**Rendszerbiztonsági igényspecifikáció**

{TÖRLENDŐ\_RÉSZ} **Sablon** {TÖRLENDŐ\_RÉSZ\_VÉGE}

**<Érintett alkalmazás neve (Rövidítése)>**

**<n.m> verzió**

Készült: <év>. <hónap>. <nap>.

**Készítette:**

# Dokumentum kontroll

## Dokumentum jellemzők

|  |  |
| --- | --- |
| Projekt hivatalos neve: | <Projekt hivatalos neve> |
| Projekt rövid neve | <projekt rövid neve> |
| Dokumentum címe: | <Projekt hivatalos neve> – <Alcím> – <Érintett alkalmazás neve (Rövidítése)> |
| Verziószám: | <n.m> |
| Állapot: |  |
| Kiadás kelte: | <0000>. <00. 00.> |
| Utolsó mentés kelte: | <0000>. <00. 00.> |
| Készítette: |  |
| Fájlnév: | <FileName> |

## Jóváhagyások

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Név | Szervezeti egység | Szervezet | Dátum | Aláírás |
| <XY> |  | <IdomSoft Zrt.> | <0000>. <00. 00.> |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Változtatások jegyzéke

|  |  |  |
| --- | --- | --- |
| Verzió | Dátum | Változtatás rövid leírása |
| <1.0> | <0000>. <00. 00.> | <Első verzió> |
|  |  |  |
|  |  |  |

## Kapcsolódó dokumentumok

|  |  |
| --- | --- |
| Dokumentum címe | Dokumentum helye /fájl neve |
|  |  |
|  |  |

Tartalomjegyzék

[1 Dokumentum kontroll 2](#_Toc180070449)

[1.1 Dokumentum jellemzők 2](#_Toc180070450)

[1.2 Jóváhagyások 2](#_Toc180070451)

[1.3 Változtatások jegyzéke 2](#_Toc180070452)

[1.4 Kapcsolódó dokumentumok 2](#_Toc180070453)

[2 Cél- és hatáskör 8](#_Toc180070454)

[3 Fogalmak és rövidítések 8](#_Toc180070455)

[4 Rendszer biztonsági áttekintése 9](#_Toc180070456)

[4.1 Rendszer biztonsági besorolása 9](#_Toc180070457)

[4.2 Jogszabályi háttér 9](#_Toc180070458)

[4.3 Szabályozói környezet 10](#_Toc180070459)

[4.4 Rendszerre vonatkozó fenyegetések azonosítása 10](#_Toc180070460)

[4.5 Biztonsági feltételezések 11](#_Toc180070461)

[4.6 Biztonsági szabályok áttekintése 11](#_Toc180070462)

[5 Követelmények jegyzéke 12](#_Toc180070463)

{TÖRLENDŐ\_RÉSZ}

**Informatív leírás**

Ezen sablon annak érdekében került kiadásra, hogy segítséget nyújtson az egységes Rendszerbiztonsági igényspecifikáció dokumentumok létrehozásában. Az Informatív leírás fejezet általános információkat fogalmaz meg, mely nem eleme a sablon alapján kialakításra kerülő Rendszerbiztonsági igényspecifikáció dokumentumnak. Az elkészítés során törölni kell a fájlból minden további, a kitöltést segítő magyarázó résszel együtt.

**Dokumentum célja**

A dokumentum meghatározza azokat a fejlesztendő rendszerrel szemben támasztott biztonsági követelményeket, amelyeket a biztonsági funkciók tervezéséhez kell felhasználni. Ez a dokumentum részletezi a biztonsági igények meghatározását, de nem tartalmazza a megoldás részleteit.

Az igénymeghatározáshoz az alábbi szempontok meghatározása szükséges:

* a rendszer biztonsági tervezését befolyásoló fenyegetések azonosítása,
* a rendszerbiztonsági szabályainak megfogalmazása, ezen belül a rendszerbiztonsági-és szervezeti biztonsági szabályok azonosítása,
* a Rendszer működési környezetére vonatkozó biztonsági feltételezések megfogalmazása.

A biztonsági problémameghatározással párhuzamosan el kell végezni a rendszer előzetes besorolását az Ibtv. (2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról) szerinti biztonsági osztályba. Az Ibtv. a fejlesztésre vonatkozóan számos kontrollterületre fogalmaz meg elvárást, amelyek kihatással vannak a kialakítandó rendszer architektúrájára, a beépítendő biztonsági funkciókra.

A biztonsági problémameghatározás és a rendszer (Ibtv. szerinti) biztonsági osztály együttesen képezik a rendszer biztonsági követelményeinek az alapját. A biztonsági igényspecifikáció ezen követelmények meghatározásával ér véget.

Mivel a dokumentum a fejlesztés korai szakaszában készül el, az nem részletezi a biztonsági funkciók működését, azonban szükséges, hogy a biztonsággal érintett területeket kijelölje, valamint meghatározza a biztonsági funkciók tervezési irányait.

A rendszerbiztonsági igényspecifikáció összességében egy elemző, megalapozó dokumentumnak tekinthető, aminek elolvasása segít megérteni, a biztonsági követelmények értelmét, illetve azok helyét és szerepét a rendszert használó szervezet életében.

Az igényspecifikáció az elvárások, szabályozások elemzését, feldolgozását elvégzi, és egységes formában prezentálja az összes teljesítendő követelményt.

**Dokumentumnak nem célja**

Mivel a dokumentum a fejlesztés korai szakaszában készül el, az nem részletezi a biztonsági funkciók működését. A dokumentum nem részletezi a biztonsági funkciók megtervezését, ahogyan azt sem, hogy azok hogyan teljesítik a biztonsági célokat.

**Felhasználói kör**

A rendszerbiztonsági igényspecifikáció az alábbi felhasználói kör számára készül:

| Felhasználói kör | Felhasználás módja |
| --- | --- |
| Üzemeltetés, vezető | Üzemeltetési biztonsági követelmények teljeskörűsége  Az üzemeltetési környezetre vonatkozó feltételezéseket teljesíthetősége |
| Biztonsági architekt | A rendszer fejlesztésével kapcsolatos elvárások teljeskörűen rögzítésre kerültek  Szervezetben meghatározott technikai biztonsági követelmények teljeskörűsége  Fejlesztésre vonatkozó biztonsági követelmények teljessége |
| Biztonsági felelős | A szervezeti biztonsági szabályokból megfogalmazott feltételezések helyessége  A szervezet kockázatarányos védelme szerint releváns fenyegetéseket a projekt azonosította  Rendszer által teljesítendő biztonsági szabályok teljeskörűsége  Biztonsági követelmények teljeskörűsége  Jogszabályi követelményekből levezethető biztonsági követelmények teljeskörűsége |

**Felhasznált dokumentumok**

* Ajánlattételi felhívás műszaki követelményei
* Igazgatási koncepció

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Cél- és hatáskör

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: a rendszerbiztonsági igényspecifikáció célja és hatásköre.

Az fejezet tartalmi elvárásai: azonosítsa a rendszerbiztonsági igényspecifikáció célját, vagyis a biztonsági követelmények hatáskörét.

A rendszerbiztonsági igények túlmutathatnak a fejlesztett rendszer határain és magában foglalhatják:

* a Szállító által biztosított dobozos termékek integrációját,
* a Megrendelő szervezet által biztosított szolgáltatásokkal való integrációt.

A projekt méretétől és az előzőekben megfogalmazott nem funkcionális követelmények részletességétől függően a rendszerbiztonsági igényspecifikáció hatókörébe tartozhat:

* minden, a fejlesztendő rendszer bizalmasságával, sértetlenségével vagy rendelkezésre állásával kapcsolatos, nem funkcionális követelmény azonosítása. Például:
  + katasztrófatűrési képességek,
  + válaszidők,
  + adatmegőrzésre vonatkozó elvárások,
* a szervezeti, működési feltételezések azonosítása, melyek egyaránt vonatkozhatnak technológiai elemekre vagy szervezeti működési rendekre.

A dokumentum a biztonsági tervezés kezdeti dokumentuma, ezért az itt megfogalmazott követelményeket a fejlesztés előrehaladásával felül kell vizsgálni a lefedettség érdekében.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Fogalmak és rövidítések

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: ismerteti a rendszerbiztonsági igényspecifikációban használt fogalmakat és rövidítéseket.

Az alfejezet tartalmi elvárásai: bontsa alá a fogalmakat és azok magyarázatát megengedett struktúrában (fogalmak, rövidítések). Itt kell bevezetni a dokumentumban használt általános jelöléseket is.

Az alfejezett formai elvárásai: fogalmak és magyarázatuk táblázatban, betűrendben.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Rendszer biztonsági áttekintése

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: ismerteti az alkalmazás biztonsági jellemzőit.

A fejezet tartalmi elvárásai: ismertesse azt a működési, üzemeltetési, szervezeti környezetet, amiben a rendszer el lesz helyezve. A fejezet tartalmazza a követelmények tételes felsorolása előtt áttekintő, értelmező magyarázatokat is.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Rendszer biztonsági besorolása

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: a rendszer kezdeti **Ibtv.** szerinti biztonsági besorolása.

Az alfejezet tartalmi elvárásai: biztonság alapján sorolja be a bizalmasság, sértetlenség és rendelkezésre állás szempontokat az Ibtv. szerinti 5 fokozatú skálán. A besorolást bemutatni és indokolni kell az **Osztályba sorolás és védelmi intézkedés űrlapon (OVI tábla)** megadott szempontok szerint.

A biztonsági osztály azért számít kezdetinek, mert a fejlesztés ezen szakaszában még nem történik meg a rendszer minden lényeges komponensének azonosítása. Előfordulhat, hogy a biztonsági tervezés során a fejlesztendő rendszer egyes komponensei alacsonyabb besorolást kapnak.

Az alfejezett formai elvárásai: az indoklás célszerűen követi az OVI tábla osztályba sorolás lapjának szempontjait és az ott rögzített szempontok szerint magyarázza a biztonsági osztályt. Amennyiben a Megrendelő már az előkészítési szakaszban elvégezte a besorolást, elegendő, ha a fejezet rögzíti a biztonsági osztályt.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Jogszabályi háttér

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: a biztonsági követelmények szempontjából fontos jogszabályok azonosítása.

Az alfejezet tartalmi elvárásai: csak a teljes igazgatási jogszabályi listának részhalmaza lehet és nem ismételheti meg az igazgatási koncepcióban és általában az igazgatási folyamatokat meghatározó jogszabályokat. A fejezet tartalmazhat egyéb, rendszerbiztonsági szempontból fontos jogszabályt is.

Fontos még, hogy a fejezet a jogszabályokon túl ismertesse röviden (a konkrét jogszabályi helyekre mutató hivatkozással) az azokban szereplő követelményeket. Ez alól kivétel az **Ibtv** követelmények ilyen típusú bemutatása.

Az alfejezett formai elvárásai: jogszabályok felsorolása, az egyes jogszabályok biztonsági követelményeinek rövid összefoglalása, majd az abból levezetett követelmények alábontása.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Szabályozói környezet

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: a Megrendelő szervezetben érvényes biztonsági követelmények azonosítása.

Az alfejezet tartalmi elvárásai: emelje ki a szabályozási rendszerből levezetett konkrét követelményeket, a fejlesztendő rendszerre releváns módon. Például: ha a belső szabályozási rendszer előírja, hogy a hálózati kapcsolatokat még a szerverzónában is titkosítani kell, akkor a fejezet vagy ismertesse ezt, vagy írja elő, hogy hogy a belső PKI rendszer által kiadott tanúsítványokat minden adatkapcsolat titkosítására használni kell.

Az alfejezett formai elvárásai: fontos belső szabályozások felsorolása, az egyes jogszabályok biztonsági követelményeinek rövid szöveges összefoglalása, majd az abból levezetett követelmények alábontása.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Rendszerre vonatkozó fenyegetések azonosítása

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: a rendszert fenyegető aktorok (fenyegetések) azonosítása.

Az alfejezet tartalmi elvárásai: azonosítsa a fenyegetéseket. A fenyegetések azonosításához az alábbi információkra van szükség:

* a fenyegetés neve,
* a fenyegetést rendszerre gyakorolt hatása,
* a fenyegetés képességei (hogyan tudja a fenyegetést kifejteni).

Amennyiben a rendszer bonyolultsága nem indokolja, a fenyegetések részletes azonosításától el lehet tekinteni. Erre elsősorban a következő esetben van mód:

* egyszerűbb rendszerek,
* 4-nél alacsonyabb biztonsági osztályú rendszerek.

A fenyegetések meghatározása a rendszer védelmének pontosabb megértéséhez, valamint a biztonsági funkciók tervezéséhez szükséges. A fejezetben kifejthető pl.: a belső támadó, az esetlegesen rendszert használó kiemelt ügyintéző, vagy internetes bűnöző.

Az alfejezett formai elvárásai: a fenyegetések listája a fejezetben megadott tartalommal.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Biztonsági feltételezések

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: a rendszer adminisztratív, technológiai környezetére vonatkozó feltételezések.

Az alfejezet tartalmi elvárásai: a rendszerfejlesztés ebben a szakaszában feltételezésként lehet rögzíteni azon elvárásokat, amik a rendszerfejlesztés hatáskörén kívül esnek, de a rendszer működéséhez szükségesek. Külső feltételnek számít minden olyan körülmény, információ, eljárási szabály, amelyeket a rendszer környezetének kell biztosítani. A fejezet tartalmazza ennek a kezdeti felmérését. A rendszertervezés előrehaladásával a biztonsági feltételezések rendszere fokozatosan bővülhet, ahogy a részletek kibontása megtörténik.

Példa biztonsági feltételezések:

* a rendszer környezetében rendelkezésre áll egy központi naplóelemző rendszer,
* az alkalmazás számára tartalék helyszín biztosított,
* a kapcsolódó rendszer irányából érkező adatok nem manipuláltak.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Biztonsági szabályok áttekintése

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: a szervezet biztonsági szabályainak áttekintése.

Az alfejezet tartalmi elvárásai: a szervezet biztonsági szabályai azon szervezeti és technológiai szabályok összessége, amelyek a fenyegetések és feltételezések ismeretében támogatják a rendszer biztonságos működését.  
A fejezet legyen egy informatív leírás, ami segíti a követelményjegyzék értelmezését. A biztonsági szabályok közé elsősorban a rendszer és használóinak viszonyát befolyásoló szabályok tartoznak (pl. jogosultságkezelés, naplózás, üzemeltetés). A szabályok kiterjedhetnek a követelményeknél megadott területekre is. A biztonsági szabályok elsősorban a Megrendelő szervezetébe helyezi a rendszert.

Az alfejezett formai elvárásai: Szabad szöveges leírás.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Követelmények jegyzéke

{TÖRLENDŐ\_RÉSZ}

Az fejezet célja: a rendszer biztonsági követelményeinek felsorolása.

Az fejezet tartalmi elvárásai: sorolja fel a követelményeket, opcionálisan strukturálisan alábontva. A biztonsági követelmények egy lehetséges csoportosítása:

* Authentikáció követelményei,
* Authorizáció követelményei,
* Rendszerintegrációs követelmények,
* Igénybe vett külső biztonsági szolgáltatások,
* Kártékony kód védelem,
* Titkosításra vonatkozó elvárások,
* Integritásvédelemre vonatkozó elvárások,
* Üzemeltetési követelmények,
* Hálózati védelem elvárásai,
* Kriptográfiai algoritmusokra vonatkozó követelmények,
* Felhasználói felületre vonatkozó követelmények,
* Biztonsági naplózás követelményei,
* Anonimizálás követelményei,
* Rendszer élesítésére, változáskezelésére vonatkozó követelmények,
* Konfigurációkezelésre vonatkozó követelmények,
* Alkalmazásfejlesztésre vonatkozó követelmények.

A fejezet pontosan írja le a követelményeket, vagyis kerülje az általánosító, nyílt végű elvárásokat („feleljen meg X és Y jogszabálynak"). A leírás legyen olyan részletességű, hogy azt egy informatikus szakember képes legyen végrehajtani.

Az alfejezett formai elvárásai: táblázat, tartalma az egyes területek szerint strukturális alábontásban sorfolytonos, egyedi sorszámmal ellátott lista.

{TÖRLENDŐ\_RÉSZ\_VÉGE}