CSABACAST KFT.

Megnevezés:

Információbiztonsági Szabályzat

Készítette: Szűcs Attila

Ellenőrizte: **Boronkay László**

2.1. Személyi hatálya

Jelen Szabályzat mindenkire nézve kötelező, aki használja a Cég számítógép-hálózatát, annak berendezéseit (a továbbiakban: felhasználók). Az előbbieknek megfelelően a Szabályzat személyi hatálya kiterjed a Cég összes munkavállalójára, aki a Cég számítógép-hálózatát és eszközeit használja. Ha a Cég harmadik félnek is lehetőséget biztosít hálózatának használatára, akkor a harmadik fél is köteles a Szabályzatban foglaltakat betartani.

2.2. Tárgyi hatálya

A Szabályzat tárgyi hatálya kiterjed:

- a védelmet élvező elektronikus adatok teljes körére, felmerülésüktől és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájától függetlenül,
- a Cég által bármely jogcímen használt valamennyi informatikai berendezésre,
- valamint az informatikai eszközök műszaki dokumentációira,
- az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- a rendszer- és felhasználói programokra,
- az adatok felhasználására vonatkozó utasításokra,
- az adathordozók tárolására, felhasználására.

3.1. Jogszabályi háttér

- Magyarország Alaptörvénye
- az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV.tv.
- 2013. évi V. törvény a Polgári Törvénykönyvről
- a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról szóló 2006. évi V. törvény és kapcsolódó végrehajtási rendeletei
- a szerzői jogról szóló 1999. évi LXXVI. törvény és kapcsolódó végrehajtási rendeletei
- 1959. évi IV. törvény (régi Ptk.) és kapcsolódó végrehajtási rendeletei (2014.03.15. előtti jogügyletek esetén)
- a polgári perrendtartásról szóló 2016. évi CXXX. törvény és kapcsolódó végrehajtási rendeletei
- a munka törvénykönyvéről szóló 2012. évi I. törvény és kapcsolódó végrehajtási rendeletei
- 1993. évi XCIII. törvény a munkavédelemről
- a fogyasztóvédelemről szóló 1997. évi CLV.tv.
- 1997. évi XI. törvény a védjegyek és a földrajzi árujelzők oltalmáról
- a közérdekű adatok elektronikus közzétételére, az egységes köz-adatkereső rendszerre, valamint a központi jegyzék adattartalmára, az adatintegrációra vonatkozó részletes szabályokról szóló 305/2005. (XII.25.) Korm. rendelet
- az elektronikus kereskedelmi szolgáltatások, valamint információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- a közbeszerzésekről szóló 2015. évi CXLIII. törvény és kapcsolódó végrehajtási rendeletei
- 276/2014. (XI.6.) Korm. rendelet a minősített adatot, az ország alapvető biztonsági, nemzetbiztonsági érdekeit érintő vagy a különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 218/2011. (X. 19.) Korm. rendelet hatályon kívül helyezéséről, valamint az ezzel összefüggő átmeneti rendelkezésről
- 2016. évi XXX.tv. a védelmi és biztonsági célú beszerzésekről
- a kutatás-fejlesztésről és a technológiai innovációról szóló 2014. évi LXXVI. törvény
- 2010. évi CLVII. törvény a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről
- 2009. évi CLV. törvény a minősített adat védelméről
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról
- 1995. évi CXIX tv. A kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcímadatok kezeléséről
- 2012. évi C. tv. a büntető törvénykönyvről
- a kis- és középvállalkozások helyzetével, támogatásával összefüggő adatszolgáltatásról szóló 5/2009.

4. A felülvizsgálat (revízió) időpontja és a Szabályzat változásmenedzsmentje

4.1. A Szabályzat karbantartása

A Szabályzatot az informatikában – valamint a Cégnél – a fejlesztések során bekövetkező változások miatt időközönként, szükségszerűen aktualizálni kell.

A Szabályzat felülvizsgálatára az alábbiak szerint kerül sor:

- évente egy alkalommal (az esedékes következő felülvizsgálati időpontot a dokumentum lezárásakor kell kijelölni.)
- minden olyan esetben, amikor a szabályzatban leírtakban jelentős változás(ok) történnek.
- a tervezett változásokat a verziószám tizedesének növelésével jelöljük, éves felülvizsgálatot követően a verziószám egy egész jeggyel emelkedik.

A felülvizsgálat a belső szabályozó dokumentumok elkészítésének, módosításának helyben kialakított, külön eljárási rendje szerint történik.

4.2. A Szabályzat alkalmazásának módja

A Szabályzat megismerését az érintett munkavállalók részére a vezetők oktatás formájában biztosítják.

A Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni a Szabályzat előírásainak megfelelően.

Az Információbiztonsági Politika célja, hogy a Cég szervezeti egységei részére egységes és általános értelmezést adjon az informatikai rendszerekben kezelt adatok bizalmassága, hitelessége, sértetlensége, rendelkezésre állása és funkcionalitásainak biztosítása érdekében követendő irányelvekre. Az irányelvek figyelembevételével meghatározható az információbiztonsági szabályozás alapján minősített adatokat kezelő informatikai rendszerek biztonsági osztályba sorolása; kidolgozhatóak a konkrét, rendszer szintű információbiztonsági szabályozások, amelyek az informatikai rendszer teljes életciklusában meghatározzák a szabványos biztonsági funkciók tervezéséhez, megvalósításához, üzemeltetéséhez és megszüntetéséhez szükséges alapelveket és követelményeket.

5.1. Az Információbiztonsági Politika elfogadása és közzététele

Az Információbiztonsági Politikát a Szabályzat részeként kezeljük, ezért elfogadása és közzététele a Szabályzattal megegyező módon történik, azaz az üzemeltetési felelős előterjesztése alapján az ügyvezető fogadja el. A jelen Szabályzat mellékletét képező Információbiztonsági Politika kifüggesztve is megtekinthető.

5.2. Az Információbiztonsági Politika rendszeres felülvizsgálata

Az Információbiztonsági Politika a Szabályzat szerves része, és azzal egy időben és azonos módon történik a felülvizsgálata:

- évente egy alkalommal (az esedékes következő felülvizsgálati időpontot a dokumentum lezárásakor kell kijelölni),
- minden olyan esetben, amikor a politikában leírtakban jelentős változás(ok) történnek.

1. A Cég igyekszik a kockázatot minimalizálni, de minden munkavállalóban tudatosítja, hogy teljes körű védelem és biztonság nincsen, és ezzel összefüggésben a maradvány kockázatokat tudatosan vállalja.
2. A Cég a felelősségeket az információbiztonság területén hangsúlyozottan elhatárolja, és az egyes szervezeti szerepkörökhöz köti.
3. A Cég hangsúlyozottan törekszik a törvényi és jogszabályi megfelelőségre, különös tekintettel a személyes adatok kiemelt védelmére. A Cég az alapvető jogok biztosának ez irányú állásfoglalásait figyelembe veszi.
4. A Cég megpróbálja kiegyensúlyozottan kezelni a mobilitás lehetősége és a biztonság közötti ellentmondást.
5. Elsődleges cél a működőképesség fenntartása, ezért az olyan felhasználókat, akik magatartásukkal más felhasználók tömegeinek munkáját veszélyeztetik, a Cég haladéktalanul kizár a szolgáltatásból mindaddig, amíg a veszélyt okozó tevékenységüket meg nem szüntetik.
6. A védelem mellett a Cég biztosítja az oktatási és kutatási tevékenységhez szükséges szabad információáramlást.
7. A felhasználói jogosultságok természetes személyhez kötöttek és nem átruházhatóak. Az információbiztonsági incidensek esetében a felelősség a jogosultsággal bíró személyhez kötődik. A Cég rosszhiszemű felhasználásnak tekinti, ha a felhasználó jogosultságát meghaladó műveleteket szándékosan kezdeményez, illetve jogosultságát megkísérli módosítani.
8. Elérendő cél, hogy a szolgáltató rendszerek üzemzavarait ne a felhasználók, hanem automatikus szolgáltatásmonitorozó komponensek jelezzék.

6.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatok és információk osztályozása jelentőségük és bizalmassági fokozatuk alapján az alábbiak szerint történik:

- közlésre szánt, bárki által megismerhető adatok,
- minősített, pénzügyi, számviteli, munka- és bérügyi titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek az adat védelme az érdekkörébe tartozik.

Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt munkavállalók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

Alapelv, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.

A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést, vagy annak a kísérletét a Cég ügyvezetőjének jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért az informatikai vezetők és a rendszergazdák felelősek.

Az adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás – során az operációs rendszerben és a felhasználói programban alkalmazott logikai, matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

6.4.3. Az informatikai vezető jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet a Cég ügyvezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthet valamennyi iratba, amely az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

7.4. Az információbiztonsági felelősségek allokációja

Azon informatikai rendszerek esetében, amelyeknek nem volt sikeres a Szabályzatnak való megfelelőségi vizsgálata, minden negatív biztonsági esemény felelőssége az üzemeltető szervezeti egység vezetőjét terheli.

Azon rendszerek esetében, ahol megfelelőségi vizsgálat sikeres volt, illetőleg a vizsgálat során készült és elfogadott hiánylistát az üzemeltető pótolta, a negatív biztonsági események felelőssége egyedi vizsgálat alapján állapítható meg. A Szabályzat betartása esetén az üzemeltető jóhiszeműnek minősül.

Az ügyvezető felelőssége az információbiztonsági eseményeknek, az incidensek tanulságainak és a pozitív példáknak a megjelenítése a cég szokásos információs csatornáin.

7.5. Új információ-feldolgozó rendszerek elfogadási eljárása

Új informatikai szolgáltatás indítási kérelemhez csatolni kell a rendszer vázlatos leírását és a tervezett SLA-t. Ezen anyagok alapján az ügyvezető a szolgáltatás engedélyezése előtt javaslatot kérhet az üzemeltetési felelőstől a Szabályzat mellékleteinek aktualizálására, az új szolgáltatás Szabályzat szerinti paramétereinek megállapítására.

7.6. Bizalmassági nyilatkozatok

Az információbiztonsági szabályok betartásával és betartatásával kapcsolatban titoktartási nyilatkozatot írnak alá a rendszerek üzemeltetői, illetve a felhasználók is abban az esetben, amennyiben erről az adott rendszer SLA-ja külön rendelkezik.

A rendszer üzemletetői a rendszer üzemeltetése során különféle személyes, illetőleg bizalmas adatokhoz férnek hozzá. Ezen adatok védelméről gondoskodni kell.

A munkavégzés során a munkavégzők részére átadott, illetve tudomásukra jutott információkat védeni kell.

Minden bizalmassági kérdésben érintett szereplővel nyilatkozatot kell kitöltetni, melynek aláírásával felvállalja, hogy a birtokában levő információval nem él vissza.

7.7. Kapcsolattartás hatóságokkal

A különböző törvényekben és rendeletekben előírt információbiztonsági adatszolgáltatási kötelezettség teljesítése az ügyvezető felelőssége. A Cég jogi képviseletet nem lát el az egyének jogvitáiban a hatóságokkal szemben.

7.8. Kapcsolattartás különleges érdekközösségekkel

Az ügyvezető felelős a különleges érdekközösségekkel történő kapcsolattartásért.

Minden hivatalos tagsági és kapcsolattartási kérdésben a Cég érdekeinek figyelembevételével az ügyvezető dönt.

A felhasználók egyéni tagsága az adott személy felelőssége. Egyéni tagként is köteles a kapcsolattartás során a Szabályzat rá vonatkozó előírásait betartani.

8. Az információs vagyon menedzsmentje

8.1. Felelősség az információs vagyonért

8.1.1. Információs vagyonleltár

Az információs vagyon az üzemetetési dokumentációkban leírtak alapján meghatározott.

A Cég A, B és C kategóriájú rendszereinek nyilvántartását és az általuk biztosított szolgáltatások paramétereinek nyilvántartását az Informatika végzi. Az ehhez szükséges adatszolgáltatás a rendszerek üzemeltetőinek Szabályzatból fakadó kötelezettsége.

A szoftvereket és adathordozókat az Eszközök és források leltárkészítési és leltározási szabályzatában foglaltaknak megfelelően kell leltározni.

8.1.2. Az információs vagyon tulajdonjoga

A Cég A, B és C kategóriájú rendszereinek cég-specifikus konfigurációs adatai és beállításai (minden olyan konfigurációs komponens, amely a vásárolt rendszerben található állapottól eltér) a Cég tulajdonát képezik. Ugyanezen rendszerekben tárolt minden céges adat a Cég tulajdonát képezi. Ezen adatok felhasználási joga kizárólag a Céget illeti meg.

8.1.3. Az információs vagyon használatának szabályai

Minden munkavállaló és üzleti partner a számára meghatározott jogosultsággal léphet be a különböző rendszerekbe. A jogosultság változását a munkavállalók esetében a felettesnél, üzleti partner esetében a megbízó szervezeti egység vezetőjénél kell kezdeményezni.

Az SLA-k rögzítik az egyes szolgáltatásokkal kapcsolatos információs vagyon, valamint jogosultságkezelési és használati szabályokat. Mindenfajta változtatás az SLA-k változtatási rendjének megfelelően végezhető.

Adatok kiadása a különböző biztonsági osztályba sorolt rendszerekből csak az adott szervezeti egység vezetőjének engedélyével lehetséges, kivételt ez alól az az eset képez, amikor az adatcserét, adatátadást jogszabály vagy szerződés rögzíti. Ebben az esetben a szerződésnek tartalmaznia kell az adatkezelésre vonatkozó szabályokat.

- Olyan információk, amelyekre semmilyen korlátozás nem vonatkozik, és amelyeket például a vállalat újságokban vagy az interneten közzétehet.
- A vállalati információk nyilvános felhasználásához a felelős egység jóváhagyása szükséges. Példák: sajtóközlemények, termékkatalógus az ügyfelek számára

2) Belső:

- Ezen információk jogosulatlan ismerete, megosztása vagy felhasználása csak kis mértékben befolyásolja a termék vagy projekt célkitűzéseinek elérését. Ezért ez az információ hozzáférhetővé tehető a jogosult személyek csoportja számára.
- A titoktartás elvesztése kisebb, bár kisebb következményekkel járhat; például:
    - valószínűtlen az egyes személyek vagy szervezetek kártérítési igénye

3) Bizalmas

Azok az információk, amelyek ismerete vagy illetéktelen személyek számára történő nyilvánosságra hozatala veszélyeztetheti a termék és a projekt célkitűzéseinek elérését, ezért csak engedélyezett személyek korlátozott csoportja számára szabad hozzáférhetővé tenni.

A titoktartás elvesztése esetén a következmények valószínűek és mérhetőek, pl.:

- az ügyfelek elvesztése
- az értékesítési adatok / forgalom visszaesése
- egyes személyek vagy szervezetek kártérítési igényei

Példák: személyes adatok, amelyek meghaladják az üzleti kommunikációs adatok (pl. Fizetés) költségvetési terveket, felülvizsgálati jelentések

4) Titkos

Azok az információk, amelyek ismerete vagy illetéktelen személyek számára történő nyilvánosságra hozatala súlyosan veszélyeztetheti a vállalat céljainak elérését, ezért erősen korlátozó terjesztési listára és szigorú ellenőrzésre szorul.

A titoktartás megsértése jelentős hatással van a vállalat arculatára / megjelenésére és / vagy gazdasági következményekre, pl.:

- az ügyfelek jelentős vesztesége
- az értékesítési adatok / forgalom hirtelen csökkenése
- kártérítési igények számos személy vagy szervezet részéről
- kizárás bizonyos piacokról

8.2.6. Információk címkézése és kezelése

1) Nyilvános:

- Címkézés: opcionális, feltéve, hogy az információ
- Sokszorosítás és terjesztés: nincs korlátozás
- Tárolás: nincs korlátozás
- Törlés: nincs korlátozás
- Eltávolítás: nincs korlátozás

2) Belső:

- Címkézés nincs, vagy a dokumentum belső oldalán
- Sokszorosítás és terjesztés: csak a csoport felhatalmazott alkalmazottai és a feladat- vagy alkalmazási területen belül felhatalmazott harmadik felek számára.
- Tárolás: védelem az illetéktelen hozzáférés ellen
- Törlés: a már nem szükséges adatokat törölni kell

3) Bizalmas

- Címkézés: A dokumentum minden oldalán elektronikus és nyomtatott formában
- Sokszorosítás és terjesztés: Az információt terjesztő személy felelős a megfelelő terjesztési útvonalak használatáért, annak érdekében, hogy az információkat és és adatokat megvédje a jogosulatlan hozzáféréstől és/vagy a jogosulatlan lehallgatásról (pl. titkosítás)
- Tárolás: csak a csoport felhatalmazott alkalmazottainak és a feladat- és alkalmazási területen belül felhatalmazott harmadik feleknek korlátozott köre számára hozzáférhető (pl. zárt felhasználói csoportok által).
- A bizalmas dokumentumokat zárt acélbútorokban, vagy olyan helyiségekben kell tárolni, amelyek használaton kívül zárva vannak, és amelyeket csak korlátozott számú személy nyithat ki.
- Törlés: a már nem szükséges adatokat törölni kell
- Eltávolítás: megfelelő ártalmatlanítás
- Hitelesítés: erős hitelesítés

10.1. Biztonsági zónák, területek

10.1.1. Fizikai biztonsági határvédelem

A, B kategóriájú szolgáltató-rendszer kritikus fizikai komponensei (szerver, tároló alrendszer, router… stb.) csak külön erre a célra kialakított, megfelelő biztonsági paraméterekkel rendelkező helyiségekben működtethetők. A helyiségeknek mechanikai nyitórendszerrel (biztonsági zár vagy beléptető kártyával működtethető mágneses zár) és beléptető rendszerrel kell rendelkezniük. A beléptető rendszer szükséges alapfunkciói: belépő személy azonosítása kód vagy kártya alapján, belépési jogosultság megállapítása, belépési időpont regisztrálása, jogosulatlan belépés jelzése a biztonsági személyzet felé.

A C kategóriájú rendszerek esetében minimálisan biztonsági zárral ellátott helyiséget kell biztosítani.

10.2. Fizikai belépési szabályozás

Az A és B kategóriájú rendszerek komponenseit tartalmazó szolgáltató helyiségekbe (géptermek, kábelrendezők) való belépési jogosultságot az ügyvezető, C kategóriájú rendszer esetében az üzemeltető szervezeti egység vezetője engedélyezi a munkavállalónak vagy a partnernek a helyiségek és a végezhető tevékenységek felsorolásával.

A belépési lehetőséggel rendelkezők ezen jogosultságukat nem ruházhatják át másik munkavállalóra vagy partnerre.

Jogosulatlan személy beengedéséből fakadó eseményekért a felelősség a beengedő személyt terheli. Az illegálisan szerzett belépési lehetőség használata betörésnek minősül és jogi következményeket von maga után.

10.3. Irodák, szobák és egyéb létesítmények fizikai biztonsága

Az informatikai rendszerek működtetéséhez szükséges egyéb munkaterületek használatának módja megegyezik az általános területek használati módjával. Kitüntetett hozzáférést vagy védett adatokat tartalmazó kiegészítő rendszerkomponensek (mentési berendezés, fejlesztői rendszer, felügyelő terminál, stb.) csak beléptető rendszerrel védett munkaszobában és irodában helyezhetőek el.

Az informatikai célú helyiségekkel kapcsolatos kérdésekben az üzemeltetési felelős a felelős a ki- és az átalakítás koordinációjáért, a szakmai a biztonsági szempontok betartásáért.

Kiemelt fontosságú helyiség a szerverszoba, mely használatának szabályait az ebben a témakörben irányadó szabályok részletezik.

10.4. Külső és környezeti károk elleni védelem

A, B és C kategóriájú szolgáltató-rendszer kritikus fizikai komponensei csak a hatályos szabályozásnak megfelelő tűz- és villámvédelmi rendszerrel felszerelt helyiségekben üzemeltethetők. Talajszinten, vagy az alatt elhelyezkedő helyiségek esetében az ár- és belvízvédelmi szabályozásnak is meg kell felelni.

Egyedi esetben az ügyvezető egyéb előírásokat is megfogalmazhat.

A tűzvédelmi rendelkezéseknek megfelelően az erősáramú ellátó rendszernek tartalmaznia kell olyan központi áramtalanítókapcsolót, amely tűzjelzés esetén a biztonságos oltás feltételeit megteremti.

15. A központi számítógép és a hálózat információbiztonsági követelményei

15.1. Központi gépek

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén az adatvesztéstől.

A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni.

Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

15.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.

Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.

Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

A Cég informatikai eszközeiről programot, illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, ezen elemeket mindennemű sérüléstől meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

A felhasználónak minden esetben vissza kell igazolnia új jelszavának átvételét ellenőrizhető úton (pl.: e-mailben vagy személyesen).

A jelszónak minden felhasználó számára szabadon megváltoztathatónak kell lennie.

A felhasználói jelszavakkal kapcsolatban – amennyiben az adott rendszerben erre lehetőség van – biztosítani kell a következő követelmények teljesülését:

- Az alkalmazottak nem generálhatnak azonos jelszavakat üzleti és nem üzleti célokra
- Az alkalmazottak nem generálhatnak azonos jelszavakat a külső csoport által biztosított rendszerek és rendszerek számára, amelyeket harmadik felek biztosítanak, pl. g az interneten (alkalmazások, regisztrációs szolgáltatások, …)
- A felhasználóknak be kell tartaniuk a rendszer által előírt minimális jelszóhosszt. Ezeket a jelszó irányelv határozza meg.
- Nem szabad egyszerű jelszavakat (pl. „Test123456”, „123456abcde”) vagy kontextus-specifikus szavakat (pl. Személyes témák, például név, születési dátum) használni.
- Ha bizonyos rendszerek vagy alkalmazások nagyobb jelszó-összetettséget igényelnek (a jelszó-irányelvben meghatározottak szerint), akkor a kényszerített összetettséget kell használni.

A felhasználói azonosítók és jelszavak nem tárolhatóak rejtjelezetlen formában. Felhasználói azonosítók, jelszavak, kriptográfiai kulcsok és az ehhez tartozó jelszavak nyomtatott formában, lezárt, lepecsételt borítékban, lemezszekrényben tárolhatóak. A lezárt borítékot a lezárónak alá kell írni, a lezárás dátumának feltüntetésével.

Biztosítani kell, hogy a felhasználók tényleges hozzáférési jogosultsága munkakörüknek megfelelő legyen.

Az Informatika vezetője a rendszergazdák, a Munkaügyi Csoport és az alkalmazásgazdák bevonásával a jogosultságokat rendszeres időközönként ellenőrzi. Az általános felhasználók esetében ezt évente, míg a kiemelt jogosultsággal rendelkező felhasználók esetében legalább 3 havonta kell megtenni. Rendszeresen ellenőrizni kell azt is, hogy privilegizált jogokkal csak egyedileg azonosítható felhasználók, csoportok és eszközök rendelkezhessenek.

A munkakörök változásakor a hozzáférési jogosultságokat felül kell vizsgálni, és az új munkakörnek megfelelően módosítani kell. A munkakörök változásáról a munkahelyi vezetők és a Munkaügyi Csoport köteles értesíteni az Informatikát.

Több faktoros azonosítást a Cég nem használ.

17.2.3. A felhasználó feladatai

Meg kell akadályozni az illetéktelen felhasználói hozzáférést az informatikai rendszer erőforrásaihoz. A biztonság hatékonyságához nélkülözhetetlen az engedéllyel rendelkező felhasználók együttműködése.

A felhasználóknak tudomással kell bírniuk a hozzáférés hatékony ellenőrzésére alkalmas eszközök használatáról, különös tekintettel a jelszavak használatára és a felhasználó kezelésében lévő berendezések biztonságára.

A jelszavakat bizalmasan kell kezelni, azok más személyeknek nem adhatók meg, nyilvánosságra nem hozhatók.

A jelszavakat nem szabad papíron tárolni. Amennyiben ez elkerülhetetlen (pl.: a kezdeti jelszó), akkor

kártérítési igényeket támaszthat.

A vállalatra vonatkozó előírásokat be kell tartani.

A licencszoftvert csak a megállapodás szerinti célra szabad felhasználni, kizárólag a meglévő rendelkezéseknek és a gyártóval kötött licencszerződéseknek megfelelően.

21.5. Adatvédelem

Az adatvédelemre vonatkozó nemzeti törvényeket és előírásokat be kell tartani.

A vállalkozókat a beszállító cég vezetésének köteleznie kell arra, hogy teljesítse az adatvédelemre vonatkozó jogszabályi követelményeket.

21.6. A szerződéses megfelelés

A Szállító informatikai szervezetének meg kell felelnie a megrendelő szerződéses követelményeinek. Intézkedéseket kell végrehajtani annak biztosítására, hogy a beszállítók saját szervezeti szabályzatait felülvizsgálják és frissítsék a jelenlegi szerződéses követelményeknek megfelelően.

21.7. Irányelvek és szabályzatok

A szállítónak politikákat és szabályozásokat kell biztosítania alkalmazottai számára, hogy biztosítsák a követelményeknek való megfelelést, valamint a megrendelő fél információinak, hardvereinek és szoftvereinek megfelelő kezelését.

Harmadik fél biztonsági kockázatértékelési kérdőíve

CONFIDENTIAL

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	CSABAcast Megjegyzések/Kérdések	Harmadik fél válasza a CSABAcast 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.	Nem			
2	Van e a szervezeténél olyan személy aki az információbiztonsági feladatokkal foglalkozik?	Nem			
3	Végeznek e háttérellenőrzést azon alkalmazottaik részére, akik hozzáférhetnek az adatainkhoz és kezelik azokat?	Nem			
4	Van e a szervezetének írásos információbiztonsági szabályzata?	Nem			
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.	Nem			
5	Rendelkezik e a szervezete írásos jelszó házirenddel, amely részletezi a jelszavak szükséges szerkezetét?	Nem			
6	Minden személy részt vesz információbiztonsági képzésen?	Nem			
	Általános biztonság				
7	Van e telepítve antivírus szoftver a szervezete szerverein?	Nem			
8	Van e telepítve antivírus szoftver a szervezete munkaállomásain?	Nem			
9	A rendszer- és biztonsági javításokat rutinszerűen alkalmazzák e a munkaállomásokra?	Nem			
10	Használnak-e SPAM szűrő szervert- szoftvert?	Nem			
11	A rendszer- és biztonsági javításokat tesztelik e az éles környezetben való bevezetés előtt?	Nem			
12	Rendelkeznek e az alkalmazottak egyedi bejelentkezési azonosítóval az adatok eléréséhez?	Nem			
13	Rendelkezik -e a szervezete biztonsági intézkedésekkel az adatvédelem érdekében?	Nem			
13,1	Ha igen, kérjük, írja le a megjegyzések rovatban	Nem			
14	Korlátozzák-e a hozzáférést érzékeny adatokat tartalmazó rendszerekhez?	Nem			
14,1	Ha igen, milyen szabályozások vannak jelenleg a hozzáférés korlátozására?	Nem			
15	Korlátozott e az adatfeldolgozó berendezéseikhez (szerverekhez és hálózati eszközökhöz) való fizikai hozzáférés?	Nem			
16	Létezik -e folyamat az informatikai eszközök és adathordozók biztonságos ártalmatlanítására?	Nem			
16,1	Ha igen, kérjük, írja le a megjegyzések rovatban	Nem			
	Hálózatbiztonság				
17	A hálózat határait védi e tűzfal?	Nem			
18	Rendszeresen végeznek e hálózati sebezhetőségi vizsgálatot?	Nem			
19	Behatolásjelző rendszereket (IDS) vagy a behatolásmegelőző rendszereket (IPS) használ e a szervezete?	Nem			
19,1	Ha igen, kérjük, írja le a megjegyzések rovatban	Nem			
20	Kötelesek e az alkalmazottak VPN-t használni, amikor a szervezet rendszereit távoli helyről szeretnék elérni?	Nem			
21	Engedélyezett a vezeték nélküli hozzáférés a szervezetén belül?	Nem			
21,1	Ha igen, kérjük, írja le a megjegyzés rovatban, hogyan védett?	Nem			
	Rendszerbiztonság				
22	A számítógépes rendszerek (kiszolgálók) biztonsági mentése rendszeres ütemterv szerint történik?	Nem			
23	Ellenőrzik a biztonsági mentési és helyreállítási folyamatokat?	Nem			
24	A szervezete tárol biztonsági mentéseket a szervet telephelyin kívül?	Nem			

25	Titkosítja a szervezete a biztonsági mentéseit?	Nem			
26	A szervezeténél van kiszervezett adattárolás?	Nem			
26,1	Ha igen, kinek adják ki az adatokat?	Nem			
27	Szabályozva van a rendszergazdai jogosultságokhoz való hozzáférés?	Nem			
28	A kiszolgálók úgy vannak konfigurálva, hogy rögzítsék, ki férhet hozzá a rendszerhez, és milyen változtatásokat hajtottak végre?	Nem			
28,1	Ha nem, akkor biztonsági rés esetén hogyan határozza meg, hogy ki fért hozzá a rendszerhez, és milyen változtatásokat hajtott végre?	Nem			
29	Az érzékeny adatok megfelelően védettek és az adatkommunikáció titkosítva van? Például támogatja a szoftver az SSL titkosítást?	Nem			
	Üzletfolytonosság / katasztrófa utáni helyreállítás				
30	Van -e a szervezetének katasztrófa utáni helyreállítási terve az adatfeldolgozó létesítményekkel kapcsolatban?	Nem			
30,1	Van -e a szervezetének üzleti folytonossági terve?	Nem			
31	A számítógéptermek védettek e tűz és árvíz ellen?	Nem			
32	Van e a szervezetének "forró" helyreállítási helyszine?	Nem			
	Az incidensre adott válasz				
33	Ha a GDPR adatait érintő információbiztonsági jogsértés történt, értesítik a NAIH -t a jogsértésről?	Nem			
33,1	Ha igen, mennyi idő múlva értesítik a NAIH -t?	Nem			
34	Rendelkezik -e a szervezete hivatalos incidens-elhárítási tervvel?	Nem			
35	Tapasztalt -e a szervezete információ biztonsági megsértést az elmúlt három -öt évben?	Nem			
35,1	Ha igen, kérjük, dokumentálja, milyen információk vesztek el a megjegyzések rovatban?	Nem			
35,2	Ha igen, kérjük, dokumentálja a megjegyzések rovatban, hogyan és milyen gyorsan értesítették az ügyfeleket.	Nem			
	Külső tárhelyszolgáltatás / harmadik fél				
36	Fogja e adatainkat tárhelyszolgáltatónál tárolni?	Nem			
36,1	Ha igen, kérjük, adja meg a tárhelyszolgáltatás nevét, és hogy ISO27001 tanúsítvánnyal rendelkeznek e?	Nem			
37	Kérjük, sorolja fel azokat a harmadik feleket, amelyeket az Ön vállalkozása használ az adataink és tanúsítványaik tárolására.	Nem			
38	Rendszeresen felülvizsgálja a harmadik feleket, akik hozzáférnek az adatainkhoz? Milyen gyakran?	Nem			