**Rendszerbiztonsági terv**

{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](#_Toc185239754)

[1.1 Dokumentum jellemzők 2](#_Toc185239755)

[1.2 Jóváhagyások 2](#_Toc185239756)

[1.3 Változtatások jegyzéke 2](#_Toc185239757)

[1.4 Kapcsolódó dokumentumok 2](#_Toc185239758)

[2 A dokumentum célja és hatóköre 8](#_Toc185239759)

[2.1 Fogalmak és rövidítések definíciója 8](#_Toc185239760)

[3 Biztonsági követelmények 8](#_Toc185239761)

[3.1 Vonatkozó <X.> biztonsági szintű elvárások 8](#_Toc185239762)

[3.2 Tervezési szempontok, megkötések 9](#_Toc185239763)

[4 Az architektúra biztonsági szempontból 9](#_Toc185239764)

[4.1 Infrastruktúra 9](#_Toc185239765)

[4.2 Platform 10](#_Toc185239766)

[4.3 Platform rendszerkomponensek 10](#_Toc185239767)

[4.4 Megfelelés a biztonsági elvárásoknak 10](#_Toc185239768)

[5 Adatok védelme 11](#_Toc185239769)

[5.1 Alkalmazás adatok 11](#_Toc185239770)

[5.2 Infrastruktúra adatok 11](#_Toc185239771)

[6 Operációs rendszerek 11](#_Toc185239772)

[6.1 Authentikáció és jogosultság kezelés 11](#_Toc185239773)

[6.2 Felhasználói fiókok, szerepkörök és jogosultságok 12](#_Toc185239774)

[6.3 Helyi és központi naplózás 12](#_Toc185239775)

[6.4 Menedzsment lehetőségek/megoldások 12](#_Toc185239776)

[6.5 Kommunikációs kapcsolatok védelme 13](#_Toc185239777)

[6.6 Egyéb rendszerkomponens specifikus biztonsági funkcionalitások 13](#_Toc185239778)

[7 Címtár és DNS szolgáltatás 13](#_Toc185239779)

[7.1 Authentikáció és jogosultság kezelés 13](#_Toc185239780)

[7.2 Felhasználói fiókok, szerepkörök és jogosultságok 14](#_Toc185239781)

[7.3 Helyi és központi naplózás 14](#_Toc185239782)

[7.4 Menedzsment lehetőségek/megoldások 14](#_Toc185239783)

[7.5 Kommunikációs kapcsolatok védelme 14](#_Toc185239784)

[7.6 Egyéb rendszerkomponens specifikus biztonsági funkcionalitások 14](#_Toc185239785)

[8 Monitoring rendszer 14](#_Toc185239786)

[8.1 Authentikáció és jogosultság kezelés 15](#_Toc185239787)

[8.2 Szerepkörök és jogosultságok 15](#_Toc185239788)

[8.3 Helyi és központi naplózás 15](#_Toc185239789)

[8.4 Menedzsment lehetőségek/megoldások 15](#_Toc185239790)

[8.5 Kommunikációs kapcsolatok védelme 15](#_Toc185239791)

[8.6 Egyéb rendszerkomponens specifikus biztonsági funkcionalitások 15](#_Toc185239792)

Ábrajegyzék

**Nincs ábrajegyzék-bejegyzés.**

{TÖRLENDŐ\_RÉSZ}

**Informatív leírás**

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

**A dokumentum célja**

A rendszerbiztonsági terv (RBT) meghatározza az Állami Alkalmazásfejlesztési Központ (ÁAFK) kezelésének hatókörébe tartozó — belső és külső — alkalmazásfejlesztő csapatok/projektek számára az információbiztonsági szempontokat előíró és részletező kereteket és peremfeltételeket.

**Dokumentumnak nem célja**

Az RBT-nek nem célja az adott alkalmazás környezetén túlmutató, ahhoz kapcsolódó háttérrendszerek információbiztonsági szempontjainak vizsgálata — kivételt képeznek az interfészek, amelyek a dokumentum hatókörébe tartoznak.

**Felhasználói körök**

A migrációs terv az alábbi felhasználói kör számára készül (az alkalmazást szállító kivételével):

|  |  |
| --- | --- |
| **Felhasználói kör** | **Felhasználás módja** |
| Alkalmazáskörnyezet szállító | Az alkalmazással kapcsolatos információbiztonsági megoldások és elvárásoknak megfelelés dokumentálása. |
| Megrendelő oldali informatikai szakterületek | Az alkalmazás illesztését megelőzően az információbiztonsági kontrollok ellenőrzése.A kapcsolódó háttérrendszerek információbiztonsággal kapcsolatos követelményeinek megfogalmazása és ellenőrzése. |
| Megrendelő oldali alkalmazás- és infrastruktúra üzemeltetés | Az alkalmazás környezet üzemeltetéséhez szükséges IBIR kompetenciák kialakítása, különös tekintettel az információbiztonsági kontrollok ellenőrzésére, kézbentartására. |
| Központi alkalmazás-szolgáltató | Az ÁAFK információbiztonsági követelményeknek való megfelelés ellenőrzése során. |

**Felhasznált dokumentumok**

* Útmutató az Állami Alkalmazás-Fejlesztési Környezet dokumentációs sablonjaihoz

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# A dokumentum célja és hatóköre

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: bemutatja a dokumentum célját és hatókörét.

A fejezet tartalmi elvárása:

* határozza meg a kapcsolódó alapkövetelményeket,
* rögzítse ezen követelmények fejezeteit,
* segítse rövid tartalommal az egyes fejezetekhez kapcsolódó elvárások körvonalazását.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Fogalmak és rövidítések definíciója

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: bemutatja az RBT-ben használt fogalmakat és rövidítéseket.

Az alfejezet tartalmi elvárásai:

* alábontja vagy egységesen kezeli a fogalmakat és azok magyarázatát megengedett struktúrában (fogalmak, rövidítések),
* bevezeti a dokumentumban alkalmazott általános jelöléseket.

Az alfejezet formai elvárása: fogalmak és magyarázatuk táblázatban, betűrendben.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Biztonsági követelmények

## Vonatkozó <X.> biztonsági szintű elvárások

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: bemutatja a biztonsági besorolást és a kapcsolódó kontrollokat.

Az alfejezet tartalmi elvárása: sorolja fel a biztonsági osztálynak megfelelő adminisztratív, logikai és fizikai elvárásokat.

Az alfejezet formai elvárása: táblázat kategóriánként.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Tervezési szempontok, megkötések

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: bemutatja a biztonsági besorolást.

Az alfejezet tartalmi elvárása: ismertesse az ÁAFK-ban fejlesztett alkalmazás környezet biztonsági tervezése és kialakítása során figyelembe vett biztonsági szempontokat, kötöttségeket és adottságokat.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Az architektúra biztonsági szempontból

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: ismerteti az architektúrát és kijelöli a biztonsági szempontokat.

A fejezet tartalmi elvárása: ismertesse az alkalmazás környezetét hardver-és szoftver komponensből felépülő architektúráját, beleértve:

* fizikai infrastruktúrát,
* logikai környezetet,
* rétegek részletezését.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Infrastruktúra

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: ismerteti az infrastruktúrát és kijelöli a biztonsági szempontokat.

Az alfejezet tartalmi elvárása:

* részletezze az infrastruktúrát, amely tartalmazza:
	+ a szervereket,
	+ a virtualizációs szolgáltatásokat,
	+ az adattárolást;
* részletezze a fizikai infrastruktúrát kiegészítő terheléselosztási és tűzfal funkciókat biztosító hardverelemeket,
* részletezze az infrastruktúra elemeket összekapcsoló hálózat fizikai kialakítását.

Az alfejezet formai elvárása: ábra és szöveges magyarázat.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Platform

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: ismerteti a platformot.

Az alfejezet tartalmi elvárása, hogy részletezze:

* tűzfal zónákat,
* VLAN-okat,
* terheléselosztást és funkciókat,
* logikai topológiát.

Az alfejezet formai elvárása: ábra és szöveges magyarázat.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Platform rendszerkomponensek

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: ismerteti a platform rendszerkomponenseit.

Az alfejezet tartalmi elvárása: részletezze a rendszerkomponenseket legalább az alábbiak ismertetésével:

* Alkalmazott operációs rendszerek,
* Active Directory (AD),
* Nagios.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Megfelelés a biztonsági elvárásoknak

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: összerendeli a platform rendszerkomponenseket a biztonsági elvárásokkal.

Az alfejezet tartalmi elvárása: ismertesse, hogy a rendszerkomponensek esetében hogyan teljesülnek a 3. pontban megfogalmazott biztonsági követelmények.

Az alfejezet formai elvárása: táblázat.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Adatok védelme

## Alkalmazás adatok

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: részletezi az alkalmazás adatokat és azok tárolását.

Az alfejezet tartalmi elvárása, hogy részletezze:

* az alkalmazás adatok tárolásának megvalósítását,
* az alkalmazás adatok alapján meghatározható adatköröket.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Infrastruktúra adatok

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: részletezi az infrastruktúra adatokat és azok tárolását.

Az alfejezet tartalmi elvárása, hogy részletezze:

* az infrastruktúra adatok tárolásának megvalósítását,
* az infrastruktúra adatok alapján meghatározható adatköröket.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Operációs rendszerek

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: ismerteti a használt operációs rendszereket.

A fejezet tartalmi elvárásai:

* részletezze az összes operációs rendszerre vonatkozóan szükséges, az alfejezetekben meghatározott információbiztonsági szempontokat,
* ha több operációs rendszert használ adott alkalmazás, a fejezetet annyiszor szükséges megismételni.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Authentikáció és jogosultság kezelés

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: részletezi az authentikációt és a jogosultságkezelést.

Az alfejezet tartalmi elvárásai, hogy minimum ismertesse:

* az alkalmazott authentikációs megoldás(oka)t,
* felhasználói fiókok kezelését,
* jogosultságok kezelését.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Felhasználói fiókok, szerepkörök és jogosultságok

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: ismerteti a felhasználói fiókokat, szerepköröket és jogosultságokat.

Az alfejezet tartalmi elvárása: ismertesse a szerepkör mátrixot legalább az alábbiakkal:

* létrehozott fiókok,
* fiókhoz tartozó szerepkör,
* fiókhoz tartozó jogosultság.

Az alfejezet formai elvárása: táblázat.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Helyi és központi naplózás

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: részletezi a helyi és központi naplózást.

Az alfejezet tartalmi elvárása: részletezze az egyes rendszerkomponensek esetében:

* a helyi, illetve a távoli naplózás módját és helyét,
* a naplózandó információk típusát.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Menedzsment lehetőségek/megoldások

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: részletezi a menedzsment lehetőségeket.

Az alfejezet tartalmi elvárásai:

* az adott rendszerkomponens menedzsment biztosításának módját — interfész, protokoll, stb.,
* az adott rendszerkomponenshez való hozzáférés korlátozásának módját.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Kommunikációs kapcsolatok védelme

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: ismerteti a kommunikációs kapcsolatok védelmét.

Az alfejezet tartalmi elvárásai:

* a rendszerkomponens által a saját kapcsolódó komponenseivel létesített kommunikációjának védelmét,
* a rendszerkomponens más komponensekkel létesített kommunikációjának védelmét,
* alkalmazott titkosítási algoritmusokat.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Egyéb rendszerkomponens specifikus biztonsági funkcionalitások

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja: kifejti az egyéb rendszerkomponens-specifikus biztonsági funkcionalitásokat.

Az alfejezet tartalmi elvárása: ismertesse az egyes rendszerkomponensekre specifikus biztonsági funkcionalitásokat, pl.:

* hálózat esetében port biztonság,
* Access Control List-ek (ACL-ek),
* OS esetén kártékony kód elleni védelem.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Címtár és DNS szolgáltatás

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: részletezi a címtár és a DNS szolgáltatást.

A fejezet tartalmi elvárása: részletezi az AD (vagy másik címtár) és a DNS szolgáltatás információbiztonsági aspektusait.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Authentikáció és jogosultság kezelés

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.1-es fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Felhasználói fiókok, szerepkörök és jogosultságok

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.2-es fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Helyi és központi naplózás

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.3-as fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Menedzsment lehetőségek/megoldások

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.4-es fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Kommunikációs kapcsolatok védelme

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.5-ös fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Egyéb rendszerkomponens specifikus biztonsági funkcionalitások

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.6-os fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

# Monitoring rendszer

{TÖRLENDŐ\_RÉSZ}

A fejezet célja: részletezi a monitoring rendszert.

A fejezet tartalmi elvárása: írja le a rendszert monitorozó eszközöket és azok alapvető beállításait (amennyiben nem releváns, elhagyható ez a fejezet).

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Authentikáció és jogosultság kezelés

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.1-es fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Szerepkörök és jogosultságok

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.2-es fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Helyi és központi naplózás

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.3-as fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Menedzsment lehetőségek/megoldások

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.4-es fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Kommunikációs kapcsolatok védelme

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.5-ös fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}

## Egyéb rendszerkomponens specifikus biztonsági funkcionalitások

{TÖRLENDŐ\_RÉSZ}

Az alfejezet célja és tartalmi elvárása: lásd 6.6-os fejezet.

{TÖRLENDŐ\_RÉSZ\_VÉGE}