KASZÓ Zrt.
7564 Kaszó

INFORMATIKAI BIZTONSÁGI ÉS FEJLESZTÉSI SZABÁLYZAT

Hatályos: 2020. május 1.

KASZÓ Zrt. Kaszó 7564 Kaszó

.....
Vezérigazgató

Tartalomjegyzék

1. Szabályzat célja

Az Informatikai biztonsági és fejlesztési szabályzat (továbbiakban IBFSZ) alapvető célja, hogy a számítástechnika alkalmazása során biztosítsa a KASZÓ Zrt. -nél (továbbiakban Társaság) a következőket:

- Üzleti-pénzügyi titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartását,
- az üzemeltetett számítógépek, valamint azok kiegészítő eszközeinek rendeltetésszerű használatát,
- az üzembiztonságot szolgáló karbantartást és fenntartást,
- az adatok számítógépes feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetését, illetve minimális mértékre való csökkentését,
- az adatállományok tartalmi és formai épségének megőrzését,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartását,
- adatállományok biztonságos mentését,
- a számítógépes rendszerek zavartalan üzemeltetését,
- a feldolgozás folyamatát fenyegető veszélyek megelőzését, elhárítását,
- az adatvédelem és adatbiztonság feltételeit,
- a védelemnek működnie kell a rendszerek fennállásának egész időtartama alatt, a megtervezésüktől kezdve az üzemeltetésükön keresztül a felhasználásig.
- az üzleti alkalmazások kialakításának és továbbfejlesztésének, az új technológiák implementálásának és bevezetésének (továbbiakban informatikai fejlesztések) szabályozásával biztosítsa az elkészült informatikai rendszerek:
    - felhasználói igényeknek való legjobb megfelelését
    - minőség növekedést
    - a Társaság informatikai infrastruktúrájához való alkalmazkodást

A jelen szabályzat az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét. Szabályozza a számítástechnikai eszközök használatának, és az adatvédelmi biztonság szabályait.

2. A Szabályzat hatálya

Személyi hatálya kiterjed:

- a Társaság valamennyi szervezeti egységére munkavállalójára, valamint
- a Társasággal szerződéses jogviszonyban álló természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre, a velük kötött szerződésben, illetve a titoktartási nyilatkozatban rögzített mértékben.

Tárgyi hatálya kiterjed:

- a védelmet élvező adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül

- a Társaság tulajdonában lévő, illetve az általa bérelt valamennyi számítástechnikai és információ technológiai berendezésre-eszközre, valamint az ezek műszaki dokumentációira is
- az informatikai folyamatban szereplő összes dokumentációra
- a rendszer- és felhasználói programokra
- az adatok felhasználására vonatkozó utasításokra
- az adathordozók tárolására, felhasználására
- a Társaság által indított valamennyi olyan informatikai fejlesztésre, amelynek időbeli terjedelme előre láthatóan meghaladja a 15 fejlesztői napot.

3. A szabályzathoz kapcsolódó szabályozások

Technikai, technológiai, bizonylati fegyelem betartását, a dokumentációk meglétét az egységes eljárások előírásait és a hatékony működést biztosító feltételeket rögzíteni kell.

- adatállomány nyilvántartásba vétele
- a bizonylatok áramlási útja
- alkalmazandó védelmi módszerek és eszközök
- adatok tárolásának és kibocsátásának módja
- hibás és fölöslegessé vált adatok selejtezési és megsemmisítési rendje
- hozzáférési jogosultság
- ellenőrzési jogosultságok és kötelezettségek

Az IBFSZ -t az alábbiakban felsorolt előírásokkal összhangban kell alkalmazni:

- Szervezeti és Működési Szabályzat
- Bizonylati Szabályzat
- Leltározási Szabályzat
- Selejtezési Szabályzat

4. Védelmet igénylő adatok, eszközök köre

A védelem tárgya:

- az alkalmazott hardver eszközök és azok működési biztonsága
- az informatikai eszközök üzemeltetéséhez szükséges okmányok és dokumentációk
- az adatok és adathordozók megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig
- az adatfeldolgozó programrendszerek, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egysége, előírásszerű felhasználása, reprodukálhatósága
- minden üzleti-pénzügyi titok, jogos vagy jogtalan felhasználóval szemben
- az alkalmazott biztonsági intézkedések, azok tervei, tartalmi előírásai és eljárási szabályai

A védelem eszközei:

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi, ügyrendi intézkedések, azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

5. A védelem felelőse

A Társaság rendszergazdai, informatikai, adatvédelmi feladatait az AranyMenta Kft. (7551 Lábod, Rákóczi u. 26.) képviseletében, Somorjai Roland és Vida András végzi.

Az adatvédelmi felelős kijelölése:

A jelen szabályzatban foglaltak szakszerű végrehajtásáról az Társaság adatvédelmi felelősének kell gondoskodni, aki Somorjai Roland.

Adatvédelmi felelős feladatai:

- ellenőrzi a védelmi előírások betartását
- ellátja az informatikai titokvédelmi munka szervezését és felügyeletét
- a védelmi eszközök alkalmazására vonatkozó döntés elkészítése érdekében a szakterületek bevonásával biztonságot növelő intézkedések kialakítása
- felelős a számítástechnikai rendszerek üzembiztonságáért, biztonsági másolatok készítéséért és karbantartásáért,
- biztosítja az üzemképességet és megszervezi a műszaki ellátást,
- gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról
- védelmi eszközök működésének, szerviz ellátás biztosításának folyamatos ellenőrzése
- adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása
- a Szervezeti és Működési Szabályzat adatvédelmi szempontból való véleményezése
- adatvédelmi feladatok ismertetése, oktatása
- a védelmi rendszer érvényesülésének ellenőrzése
- az IBFSZ kezelése, naprakészen tartása, módosítások átvezetése
- felelős a Társaság számítógépes rendszere, hardver eszközeinek karbantartásáért, és időszakos hardver tesztjeiért
- nyilvántartja a beszerzett, ill. üzemeltetett hardver és szoftver eszközöket a Társaság analitikus nyilvántartásai segítségével
- ellenőrzi a vásárolt és ingyenes szoftverek helyes működését, vírusmentességét, a használat jogszerűségét
- a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek izolálásáról
- folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonsága szempontjából a lényeges paraméterek alakulását
- ellenőrzi a rendszer önadminisztrációját
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására
- tevékenységéről rendszeresen beszámol az Társaság vezetőjének, évente egyszer írásban

Az adatvédelmi felelős ellenőrzési feladatai:

- évente egy alkalommal részletesen ellenőrzi az IBFSZ előírásainak betartását
- rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot
- ellenőrzi a számítástechnikai munkafolyamat bármely részét előzetes bejelentési kötelezettség nélkül
- adatvédelmi szempontból ellenőrzi az IBFSZ naprakészségét, illetve azok végrehajtását

Az adatvédelmi felelős jogai:

- előírások ellen vétőkkel szemben felelősségre vonási eljárást javasolhat a Társaság vezetőjénél
- bármely érintett szervezeti egységnél jogosult ellenőrzésre
- betekinthet valamennyi iratba, ami a számítástechnikai feldolgozásokkal kapcsolatos a titoktartási kötelezettség mellet
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére, illetve bevezetésére
- adatvédelmi szempontból az informatikai beruházásokat véleményezi

6. Az IBFSZ alkalmazásának módja

Az IBFSZ megismerését az érintettek részére az adatvédelmi felelős oktatás formájában biztosítja. Erről nyilvántartást vezet.

Az IBFSZ karbantartása

Az IBFSZ -ot az informatikában - valamint a Társaságnál- a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Ez az adatvédelmi felelős feladata. E tevékenységről, annak konkrét tartalmáról évente egyszer írásbeli beszámolót kell készíteni.

Az adatvédelmi felelős megbízatása

A felelőst az Társaság vezérigazgatója bízza meg. Írásbeli meghatalmazás alapján jogosult ellátni a hatáskörébe tartozó feladatokat.

A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság. Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk:

- közlésre szánt, nyilvános adat
- minősített adat, üzleti-pénzügyi titok

A számítógépes feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik. Különös védelmi utasítások és szabályozások nem mondhatnak ellent a törvények és a jogszabályok mindenkori előírásainak.

Az üzleti-pénzügyi titoknak minősülő adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot.

A kijelölt dolgozók előtt a titokvédelmi és egyéb rendszabályokat, a betekintési jogosultság terjedelmét, gyakorlási módját és időtartamát ismertetni kell.

A titkot képező adatok védelmét, a feldolgozás - 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). Ezek technikai megvalósítását a rendszergazda végzi.

7. Elektronikus hivatalos kommunikáció

A Társaság - mint 100 %-os állami tulajdonban lévő gazdasági társaság - esetében a tulajdonosi joggyakorló iránymutatása szerint az elektronikus hivatalos kommunikáció elsősorban kormányzati e-mail címek igénybevétele útján folyhat.

Kormányzati e-mail címnek kell tekinteni:
a) a gov.hu végződésű e-mail címeket,
b) a Kormány, illetve a Kormány tagja által irányított vagy felügyelt szerv által biztosított hivatalos elektronikus levelezési címeket,
c) a Kormány tagja vagy kormánybiztos tulajdonosi joggyakorlása alá tartozó gazdasági társaság által biztosított hivatalos elektronikus levelezési címeket,
d) a Kormány, illetve a Kormány tagja által irányított vagy felügyelt szerv vagy a Kormány tagja vagy kormánybiztos tulajdonosi joggyakorlása alatt álló gazdasági társaság tulajdonosi joggyakorlása alá tartozó gazdasági társaság által biztosított hivatalos elektronikus levelezési címeket, valamint
e) a Kormány irányítása vagy felügyelete alá nem tartozó, Alaptörvényben meghatározott szerv hivatalos elektronikus levelezési címeit.

Kizárólag kormányzati e-mail címre küldhetők ki az alábbi iratok:
- törvényjavaslatot tartalmazó irat,
- Kormány részére készült előterjesztés, jelentés,
- Kormány döntését igénylő előterjesztés,
- politikai felsővezetői (miniszterelnök, miniszter, államtitkár) döntést igénylő előterjesztés, különösen miniszteri rendelettervezet,
- politikai felsővezető részére készülő előterjesztés, jelentés,
- politikai vezető (kormánymegbízott) részére készülő előterjesztés, jelentés,
- biztosi jogviszonyban álló (kormánybiztos, miniszterelnöki biztos, miniszteri biztos) részére készülő előterjesztés, jelentés,
- szakmai felsővezető (közigazgatási államtitkár, helyettes államtitkár, központi hivatal vezetője és vezetőjének helyettese, kormányhivatal főigazgatója) részére készülő előterjesztés, jelentés
- szakmai vezető (kormányhivatal igazgatója, járási hivatal, illetve fővárosi kerületi hivatal vezetője és vezetőjének helyettese, főosztályvezető, osztályvezető) részére készülő előterjesztés, jelentés,
- minden olyan irat, amely a Kormánynak, a Kormány tagjának, politikai felsővezetőnek vagy vezetőnek, szakmai vezetőnek vagy felsővezetőnek, biztosi jogviszonyban állónak a döntését tartalmazza, mely nem kerül nyilvánosan közzétételre,
- a fentiekről készült tervezet, másolat vagy kivonat, a fentiekkel kapcsolatos munkaanyag

Ezen irattípusok nem kormányzati e-mail címre történő kiküldése csak és kizárólag Galamb Gábor vezérigazgató írásbeli engedélye alapján történhet.
Amennyiben a fenti irattípusok közé tartozó irat nem-kormányzati e-mail címre történő továbbítására engedély nélkül kerül sor, akkor az minden esetben munkajogi következményekkel fog járni az intézkedésben részt vevő munkavállalók irányában.

Amennyiben a fentiek szerinti irat nem kormányzati e-mail címre történő megküldése szükséges, akkor az irat továbbítása helyett elsősorban az irat tartalmának kivonatolása útján kell az abban foglaltakat a címzettel közölni. Ennek során lehetőleg kerülni szükséges az utalást arra, hogy a kérdéses tartalom végső soron honnan származik és azt milyen dokumentum tartalmazza, ehelyett elsősorban általános körülírással szükséges utalni a dokumentumban foglaltak keletkeztetőjére.

Minden olyan esetről, amikor a fentiek szerinti irat nem kormányzati e-mail címre történő továbbítására engedély nélkül került sor haladéktalanul értesíteni kell az Agrárminisztérium Személyügyi és Igazgatási Főosztályát (eset leírása, a kiadott irat ismertetése, a címzett e-mail cím megjelölése, az alkalmazott munkáltatói intézkedés bemutatása).

8. Informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas számítógépek és egyéb hardver berendezések fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel, a veszélyhelyzetek elháríthatók legyenek.

Elemi csapások, környezeti ártalmak

- Elemi csapás: földrengés, árvíz, vihar, villámcsapás, napkitörés stb. (a keletkezett kár csak a biztosító kártérítésével ellensúlyozható).
- légszennyezettség
- nagy teljesítményű elektromágneses térerő
- fokozott tűz- és robbanásveszély.

Közüzemi szolgáltatásba bekövetkező zavarok:

- feszültség-kimaradás
- feszültségingadozás

Humán kockázatok

Szándékos károkozás

- behatolás a számítástechnikai rendszerek környezetébe
- illetéktelen hozzáférés
- adatok- eszközök eltulajdonítása
- rongálás
- megtévesztő adatok bevitele és képzése
- feldolgozás, munkafolyamat zavarása, megakadályozása

Nem szándékos, illetve gondatlan károkozás

- figyelmetlenség, ellenőrzés hiánya
- szakmai hozzá nem értés
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása
- a megváltozott körülmények figyelmen kívül hagyása
- kártékony, nem kívánt szoftver behozatala a Társaság rendszereibe
- biztonsági követelmények és gyári előírások be nem tartása

- adathordozók megrongálása rossz tárolás, kezelés
- a karbantartási műveletek elmulasztása hibás működést, vagy az eszközök meghibásodását idézheti elő

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

9. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

Tervezés és előkészítés során előforduló veszélyforrások:

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása

A rendszerek megvalósítása során előforduló veszélyforrások:

- hibás adatállomány működése
- helytelen adatkezelés
- programtesztelés elhagyása, működés hiányos ellenőrzése

A működés és fejlesztés során előforduló veszélyforrások:

- emberi gondatlanság
- szervezetlenség
- képzetlenség
- szándékosan elkövetett illetéktelen beavatkozás
- illetéktelen hozzáférés
- üzemeltetési dokumentáció hiánya

10. Az informatikai eszközök környezetének védelme

<u>Vagyonvédelmi előírások</u>

- a gépterem helyiségét biztonsági zárral kell felszerelni
- a gépterembe be- és kilépés rendjét szabályozni kell
- az irodában, gépteremben csak az illetékes munkavállalók tartózkodhatnak
- az épület, iroda, gépterem kulcsának felvétele, ill. leadása csak aláírás ellenében történhet, melyet az recepciós tart nyilván
- munkaidőn túl az irodában, a gépteremben csak a munkahelyi vezető engedélyével lehet dolgozni
- az irodába, gépterembe történő illetéktelen behatolás tényét a Társaság vezetőjének azonnal jelenteni kell
- az irodahelyiségben elhelyezett számítástechnikai eszközöket csak a kijelölt dolgozók használhatják
- a számítástechnikai eszközök rendeltetésszerű használatáért a felhasználó felel

<u>Tűzvédelem</u>

A gépterem a „D" tűzveszélyességi osztályba tartozik, amely mérsékelten tűzveszélyes üzemet jelent.
A tűzvédelem feladatait, sajátos előírásokat az irodaépületre a
Műszaki osztály Tűzvédelmi utasítása tartalmazza.

Ebben meg kell határozni az alábbiakat:

- tűzvédelmi eljárásokat
- tűzmentesítési eljárásokat
- menekülési útvonalakat
- fontosabb mentési eljárásokat

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.
A nagy fontosságú pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos tárolóeszközben kell őrizni. Ezen adatállományok kijelölése a rendszergazda feladata.

11. Az informatikai alkalmazásánál felhasználható védelmi eszközök és módszerek

A gépterem és a számítógépet befogadó irodahelyiség védelme

Elemi csapás vagy a gépterem, ill. az irodahelyiség részleges vagy teljes károsodásakor a lehetséges intéznivalók:

- menteni a még használható anyagot
- biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása
- új adatfeldolgozás, helyiségek kialakítása
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást

Hardver védelem

A berendezések hibátlan és üzemszerű működését biztosítani kell.
A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.
A karbantartási munkákat tervezetten, körültekintően és gondosan kell elvégezni.
A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- tapasztalatokat,
- hardver tesztek által feltárt hibákat.

Az adatrögzítés védelme:

- adatbevitel hibátlan műszaki állapotú berendezésen történjen
- tesztelt adathordozóra lehet adatállományt rögzíteni
- a bejelentkezési azonosítók használatával lehet szabályozni, hogy ki milyen szinten férhet hozzá a munkakö ehez szükséges adatokhoz. A tárolt adatokhoz csak az illetékes szervezeti egységek személyei férjenek hozzá

Adathordozók védelme

Az adathordozók logikai védelmét az operációs rendszer és az ehhez tartozó ellenőrző, file-kezelő rutinok alkalmazásával lehet biztosítani. A számítástechnikai berendezések üzemeltetéséért a rendszergazda köteles gondoskodni a feldolgozások igényeinek megfelelő

adathordozók biztosításáról, beleértve a biztonsági másolatok eszközigényeit, illetve az üzemeltetés biztonságát növelő generációs adatállományok alkalmazását is.

Adathordozók tárolása

Az adathordozók tárolására a géptermen kívüli műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő tárolóeszközt, helyiséget kell kijelölni, illetve kialakítani. A használni kívánt adathordozót a tárolásra kijelölt helyről kell kivenni és oda kell vissza is helyezni, a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

Adathordozót harmadik félnek átadni csak a Társaság vezetőjének írásos engedélyével szabad, kivéve a jogszabály kötelezettség vagy hatósági eljárás során történő adatszolgáltatást.

Nyilvántartás

Az adathordozókról nyilvántartást kell vezetni. Az azonosító adaton kívül a felírás és megőrzés dátumát, védettség tényét, jogosultsági és illetékességi adatokat, valamint az adathordozó kiadására és visszavételezésére vonatkozó információkat kell tartalmaznia.

A nyilvántartásnak naprakészen követnie kell az adathordozók fizikai mozgását.

Megőrzés

Az adatállományok és adathordozók megőrzési ideje a keletkezési, vonatkozási időtől számított minimum 11 év. (Az állományba a vonatkozási időszakra történő utolsó bejegyzéstől számított 10+1 év)
Társadalombiztosítással kapcsolatos adatállományok nem selejtezhetőek.
Társadalombiztosítással kapcsolatos adathordozók nem selejtezhetőek megfelelő másolat megléte nélkül. Társadalombiztosítással kapcsolatos adatoknak nincsen lejárati idejük.
A Társaság törekszik az ügyvitellel kapcsolatos adatállományok (iktatóprogram, Libra, stb.) tizenegy éven túli időtartamra történő megőrzéséről, a technológia fejlődése és a rendelkezésére álló erőforrások és lehetőségek figyelembe vételével.

Karbantartás

Az adathordozókat félévenként tisztítani kell és ellenőrizni a mágneses adathordozók állapotát, előregedését. A nem mágneses adathordozókat műszaki leírásuknak megfelelően kell karbantartani.

Selejtezés, sokszorosítás, másolás

Olyan mágneses adathordozót, amelyet javíthatatlan fizikai károsodás ért selejtezni kell. Tehát:

- fizikailag sérült, javíthatatlan
- gyári, raktározási hibából következően felhasználásra alkalmatlan (deformálódott)
- mágnes adathordozóknál, ha a kapacitás a névleges érték 75 %-ánál kevesebb
- véglegesen elhasználódott

A működésre alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni.

Az újból felhasználható adathordozókat törlő-felülíró szoftverek segítségével kell kezelni (Gutmann eljárás, US DoD 522-22.M szabvány vagy ezekhez hasonló procedúra). Ha ez nem lehetséges fizikailag meg kell semmisíteni az adathordozót. Ezt az eljárást kell alkalmazni, ha a Társaság az adathordozót, vagy ha az adathordozót magában foglaló eszköz/berendezés értékesítésre kerül.

A selejtezést a selejtezési szabályzatnak és a szervezet iratkezelési szabályzatának megfelelően kell lefolytatni.
Sokszorosítást, másolást csak az érvényben lévő szabályzó környezet szerint szabad végezni. Biztonsági másolat, adatmentés, archív adatállomány előállítása másolásnak számít.

Leltározás

Az adathordozókat a leltározási szabályzatnak megfelelően kell leltározni.

File-ok védelme

Az adatállományok, file-védelme során gondoskodni kell arról, hogy azok ne károsodjanak. A fontosabb file-okat tartalmazó adathordozóról másolatot kell rendszeres időszakonként készíteni.
A másolt adathordozó csak a Társaság vezetője engedélyével adhatók ki harmadik félnek.

Vállalatirányitási rendszer védelme

Az üzemeltetésért felelős rendszergazdának biztosítani kell, hogy a Vállalatirányitási rendszer naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

Teendők a következők:

- név szerint kell kijelölni azokat a személyeket, akik a rendszerszoftverben módosításokat végezhetnek
- a módosítással egy időben, a dokumentációban is át kell vezetni a változásokat
- a változtatásokról nyilvántartást kell vezetni

Felhasználói programokhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférés megakadályozását biztosítani kell.
Gondoskodni kell arról, hogy a tárolt Adatállományok programok, file-ok ne károsodjanak, a követelményeknek megfelelően működjenek.

Programok megőrzése, nyilvántartása

A programokról naprakész nyilvántartást kell vezetni, a nyilvántartásból egyértelműen megállapítható legyen a program azonosítására és kezelésére vonatkozó adatok.

A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

- a program azonosítója
- a program megnevezése
- a program készítőjének neve
- a program felhasználási helye

A program dokumentáció a rendszerdokumentációnak része.

12. A központi számítógép(ek) és a hálózat munkaállomásainak működésbiztonsága

Központi gép(ek): (Libra3s, NAS)

Szünetmentes tápegység használata kötelező, mert megvédi a központi gépet az esetleges feszültség ingadozástól és áram kimaradás esetén az adatvesztéstől. A központi gép fontos állományairól -Libra3s- hetente biztonsági másolatot készít a rendszergazda. A biztonsági mentés állománya a NAS fájl szerveren kerül elhelyezésre. A biztonsági mentések állománya

időszakosan, a NAS file szervertől fizikailag elkülönült adathordozóra mentésre kerül. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes feladatokhoz igazítottan kell alkalmazni.
A Libra3s vállalatirányítási rendszer meghibásodása esetén szükség szerint, a Libra Szoftver Zrt. (1113 Budapest, Karolina út 65.) munkatársának, telefonos egyeztetés után, a Társaság gazdasági igazgatójának szóbeli engedélyével „távoli asztal hozzáférést" biztosítható. A hozzáférés megelőzően a rendszergazdát értesíteni kell.

A központi gépteremhez, központi gépekhez a következő személyek férhetnek hozzá:

- Vezérigazgató
- Gazdasági igazgató
- Rendszergazda
- Belső ellenőr

A felsorolt személyeken kívül kizárólag a vezérigazgató, vagy gazdasági igazgató eseti engedélyével lehet a gépteremben tartózkodni.

Munkaállomások

Szünetmentes tápegység használata kötelező, mert megvédi a munkaállomást az esetleges feszültség ingadozástól és áram kimaradás esetén az adatvesztéstől. A rendszerbe új alkalmazást futtatni (idegen adatot importálni, betölteni) csak a rendszergazdával történő egyeztetés és engedélyezés után lehet. Kártékony, nem kívánt programmal fertőzöttség gyanúja esetén a rendszergazdát haladéktalanul értesíteni kell. Az adat felvitelt a fertőzöttség megszüntetéséig fel kell függeszteni. Új rendszereket, alkalmazásokat használatba vételük előtt adaptálni kell. Hibátlan működésükről tesztadatok, tesztfolyamatok segítségével meg kell győződni.
A Társaság rendszeriből szoftver(eke)t, adatállomány(oka)t másolni a jogos belső felhasználói igényeken túlmenően szigorúan TILOS!
Az általános ügyviteli célú valamint az irodai alkalmazások állományainak (szövegszerkesztő, táblázatkezelő, adatbázis kezelő, prezentáció, kép, levelező stb.) biztonsági másolatáról a munkaállomáson dolgozó érintettek kötelesek gondoskodni a rendszergazda iránymutatása alapján. A Kaszó NAS file szerveren minden felhasználónak rendelkezésére áll egy saját mentési könyvtár (home mappa) melyre legalább kéthetes idő intervallumban biztonsági mentést kell készíteni.

Mobil telefonok, okos telefonok, hordozható eszközök stb.

A Társaság hálózatára mobil eszközről, telefonról vezeték nélküli eszközökön át nem lehetséges a kapcsolódás biztonsági megfontolásból. Eltérő IP cím tartományból kapnak IP címet az ilyen eszközök, így nem kapcsolódhatnak a szerverekhez.

13. Informatikai Fejlesztések

13.1. Informatikai fejlesztések során alkalmazott elvek, követelmények

Az informatikai fejlesztésekkel szembeni általános elvárások

- Az informatikai fejlesztési tevékenység során törekedni kell a legjobb üzleti gyakorlat lehetőség szerinti alkalmazására, egyidejűleg a fejlesztések eredményeképpen a működésnek a legjobb üzleti gyakorlathoz való közelítésére, megvalósítására.
- Az informatikai fejlesztési tevékenység alapja a mindenkor hatályos éves informatikai beruházási terv

- Az éves informatikai beruházási terv változtatása, a prioritások átrendezése, tételek törlése, illetve új tételek beillesztése a hatályos szabályozások és előírások szerint történhet.
- Minden rendszerbe állításra kerülő eszköznek meg kell felelnie a hatályos előírásoknak, valamint a Társaság hatályban lévő informatikai biztonsági, információbiztonsági, üzembiztonsági és teljesítmény-követelményeinek.
- Az eszközöket úgy kell megválasztani, hogy működésük, felépítésük megfeleljen a vonatkozó iparági szabványnak, valamint a piacon érvényesülő szokásoknak, elveknek.
- Az eszközök megválasztásánál törekedni kell arra, hogy az üzemeltetés a lehető legnagyobb mértékben automatizálható és menedzselhető legyen.
- A Társaság informatikai rendszerébe csak olyan szoftverelem kerülhet, amelynek jogtiszta volta egyértelműen igazolható.
- Az adatok mozgatása során lehetőség szerint előnyben kell részesíteni a nagyobb biztonságot és rendszerintegrációt garantáló megoldást.

Fejlesztési csatornák

A Társaság az informatikai fejlesztéseket külső szállítók igénybevételével valósítja meg. A külső szállítóval kötött szerződésben meghatározásra kerül az alkalmazandó fejlesztési keretrendszer, futtató operációs rendszer és adatbázis kezelő rendszer lehetséges fajtája. A belső erőforrásból megvalósuló informatikai fejlesztések a meglévő technológiák felhasználásával történnek.

A fejlesztés eredményével szembeni elvárások

Az informatikai fejlesztések megvalósítása során – a rendelkezésre álló erőforrások szem előtt tartásával – a magas funkcionalitású, megbízható, széles körben alkalmazott integrált rendszereket kell alkalmazni. Ha az adott feladat egészére, vagy egy részére létezik már alkalmazott megoldás, meg kell vizsgálni annak alkalmazhatóságát. Kiemelt szempontként kell kezelni a meglévő, a stratégiai célokat támogató, korábbi beruházások védelmét. Általános szabály, hogy az informatikai fejlesztések során nyitott, megengedő alkalmazások kerüljenek megvalósításra. Az alkalmazásoknak segíteniük kell a rugalmas munkavégzést. Az alkalmazások megvalósítása során az egyes funkcionális rétegeket – adatkezelés, üzleti logika, felhasználói felület – úgy kell megvalósítani, hogy az egyes rétegek önmagukban módosíthatóak, áthelyezhetőek és konfigurálhatóak legyenek, a funkcionális rétegen belüli változtatás a kapcsolódó réteg(ek) számára ne legyen látható.

Az informatikai fejlesztések során

- a fejlesztésekbe a lehető legnagyobb mértékben be kell vonni a belső szakértőket és fel kell használni a saját erőforrásokat
- kizárólag saját erőforrásokon alapuló fejlesztéssel csak azok az igények teljesíthetők, melyek a meglévő fejlesztő eszközökkel, kis munkaráfordítással elvégezhetőek
- meg kell valósítani a rendszerek lehető legnagyobb mértékű integrációját kivéve, ha ez ellen – konkrét esetben – jól meghatározott érvek (pl. jogszabályi előírások, biztonsági szempontok stb.) hozhatók fel
- a kialakítandó rendszer adatbázis-kezelő platform független legyen annak érdekében, hogy a kiszolgáló adatbázis-kezelő cseréje könnyen, relatív kis ráfordítással elvégezhető legyen

- a Társaság szakemberei által rugalmasan paraméterezhető rendszerek kerüljenek bevezetésre, amelyekben a módosuló folyamatok belső erőforrással, paraméterezéssel lekövethetőek.

Megbizhatóság

Amennyiben az adatosztályozás azt megköveteli, az alkalmazói rendszereket úgy kell megvalósítani, hogy azok képesek legyenek kihasználni a műszaki-technikai infrastruktúra által biztosított, rendelkezésre állási és hibatűrési lehetőségeket.

Minőségbiztosítás

A minőségbiztosítás célja, hogy elősegítse, lehetőség szerint garantálja a fejlesztés termékeinek (a rendszertervek, a működő rendszer és a dokumentációk) elkészítésének szakszerűségét, az elvárt sikerkritériumok teljesülését.

A minőségbiztosítás eszközei:

- a termékek minőségi paramétereinek meghatározása,
- az átvételi, ellenőrzési pontok kijelölése,
- a szállítói szerződések betartásának folyamatos ellenőrzése,
- a követelményspecifikációban megfogalmazott célok, feladatok, keretek összhangjának folyamatos ellenőrzése,
- részvétel a tesztelési folyamatokban és/vagy azok ellenőrzése dokumentumokon keresztül,
- az átvett termékek és dokumentumok ellenőrzése,
- szállítói minősítési rendszer működtetése.

A minőségbiztosítási folyamattal feltárt hiányosságok, hibák megszüntetése az informatikai fejlesztés témavezetőjének felelőssége.
A megvalósítási folyamatban alkalmazható független vagy nem független belső minőségbiztosítási csoport, vagy független külső minőségbiztosító.
A minőségbiztosítás konkrét fejlesztésben alkalmazott eszközeit a követelményspecifikációban kell feltüntetni.

Alkalmazkodás a meglévő Társasági környezethez

Az informatikai fejlesztéseknek a konkrét szakmai/felhasználói célok megvalósításán túlmenően teljesíteniük kell a kompatibilitási, összekapcsolhatósági követelményeket is.

Az alkalmazásintegráció célja egy olyan informatikai környezet kialakítása, amely összeköti a Társaságnál használt szoftverrendszereket, és ezek összehangolásával biztosítja a Társaság szervezeti egységei számára szükséges szolgáltatások technológiai hátterét. Ezáltal lehetővé válik a régi alkalmazások által nyújtott funkciók megtartása, valamint a megváltozott igények kielégítő új komponensek rendszerbe illesztése, a változások gyors implementálása és azok rugalmas, fokozatos bevezetése a rendszer zavartalan működése mellett. Az alkalmazásintegráció érdekében az üzleti logikát a szolgáltatásorientált architektúra (SOA) elvárásainak megfelelő kialakításra kell törekedni.

A fejlesztés során adottnak kell tekinteni a kapcsolódó rendszereket és infrastrukturális szolgáltatásokat (operációs rendszerek, levelezőrendszer, adatbázis-kezelő infrastruktúra, hálózati topológia, informatikai védelmi rendszerek, felügyeleti és menedzsment eszközök), amelyek technológiájához és üzemeltetési szabályrendszeréhez alkalmazkodni kötelező. A

fejlesztés során meg kell tervezni és meg kell valósítani a kapcsolódó infrastruktúra mennyiségi, vagy minőségi bővítését is, illetve ha új elemre van szükség, akkor annak létrehozását és működtetését is.

Az alacsony üzemeltetési költségek érdekében korlátozott számú működési platform üzemeltetését biztosítjuk. A fejlesztés/beszerzés előterjesztésében ki kell térni a szükséges futtató környezetre, külön bemutatva az éles, valamint a fejlesztői és teszt környezetek erőforrás igényét.

Minden kliens megoldás esetében kötelező az automatikus működésű telepítő eljárás elkészítése, amely illeszkedik a Társaság kliens-telepítéseket végző architektúrájához.

Az alábbi általános követelmények mind a készen vásárolt, mind az egyedi fejlesztésű rendszerek esetében figyelembe veendők, a további elvárások a rendszer általános, vagy egyedi jellegétől függőek:

A rendszerek tervezésekor – mind műszaki, mind pénzügyi szempontból – a működéshez és működtetéshez tartozó minden elemet – hardver, szoftver, egyéb eszközök – figyelembe kell venni, függetlenül azok meglététől. Az erőforrás és kapacitásterveknek a működő rendszer teljes erőforrás-igényét be kell mutatniuk (pl. memória, adattároló, licence, mentés-archiválás, emberi erőforrás stb.).

A reprodukálhatóság és ellenőrizhetőség érdekében az alkalmazáshoz kötelező olyan automatizált eljárások szállítása, amelyek képesek:

Egy működő rendszerpéldány felépítésére (telepítés), induló adatokkal való feltöltésére, és egy már működő rendszerpéldány adatainak áttöltésére, igény szerint a rendszer tervezésekor meghatározott adatok tartalmi megváltoztatásával, különös tekintettel az üzleti szempontból kritikus, illetve az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény által érintett adatok azonosíthatatlanságára vonatkozóan.

A rendszereknek hosszú időn át, teljesítményvesztés nélkül működniük kell, az adatok mennyiségi növekedése – az üzemeltetési leírásban rögzített értéken belül – a feldolgozási időt érdemben nem befolyásolhatja.

A rendszerek tervezésekor hosszú, legalább 11 éves működési időtartamot kell figyelembe venni.

A rendszer tervezése és fejlesztése során kizárólag olyan megoldások alkalmazhatóak, amelyek biztosítják az átadandó rendszer informatikai infrastruktúrába illeszthetőségét és üzemeltethetőségét.

A Társaság a fejlesztés során a készítés alatt álló, illetve az elkészült kódot – akár harmadik fél bevonásával is – ellenőrizheti abból a szempontból, hogy az megfelel-e az utasításban, illetve a specifikációban foglaltaknak (code review). A fejlesztőnek az ellenőrzés lehetőségét folyamatosan biztosítania kell.

A Társasági arculatnak, az általános felhasználói és iparági-szakmai elvárásoknak megfelelő, a környezetében működő termék/termékek készítését várja el.

A fejlesztési és tesztelési környezetek kialakítását az éles rendszertől elkülönülten, lehetőleg virtuális környezetben kell megvalósítani.

Meglévő, üzemelő rendszer módosítása esetén a fejlesztői környezetnek – az aktuális fejlesztésektől eltekintve – a beállítások tekintetében meg kell egyeznie az éles üzemi rendszerrel.

Biztonsági elvárások

Az informatikai fejlesztésekkel kapcsolatos információbiztonsági elveket és követelményeket jelen szabályzat határozza meg.
A fejlesztési feladat indításakor az adatvédelmi felelős meghatározza a fejlesztendő rendszer biztonsági besorolását.

A fejlesztés tervezési szakaszában a rendszer biztonsági osztályba sorolása alapján a fejlesztő egyeztet az adatvédelmi felelőssel, a kockázatokkal arányos védelmi intézkedésekről, az adattárolás, felhasználói felület, adatkapcsolatok, naplózás, mentés és felügyelet módjáról.
A rendszer tervezője a meghatározott védelmi elvárások szerint tervezi meg a fejlesztés során alkalmazott technológiai lépéseket és ennek figyelembe vételével készíti el a rendszertervet.
Adott rendszer besorolás szerinti elvárásaitól eltérni kizárólag az adatvédelmi felelős jóváhagyásával lehet.

Külső fejlesztői hozzáférés

A külső fejlesztői hozzáféréssel kapcsolatos rendelkezéseket az IBFSZ -al összhangban írásban le kell fektetni az informatikai fejlesztés tervezési szakaszának lezárása előtt.

Címtár használata

A címtárra épülő szolgáltatásokat a Társaság által kiválasztott címtárszolgáltatásban kell megvalósítani.

Levelezés, értesítések küldése

A levelezést, értesítés küldését a Társaság által kiválasztott levelezőrendszer támogatásával kell megvalósítani.

PKI

Amennyiben a digitális hitelesítés, vagy titkosítás előírt, a Társaság PKI infrastruktúráját kell alkalmazni. Ha az alkalmazás publikus szolgáltatást (is) nyújt, minősített hitelesítő szolgáltató tanúsítványait kell alkalmazni.

DNS

A szolgáltatás, a lehetőségekhez mérten regisztrálható legyen a DNS-ben, illetve ha regisztrálható, akkor a szolgáltatás DNS lekérdezés alapján legyen elérhető.

Virtuális környezet

Az alkalmazás legyen képes a Társaság által kiválasztott környezetben kialakított virtuális infrastruktúrával történő együttműködésre. Fizikai környezet kialakítására csak a rendszer tervezésekor beszerzett előzetes engedély alapján van mód.

Archiválás

Az alkalmazások megvalósítása során olyan megoldást kell alkalmazni, mely kizárólag a működéshez ténylegesen szükséges adatokat tartja az operatív adattárban, a már nem szükséges adatokat ettől elkülönülten kezeli, ezáltal megoldhatóvá válik az elkülönülten kezelt adatok archiválása.

Az operatív adattár mérete nem nőhet a tervezési maximum fölé. A rendszer válaszideje az adatok mennyiségének növekedésével sem haladhatja meg a tervezési értéket.
Az alkalmazás támogatja az archív adatok egészének, vagy egy részének visszatöltését. A rendszert a korábbi verziókban archivált adatok visszatöltésére is fel kell készíteni.

13.2 Informatikai fejlesztési igény bejelentése és jóváhagyása

Informatikai fejlesztést a Társaság bármely szervezeti egysége kezdeményezhet, az alábbi adatok megadásával:

- A megvalósítani kívánt üzleti/technológiai igény
- Az üzleti cél

- A támogatandó folyamatok
- Az informatikai támogatás elvárt szintje (kritikus sikertényezők)
- Az elvárt előnyök
- Az informatikai fejlesztés elmaradása esetén bekövetkező károk, felmerülő költségek és egyéb kockázatok
- A bevezetés elvárt határideje
- Az érintettek
- Az igény rangsorolása
- A kezdeményező részéről a fejlesztésbe bevonni kívánt szakértők

A kezdeményező csatolja az informatikai támogatást nem igénylő megoldás(ok) vizsgálatának bemutatását. A kezdeményező vizsgálatának a nem informatikai jellegű lehetőségekre kell kiterjednie, amely lehet élőmunka, munkaszervezés, illetve valamilyen – rendelkezésre álló – egyéb eszköz alkalmazása. Informatikai fejlesztés akkor indokolt, ha a felmerült probléma megoldása hosszútávon lényegesen olcsóbb, gyorsabb és jellemzően nem egyszeri igény.

13.3 Informatikai fejlesztések eljárása

A lebonyolítás szervezeti keretei

A fejlesztési igény jóváhagyását követően a Társaság vezetője kijelöli a fejlesztés témafelelősét, és elindítja fejlesztési feladatot.
Az adott fejlesztési feladatban résztvevőket – elektronikus úton – a témafelelős kéri ki az adott fejlesztési feladattal összefüggésben felmerült kérdésekben illetékes szervezeti egységek vezetőitől, az irányításuk alá tartozó munkavállalók közül.

A fejlesztések követelményspecifikációja

A fejlesztési feladat specifikálását a témafelelős irányításával, az általa kikért munkavállalók végzik (a továbbiakban: specifikálást végző személyek).
A témafelelős – a fejlesztés igénylőjével egyetértésben – az adott fejlesztési feladathoz releváns információ tartalommal és részletességgel specifikálja a feladatot.
A fejlesztési feladat specifikálása az adott téma lehatárolásával, terjedelmének meghatározásával kezdődik, amelyet a követelményspecifikáció követelmények részében rögzíteni kell. A terjedelem meghatározásakor meg kell fogalmazni a benne foglalt és a kizárt elvárásokat is. A terjedelmet a sikertényezők meghatározásával tovább kell pontosítani, azaz meg kell határozni, hogy a rendszertől elvárt szolgáltatás teljesülése mivel és hogyan lesz mérhető, illetve elfogadható.
A téma lehatárolása után meg kell nevezni az igénykeltőket, azaz azokat a személyeket, csoportokat vagy szabályozási és egyéb környezeti elemeket akik, vagy amelyek a

létrehozandó termék teljes életútja (fejlesztés, használat, üzemeltetés, esetleg megsemmisítés) során a termékkel szemben elvárásokat fogalmaznak meg.
Ezt követően fel kell mérni a termékkel szemben támasztott követelményeket, igényeket, melyeket rangsorolni kell.
Az igények alapján kell a termék funkcióit megtervezni, amelynek során összeáll a termék rendezett funkciólistája. A funkciókkal kapcsolatos valamennyi elvárást szöveges formában rögzíteni kell.
A funkciók alacsonyabb költségen, illetve magasabb minőségen való megvalósíthatósága érdekében meg kell vizsgálni, hogy lehetséges-e több informatikai megoldás. Ezen előzetes vizsgálat során a témafelelősnek szem előtt kell tartania, hogy a vizsgálat terjedelme – a

várható külső és belső erőforrásigények becslését figyelembe véve – nem haladhatja meg a fejlesztés összes ráfordításának 15%-át.
Amennyiben több megoldás is létezik az elvárt eredmény/termék létrehozására, akkor a lehetséges megoldások funkció-teljesítés vizsgálatát is el kell végezni, beleértve a Társaságnál már rendelkezésre álló rendszerelemeket is. A vizsgálat eredményeképpen a megoldási alternatívák összehasonlíthatóak lesznek, valamint láthatóvá válik, hogy a vizsgált termék(ek) milyen mértékben teljesíti(k) a tervezett termékkel szemben támasztott elvárásokat.

Követelményspecifikáció összeállításakor ki kell térni az alábbiakra:

- Üzleti követelmények
  - Üzleti célok
  - Támogatandó folyamatok és azok elvárt szintje (kritikus sikertényezők)
  - Függőségek
  - Teljesítmény elvárások
- Funkcionális elvárások
  - Funkciólista
  - Funkciók által támogatott folyamatok leírása
- Nem funkcionális követelmények
  - Felhasználói felület (egyszerűség, egységes megjelenés más alkalmazásokkal stb.)
  - Információbiztonsági követelmények
  - Rendszerek és szolgáltatások függései, más rendszerekre gyakorolt hatás
  - Infrastrukturális hatások
- Működtetési, üzemeltetési követelmények
  - Skálázhatóság, korlátok
  - Kezelhetőség
  - Támogatás
  - Működtető személyzettel kapcsolatos követelmények
  - Várható szolgáltatási szintről megállapodás (SLA)
  - Oktatással kapcsolatos elvárások
- A minőségbiztosítás alkalmazott elemei
- Szükséges dokumentumok

13.4 A fejlesztés végrehajtása

Fejlesztési módszertanok követése

A fejlesztéshez alkalmazott módszertant a szállító és megrendelő oldali témafelelősök a feladat jellege alapján közösen választják ki.
A módszertan kiválasztásakor kiemelt szempont, hogy a megrendelő, felhasználó – lehetőség szerint – minél korábban ismerje meg a leszállítandó terméket, a funkciók nagyobb csoportjait külön tesztelési ciklusokban tudja átvenni, annak érdekében, hogy a fejlesztők felé időben megtörténhessen a visszacsatolás.
Törekedni kell olyan fejlesztési módszertanok kiválasztására, amelyek biztosítják a felhasználói és a fejlesztői erőforrások optimális és egyenletes felhasználását.

A fejlesztések környezete

Belső fejlesztés esetén saját erőforrásból biztosítjuk a fejlesztői környezetet.

Külső fejlesztéseknél alapértelmezés szerint a szállító saját telephelyén fejleszt, de külön megállapodás alapján a Társaság is biztosíthatja a fejlesztői rendszert. Az IBFSZ előírásai kötelező érvénnyel vonatkoznak a szállítóra, saját telephelyen történő fejlesztés esetén is.

Fejlesztési szakasz

A termék-funkciók megvalósításának módjára Koncepcióterv formájában kell javaslatot tenni.

A Koncepcióterv a követelményspecifikációhoz képest az alábbi kiegészítéseket tartalmazza:

- A szakmai megoldás bemutatása
  - A javasolt megoldás funkcionális felépítésének bemutatása
  - A követelményekre adott szakmai megoldási javaslatok kifejtése
  - A megvalósítandó folyamatok támogatásának szakmai leírása
  - Az esetlegesen szükséges migráció(k) felsorolása, megvalósítási javaslat ezek elvégzésére
  - Az esetlegesen szükséges külső adatkapcsolatok és azok tervezett megvalósításának bemutatása
- A megoldás informatikai architektúrájának bemutatása
  - Tervezett hardver és szoftver architektúra modell
  - A kialakításhoz szükséges lépések bemutatása
- A megvalósítás bemutatása
  - Megvalósítási ütemterv
  - Migrációs ütemterv
  - Átállási ütemterv
  - Tesztelési terv

A Koncepciótervet a kezdeményező képviselője és a témafelelős közvetlen felettese fogadja el. A kezdeményező elfogadási joga és kötelezettsége nem vonatkozik az informatikai architektúra tervre.
A fejlesztési szakasz a rendszerterv kidolgozásával folytatódik. Amennyiben a fejlesztési módszertan vagy folyamat megköveteli, a korábbi dokumentumokat (követelmény specifikáció, Koncepcióterv) módosítani kell.

A rendszerterv kidolgozása során különbséget kell tenni egyedi fejlesztés vagy piacon kapható termékek között.
Vásárolt termék bevezetése esetén a részletes tervezésnek legalább az alábbiakra ki kell terjednie:

- a rendszer paraméterezése
- egyedi kiegészítő funkciók részletes tervezése
- külső interfészek részletes tervezése
- biztonsági funkciók (jogosultsági rendszer, naplózás, archiválás, változáskezelés) részletes tervezése
- üzemeltetési, adminisztrációs feladatok részletes tervezése
- háttér-mentési, archiválási és vészhelyzeti funkciók részletes tervezése

Vásárolt termék esetében a témafelelős dönthet úgy, hogy a Koncepcióterv és a rendszerterv összevonja.
Az egyedi fejlesztések rendszertervében – a Koncepcióterv tartalmán túl – ki kell térni az alábbiakra:

- felhasználói felület szolgáltatásai
- üzleti szolgáltatások rétege
- adatelérési réteg
- külső interfész specifikáció
- meglévő környezetbe illeszthetőség terve
- biztonsági és jogosultsági rendszer,
- minőségi jellemzők (pl. rendelkezésre állás)
- alkalmazás adminisztrációja
- háttér-mentési, archiválási és vészhelyzet követelmények
- architektúra modell
- hardver és szoftver környezet függései

A rendszertervet a témafelelős fogadja el. Külső fejlesztővel megvalósított fejlesztés esetén a Társasági témafelelős elfogadása elsősorban a szükséges tartalmi elemek meglétét és kellő részletezettségét igazolja, és a külső fejlesztőt nem mentesíti a szerződésben foglalt, kifogástalanul működő rendszer kialakításának felelősségétől.
Új rendszer bevezetése esetén Implementációs tervet is készíteni kell, mely a kialakítás előtt álló rendszernek a jelenlegi infrastruktúrába való illesztését mutatja be.
A részletes tervezést a rendszerelemek fejlesztési környezetben történő kódolása, kialakítása követi.
A fejlesztés elkészítése után kell végrehajtani a Koncepcióterv részeként elkészített tesztelési tervben foglaltakat.
A fejlesztés egyik végterméke a "Telepítő csomag", amelynek részei a programok, beállítások, esetenként adatok és a telepítési útmutató, valamint – szükség esetén – a régi rendszer visszaállítási terve.
A fejlesztési szakasz termékei:

- Módosított vagy új Koncepcióterv
- Rendszerterv
- Implementációs terv (ha szükséges)
- Telepítő csomag
- Átadás-átvételi jegyzőkönyv

13.5 Tesztelési eljárás

Valamennyi, a szabályzat hatálya alá tartozó informatikai fejlesztési terméket tesztelni kell. A felhasználó a tesztelési eljárás keretében győződik meg arról, hogy az informatikai fejlesztés az általa támasztott igényeknek megfelel, és ezt dokumentált formában köteles igazolni. A teszt elvégzésének dokumentált formája a tesztlap. Amennyiben az adott fejlesztés vonatkozásában csak többfajta és azon belül többféle teszt végrehajtásával lehet meggyőződni az informatikai fejlesztés megfelelőségéről, akkor a tesztelés végrehajtásának tervezett formáját Tesztelési forgatókönyvben kell rögzíteni, melyhez csatolni kell a tesztlapokat. A Tesztelési forgatókönyvet a témafelelős fogadja el.
A tesztelést a témafelelős vagy az általa – a fejlesztés indításakor – kijelölt Társasági tesztfelelős koordinálja (továbbiakban tesztfelelős).

A tesztelési forgatókönyv első verziójában tesztelési stratégiát kell lefektetni, amelynek tartalmaznia kell

- a választott tesztelés fajtáit
- a tesztkörnyezet kialakításának módját
- a tesztelést támogató eszköz használatát, valamint
- az automatikus tesztrendszer alkalmazhatóságát

A tesztelési stratégia megalkotása időben a programozási munkák megkezdése előtt történik. A teszteseteket – beleértve azok körének a tesztelés során szükségessé vált bővítését is – a kezdeményező dolgozza ki a témafelelős közreműködésével. A kezdeményező által készített teszteseteket kell alkalmazni a fejlesztői és a felhasználói tesztek során is.

A tesztelés fajtái

A tesztelést a fejlesztési szakasz elvégzését követően kell végrehajtani. A feladat függvényben az alábbi tesztek fordulhatnak elő:

- Fejlesztői teszt (kötelező): a fejlesztő által a teszt rendszerben elvégzendő teszt, amely során a megrendelő képviselője megbizonyosodik arról, hogy az elkészített funkció üzemkész, specifikáció szerint működik és más rendszerfunkciók sem romlottak el.
- Felhasználói funkcionális teszt (kötelező): előzetes oktatást követően a leendő felhasználó által végzett teszt, amelynek a célja, hogy a felhasználói jóváhagyás megtörténjen. A teszt során vizsgálni kell, hogy a funkciók megfelelnek a felhasználói követelményeknek, és azt az elvárt válaszidővel szolgálja ki. A felhasználói funkcionális teszt részeként ellenőrizni kell, hogy az előírt információbiztonsági követelményeket a rendszer maradéktalanul teljesíti-e.
- Integrációs teszt (szükség esetén): amennyiben a fejlesztett funkció kapcsolatban áll további funkciókkal, úgy vizsgálni szükséges, hogy a funkciók együttműködése megfelel a folyamat elvárásainak. A rendszer bevezetése előtt bármely rendszerelem változása szükségessé teszi újabb integrációs teszt végrehajtását.

- Migrációs teszt (szükség esetén): amennyiben az új rendszer/rendszerelem használatához adatmigráció szükséges, úgy tesztelni kell a migráció folyamatát, és a migrált adatok rendeltetésszerű felhasználhatóságát.

- Üzemeltetési teszt (szükség esetén): tesztelni kell az új elemek üzemeltethetőségét. Az üzemeltetési teszt során figyelmet kell fordítani arra, hogy
    - definiálni kell a típushibák kezelési módját
    - a zárás hibamentesen lefusson
    - a zárás időtartama a rendelkezésre álló időbe beleférjen
    - a mentési-helyreállítási, archiválási-visszatöltési és vészhelyzet eljárások megfelelően működnek-e

- Jogosultság teszt (szükség esetén): amennyiben az új rendszer/rendszerelemhez eltérő felhasználói hozzáférés szükséges, vagy a meglevő jogosultsági struktúra módosul (például új jogosultsági szerepkör, jogosultsági objektum stb.), úgy tesztelni kell, hogy az adott felhasználói hozzáférés a kívánt mértékben biztosított-e. Vizsgálni kell továbbá azt is, hogy ne kapjanak a felhasználók a szükségesnél bővebb jogokat.

- Terheléses teszt (szükség esetén): amennyiben az új rendszer/rendszerelem tömeges használatba kerül, úgy vizsgálni kell, hogy erre képes-e. A vizsgálat végezhető teszteszköz használatával vagy szervezetten, nagyobb létszámú csapat bevonásával.

- Éles üzemi átállás tesztje (szükség esetén): amennyiben jelentős változatás kerül megvalósításra valamely rendszerben, vagy valamely számottevő rendszerelemben, úgy éles üzemi átállási forgatókönyvet kell készíteni, amelynek tesztelni kell a végrehajthatóságát.

Tesztkörnyezet

A tesztelést az üzemi környezettől eltérő, annak működését nem befolyásoló önálló tesztkörnyezetben kell elvégezni.

A tesztkörnyezet előállítása során az alábbiakra kell figyelmet fordítani:

- a rendszernek a beállítások tekintetében meg kell egyeznie a fejlesztői rendszerrel
- terheléses teszt esetén a rendszernek kapacitásában, adatmennyiségében és a beállítások tekintetében meg kell egyeznie az éles üzemi rendszerrel
- az éles rendszerekből előállított tesztrendszerek adatait személyteleníteni kell abból a célból, hogy a külsős fejlesztők üzleti titokhoz és személyes adathoz ne férjenek hozzá
- nagyobb tesztelési munkák közben a tesztrendszer frissítését kerülni kell

Tesztelési szerepkörök

A tesztfelelős koordinálja a tesztelést, elfogadja a külső fejlesztői teszteket, irányítja a belső informatikai és felhasználói tesztelőket.

Tesztfelelős feladatai:

- A Tesztelési forgatókönyv elkészítése vagy annak jóváhagyása, ha a fejlesztő készíti.
- A Tesztelési forgatókönyvben megfogalmazottak Társaság oldali betartása és betartatása.

- A Felhasználói teszt megszervezése a Társaság oldalán, beleértve az emberi és egyéb erőforrások biztosítását.
- Felhasználói teszt tervezés támogatása.
- A Felhasználói teszt Társaság oldali előrehaladásának ellenőrzése, monitorozása.
- Tesztelő felhasználók támogatása a Tesztelési forgatókönyvben leírtak végrehajtásában.
- A Felhasználói teszt adminisztrációjának, dokumentálásának követése.
- A felhasználók által bejelentett hibák kontrollálása.
- A tesztelt és a tesztelők által hibásnak ítélt teszteseteknél a hiba prioritásának és súlyosságnak egyeztetése a fejlesztővel, amennyiben a fejlesztő a hiba tesztelője általi kategorizálással nem ért egyet.

Fejlesztő feladatai:

- A fejlesztői tesztek megtervezése, elvégzése és dokumentálása.
- Amennyiben készült Tesztelési forgatókönyv, úgy annak készségszintű megismerése és betartása.
- Tesztelési forgatókönyv készítése, ha a fejlesztési megállapodás erről rendelkezik.
- A hibásnak talált teszteseteknél a hibák ütemezett javítása, annak dokumentálása.

Rendszergazda feladatai:

- Tesztelési környezet kialakítása.
- Tesztesetek véleményezése, valamint szükség szerint kiegészítése az Interfész és egyéb rendszergazdai tesztekkel.
- Felhasználói teszt támogatása: pl. fájlok betöltése, tesztadatok előállítása, problémák elhárítása.
- Hibajavítások telepítése, és a felhasználók felé jelzése.
- Rendszergazdai tesztek végrehajtása, dokumentálása.

A tesztelő felhasználó feladatai:

- A Tesztelési forgatókönyv megismerése és betartása a tesztlap kitöltése során.
- Tesztesetek tervezése.
- Tesztadat igény jelzése a rendszergazdák felé.
- Felhasználói teszt végrehajtása, annak értelemszerű dokumentálása a tesztlapon.

Tesztelési forgatókönyv

A Tesztelési forgatókönyv végleges változata tartalmazza:

- a teszt stratégiát
- a tesztelési tervet és teszteseteket (Tesztlap)
- a tesztelési környezetre vonatkozó elvárásokat

A tesztelés folyamata

A tesztelendő funkciók listájának tartalmaznia kell:

- az új fejlesztés minden végrehajtható funkcióját
- a fejlesztés által érintett, már meglevő funkciókat

A tesztelendő funkciókat és azok tesztjének ütemezését, egymásutániságát – a fejlesztő bevonásával – a témafelelős és felhasználó terület közösen határozza meg, és a Tesztelési forgatókönyvben dokumentálja azt. A szabályzat 4. számú melléklete tartalmazza, hogy az egyes teszt fajtákat milyen szerepkörökben kell elvégezni, valamint azt, hogy az egyes teszt fajták logikailag hogyan kapcsolódnak egymáshoz.
Az egyes végrehajtandó funkciók különböző módokon hajthatóak végre, emiatt tesztesetként minden lehetőséget definiálni kell. A tesztesetek összeállításakor meg kell határozni az elvárt eredményt is. A tesztelési tevékenység során az elfogadott Követelményspecifikációhoz, illetve Koncepciótervhez kell mérni az új rendszert. Az egyes funkcióknak az ebben leírt módon kell működniük.
A biztonsági követelményekkel kapcsolatos teszt megtervezése és a tesztesetek kidolgozása az adat biztonsági felelős feladata.
Minden tesztelendő funkcióról tesztlapot kell kiállítani. Amennyiben az adott funkció tesztlapjára nem fér rá az összes teszteset, úgy további tesztlapokat kell kiállítani. Tömeges teszteset esetén elfogadható a tesztesetek táblázatos formában történő csatolása. A tesztlapokról tesztlap összesítőt kell vezetni, ahol a tesztlap száma és neve mellett a tesztlap státuszát is fel kell tüntetni.

A tesztlap lehetséges státuszai:

- tesztelendő
- tesztelés alatt
- hibajavítás alatt
- újratesztelés alatt
- kész

Adott funkció és teszteset hibáját a felhasználó a tesztlapon rögzíti. A hibát körültekintően dokumentálni kell abból a célból, hogy a fejlesztő által újra előállítható legyen. Ennek keretében rögzíteni kell az alábbi adatokat:

- tesztrendszer neve/kódja
- hibás funkció neve
- tesztelő neve/elérhetősége
- tesztadatok
- elvárt eredmény
- eltérés az elvárt eredménytől
- hiba vélelmezett oka, ha vélelmezhető

A hibás funkció tesztlapját, a hiba kijavítása céljából vissza kell juttatni a fejlesztőnek. A fejlesztő a hiba kijavítása után – a fejlesztői tesztet követően – visszaadja a funkció tesztlapját felhasználói tesztre.

Tesztelési jegyzőkönyv

Amennyiben az adott fejlesztés vonatkozásában tesztelési forgatókönyv készült, akkor az elvégzett tesztről Tesztelési jegyzőkönyvet kell készíteni. A Tesztelési jegyzőkönyv tartalmaz egy összesítő lapot, amelyen az alábbi adatokat kell szerepeltetni:

- a tesztelés helyét
- a tesztelés időpontját
- a tesztelés célját

- a tesztelést vezető adatait
- a tesztelésbe bevont munkatársak, partnerek adatai, feladataik és felelősségi körük
- a teszt során felmerült hibákat, problémákat
- a teszt eredményét
- a teszt igazolását (hitelesítés)

A Tesztelési jegyzőkönyvhöz csatolni kell a felhasználó által aláírt tesztlapokat. Tesztelési forgatókönyv hiányában a tesztelést végző felhasználó által igazolt Tesztelési jegyzőkönyvet csatolni kell az üzembe helyezés megindításához.
A teszt lezárásáról a tesztfelelős a Tesztelési jegyzőkönyvben, illetve Tesztelési jegyzőkönyv hiányában a tesztelést végző felhasználó a tesztlap(ok)on aláírásával nyilatkozik, amelyben kiemelten szerepel, hogy a rendszer a Követelményspecifikációnak megfelelően működik, a tesztelést az adott felhasználó elvégezte, és a tesztet sikeresnek nyilvánította, illetve nem merült fel olyan hiba, ami az éles üzemi működést gátolja. Az éles üzemi működést nem akadályozó hibákról a Tesztelési jegyzőkönyvben jegyzéket kell felvenni, megjelölve a hibajavítás elvárt határidejét.

A tesztelési eljárás termékei

- Tesztelési forgatókönyv (adott esetben)
- Tesztlap/lapok

- Tesztelési környezet
- Tesztelők oktatása
- Tesztelési jegyzőkönyv, ennek hiányában csak tesztlap/lapok
- Dokumentált teszthibák
- Elfogadott telepítési teszt

13.6 A migráció előkészítése

Migrációs forgatókönyv

A Migrációs forgatókönyv első verziójában ki kell térni:

- a migrációs stratégiára vonatkozó elképzelésekre
- a migráció terjedelmének meghatározására
- a felelősségek megosztására
- az adattisztítás és konverzió módszerének meghatározására
- a migráció módjának rögzítésére
- a migrációs tesztek számának és céljának meghatározására
- a migráció ellenőrzésének eljárásaira

A migráció részletes tervezése

A Migrációs forgatókönyvet ki kell egészíteni a migráció konkrét végrehajtására vonatkozó elképzelésekkel:

- adatforrások meghatározása
- adattisztítás szükségességének meghatározása
- adatkinyerő, adatkonvertáló, adatbetöltő eljárások meghatározása
- migráció lépéseinek ütemezése
- migráció tesztelésének ütemezése
- migráció tényleges végrehajtása

- a migráció sikertelensége esetén alkalmazandó visszagörgetési lépések leírása, amelyek segítségével visszaállítható az eredeti, vagy azzal funkcionálisan megegyező állapot
- annak a legkésőbbi időpontnak a megjelölése, amikor a visszaállítást el kell rendelni
- a migrációban résztvevők nevesítése, feladataik és felelősségi körük kitűzése

Az adattisztítás végrehajtása a Migrációs tervben megfogalmazottak szerint történik.
Meg kell valósítani, szükség esetén ki kell fejleszteni az adatkinyerő, adatkonvertáló, illetve az adatbetöltő eljárásokat. Az adatkinyerő, adatkonvertáló, adatbetöltő eljárások fejlesztői tesztelését el kell végezni (csak az eljárásokét).
El kell végezni az adatmigrációs eljárások tesztelését, amelynek módja lehet a teljes adatbázis áttöltése, vagy annak egy előre meghatározott mennyisége (pl. az adatok 10%-a).

A migráció előkészítés termékei:

- Migrációs forgatókönyv
- Adatkinyerési eljárások
- Adatkonvertáló eljárások
- Adatbetöltő eljárások
- Letesztelt migrálási folyamat
- Teszt migrálás
- Ellenőrzött migrált adatok

13.7 Az üzembe helyezés előkészítése

Az üzembe helyezés elökészítése során a témavezető megtervezi, és a rendszergazdával engedélyezteti az átállási tervet, melyben meg kell fogalmazni

- az átállás feltételrendszerét és annak lépéseit (alkalmazások telepítése, adatbázis telepítése, adatmigráció stb. szükség szerinti ütemezésben)
- a mentési, ellenőrző és döntési pontokat
- a kommunikációs lépéseket (beleértve a szabályozással kapcsolatos feladatokat vagy pl. a túlmunka elrendelését is)
- a régi rendszer leállításának lépéseit, valamint
- a visszaállási tervet.

Az üzembe helyezéshez kapcsolódó folyamatot az Informatika Ügyrendje tartalmazza.
Az üzemeltetésre történő átadás átadás-átvételi jegyzőkönyv alapján történik. Az átadás-átvételi jegyzőkönyv tartalma és részletessége minden esetben az adott fejlesztési feladat függvénye. Az átadás-átvételi jegyzőkönyv tartalmazza a készre jelentési nyilatkozatot, valamint igazolja a Tesztelési jegyzőkönyv (ennek hiányában a tesztlap/lapok), a Felhasználói kézikönyv (vagy a meglévő kiegészítése) és Üzemeltetői kézikönyv (vagy a meglévő kiegészítése) című dokumentációk elkészültét.
Amennyiben értelmezhető, az átadás-átvételi jegyzőkönyv tartalmazza a berendezések gépkönyvei, garancia levelek, gyári számok, valamint gyártói támogató rendszerhez/rendszerekhez történő hozzáférést biztosító azonosítók átadását, elérhetőségét.
Az üzembe helyezés alapkövetelménye, hogy az nem járhat üzemidőben történő leállással, vagy az éles üzem veszélyeztetésével.

Üzemeltetésre történő átadás – amennyiben szükséges – kizárólag az üzemeltetéssel megbízott személyzet megfelelő oktatása után történhet meg. Az oktatások során törekedni kell a gyártói hivatalos, minősítést nyújtó tanfolyamok elvégzésére.

Az üzembe helyezés előkészítésének termékei:

- Jóváhagyott Telepítési csomag adathordozón
- Tesztelési jegyzőkönyvek vagy tesztlapok
- Üzemeltetési Útmutató, Felhasználói Kézikönyv
- Rendszerterv, a rendszer forráskódja a kapcsolódó fejlesztési dokumentációkkal (ha a szállítói szerződés ezt tartalmazza)
- Engedélyezett átállási terv

13.8 Oktatás

Az oktatás megtervezése és koordinációja, az oktatási anyagok elkészítése, az oktatás megszervezése, az aktív kommunikáció, az oktatás lebonyolítása és számonkérése a témafelelős felelőssége, amelyben a külső vállalkozó – a vele kötött szerződésben foglaltak szerint – közreműködik. Az oktatáshoz szükséges infrastruktúra biztosításáról a témafelelős vagy az általa megbízott munkavállaló gondoskodik.
Az oktatás előkészítése a többi, fejlesztéssel összefüggő feladattal párhuzamosan is kezdődhet.
Az oktatási tevékenység kezdésének és befejezésének időpontját a témafelelős dönti el. Az oktatást – a tesztelő felhasználók felkészítésével – általában a tesztelés indítása előtt kell megkezdeni és az átállás előtt kell befejezni.

Az oktatási tervben kell meghatározni:

- az oktatandók körét (üzemeltetés, felhasználó, kulcsfelhasználó, vezető)
- az oktatás típusát
- tematikáját
- időtartamát
- ütemezését
- az oktatással kapcsolatos logisztikai (terem, gépek, stb.) igényeket
- az oktatáshoz felhasználni kívánt tananyagokat
- az oktatás visszamérésének szükségességét (igen/nem) és ha kell, annak módját

Az oktatás előkészítésével összefüggő feladatok:

- az oktatás segédeszközeinek biztosítása
- az oktatás számítástechnikai infrastruktúrájának kialakítása
- az oktatandó rendszer telepítése
- rendszertervben meghatározott jogosultságok beállítása az oktatandó felhasználóknak megfelelően
- telepített adatbázis feltöltése az oktatáshoz szükséges adattartalommal
- kliens oldal előkészítése
- a visszaméréshez tesztlapok/kérdőívek előállítása, sokszorosítása és/vagy interjúk, számítógép előtti vizsgák, kérdőív kitöltések ütemezése stb.

Az oktatási anyagoknál kiemelt figyelmet kell fordítani a szerzői jogokra.

Az oktatás folyamatának termékei:

- Oktatási terv
- Oktatási anyagok
- Jelenléti ívek, jegyzőkönyvek
- Visszamérési eredmények

- Értékelés

13.9 A fejlesztések dokumentációs rendje

Minden fejlesztésnél kötelezően alkalmazandó dokumentumok:

- követelményspecifikáció
- koncepcióterv
- rendszerterv
- tesztelési jegyzőkönyv
- telepítési útmutató
- felhasználói kézikönyv

A fejlesztéseknél alkalmazható dokumentumok teljes körét (fentieken kívül pl. teszt forgatókönyv, migrációs forgatókönyv, üzemeltetési útmutató stb.) az szabályzat 3. számú melléklete tartalmazza. Az adott fejlesztési feladatnál kötelezően alkalmazandó további dokumentumokra a témafelelős és az igénylő képviselője a követelményspecifikációban tesz javaslatot.
Amennyiben a fejlesztés már meglévő rendszer módosítását foglalja magában, úgy a rendszer dokumentációját aktualizálni kell, különös tekintettel:

- a Koncepciótervre, a részletes tervre és implementációs tervre
- a telepítési útmutatóra
- az üzemeltetési és felhasználói kézikönyvre

A fejlesztés dokumentációs rendjének betartásáért a témavezető felelős.

14. Záró rendelkezés

Ez a szabályzat 2020. május 1-én lép hatályba.

A KASZÓ Zrt -nél az adatvédelmi felelősnek kell gondoskodni arról, hogy a szabályzatot valamennyi érintett megismerje, és ennek tényét a szabályzathoz csatolt íven aláírásával igazolja.

1. számú melléklet

Teljesítésigazolás

Dátum	Rendelt eszköz, szolgáltatás	Ki rendelte	Átvette

Kaszó,

....

Vállalkozó Jóváhagyta