létezéséig megtartja.

Az alkalmazottak és teljesítésben résztvevő partnerek által a munkaviszony vagy szerződéses jogviszony ideje alatt létrehozott dokumentumok, szabályzatok, feljegyzések nyilvántartás minták (továbbiakban Szabályzat) a Büttner Kft. szellemi tulajdona.
A felhasználók jogosultak a Szabályzatokat a Büttner Kft. megbízásából az ügyfelek számára átdolgozni, módosítani.
A felhasználók azonban nem jogosultak a Szabályzatokat terjeszteni, a nyilvánosság számára közvetíteni többszörözni, saját célra felhasználni, harmadik személy részére megismerhetővé tenni és tovább értékesíteni.

18.1.4 A feljegyzések védelme

A Büttner Kft. bármely üzleti folyamata szempontjából releváns feljegyzést meg kell őrizni, ideértve a megbeszélések jegyzőkönyveit és a csoportmunka eredményét is.
A feljegyzések kiemelt bizalmasságának következtében a Büttner Kft. kiemelt figyelmet fordít a belső dokumentumkezelési feladatokra. Minden felhasználónak kiemelt figyelmet kell fordítania a dokumentumok jelölésére, verziókezelésére és a már nem használt verziók selejtezésére.

18.1.5 Személyhez köthető információk védelme

A Büttner Kft. rendszerein és eszközein létrehozott vagy tárolt információk a Büttner Kft.-hez, mint jogi személyhez kötöttek. A Büttner Kft. vállalja, hogy az alkalmazottai vagy bármely szerződött partner által a rendszereiben kezelt - nem a Büttner Kft. tevékenységéhez köthető - adatot harmadik fél számára nem adja ki, és a lehető leggyorsabban rendelkezik az adat dokumentált megsemmisítéséről.
A Büttner Kft. magára nézve kötelező érvényűnek tekinti a EU GDPR rendeletét és a kapcsolódó magyar törtvényeket és rendeleteket. Ennek megfelelően kialakította és rendszeresen felülvizsgálj az adatkezelési szabályzatát és kapcsolódó nyilvántartásokat.

18.2 Az információs rendszerek felülvizsgálatával kapcsolatos megfontolások

Az Információbiztonsági felelős a számonkérhető azért, hogy az IT-rendszerek teljes körű belső biztonsági felülvizsgálata dokumentált módon legalább évente megtörténjen. Súlyos rendelkezésre állási probléma vagy sérülés esetén az Ügyvezető külön rendkívüli biztonsági ellenőrzést és felülvizsgálatot rendelhet el.
A felülvizsgálatok eredményei alapján az Ügyvezető rendeli el javító, helyesbítő és megelőző intézkedéseket, melyeket mindig a soron következő belső vagy külső, harmadik fél általi felülvizsgálat során kell dokumentált módon visszaellenőrizni.

18.2.1 Az információbiztonság független felülvizsgálata

A Büttner Kft. Információbiztonsági felelőse a számonkérhető a belső információbiztonsági audit elvégzéséért. Erre a feladatra a Büttner Kft. külső szolgáltatót vehet igénybe.

Budapest, 2023.06.01

dr. Büttner Tamás Antal ügyvezető
ügyvezető