1. Alkalmazási terület

1.1. Jelen Általános Információ-technológiai Feltételek (továbbiakban **„ÁIF”**) az AUDI HUNGARIA Zrt., mint megrendelő (a továbbiakban úgy is mint **„Megrendelő”** vagy **„AH”**) által igénybe vett információtechnológiai vagy kommunikációtechnológiai (továbbiakban: **„IT”**) szolgáltatásokra irányadóak. Egyéb szolgáltatások és szerződések tekintetében is megfelelően alkalmazandóak a jelen ÁIF-ben foglaltak, amennyiben **Partner** a teljesítés során hozzáférést kap a Megrendelő IT rendszereihez, vagy bármilyen egyéb módon Megrendelő IT rendszereivel dolgozik és hozzáfér a Megrendelő információihoz, adataihoz.

2. A Szerződés teljesítése

2.1. A **„Szerződés”** fogalmának meghatározása a Megrendelő Általános Beszerzési Feltételei (továbbiakban: **„ÁBF”**) I.7. pontjában található.

2.2. Ha a Szerződés tárgya valamely eredmény létrehozása, Partner vállalja, hogy a teljesítést megfelelő módon dokumentálja, és igény esetén a szolgáltatás állásáról elvárásainak megfelelően tájékoztatja a Megrendelőt.

2.3. Amennyiben Partner munkatársa Megrendelő IT rendszereihez hozzáférést kap, a munkatárs azonosító adatainak kezelésére és felhasználására az AUDI AG vagy a VOLKSWAGEN AG egy kapcsolt vállalkozásánál (továbbiakban: Konszernvállalat(ok)) kerül sor. Partner köteles az érintett munkatársaitól a fentiek szerinti adatkezeléshez történő előzetes írásbeli hozzájárulást beszerezni, és Megrendelő erre vonatkozó igénye esetén, ezen dokumentumokat részére bemutatni; ezen kötelezettségeinek megszegéséért kizárólagosan Partner felel.

2.4. A Szerződésben foglalt eltérő rendelkezés hiányában Partner valamennyi szükséges infrastrukturális szolgáltatást további költségigény nélkül teljesít Megrendelő részére. Infrastrukturális szolgáltatásnak minősül valamennyi előkészítő szolgáltatás, mely szoftver- és/vagy hardverszolgáltatás és/vagy alkalmazás előkészítéséhez szükséges (például rendszerek tervezése, kialakítása, felépítése vagy telepítése, IT munkahely).

2.5. Megrendelő erre vonatkozó igénye esetén Partner támogató szolgáltatásokra (support) is ad ajánlatot a szokásos piaci feltételeknek megfelelően. Támogató szolgáltatásnak minősül valamennyi szoftver- és/vagy hardver szolgáltatást és/vagy alkalmazást és/vagy infrastrukturális szolgáltatást kísérő szolgáltatás (például oktatás, tanácsadás, optimalizálás, karbantartás/megóvás).

3. Licencfeltételek

3.1. Open Source szoftverek

3.1.1. A Szerződés teljesítése során nyílt forráskódú szoftver alkalmazása csak a Megrendelő előzetes, írásbeli hozzájárulásával lehetséges.

3.1.2. Amennyiben Partner a Megrendelő előzetes írásbeli hozzájárulása nélkül alkalmaz nyílt forráskódú szoftvert, úgy Megrendelő igénye esetén köteles a nyílt forráskódú szoftvert egy egyenértékű zárt forráskódú szoftverrel helyettesíteni.

3.1.3. Partner teljes körűen mentesíti a Megrendelőt harmadik személy azon követelései és az azokhoz kapcsolódó költségek alól, melyek nyílt forráskódú szoftverek a Megrendelő előzetes, írásbeli hozzájárulása nélküli, Partner általi alkalmazásából erednek.

3.2. Click Wrap-/ Shrink Wrap-licenc

3.2.1. Click Wrap-/ Shrink Wrap licencfeltételek alkalmazását Megrendelő kizárja.

3.3. Licenc-auditok

3.3.1. Amennyiben Partner írásban, megfelelő indokolással közli a Megrendelővel, hogy álláspontja szerint Megrendelő megsérti valamely általa átadott szoftver felhasználási jogának szabályait, úgy az érintett szoftverrel kapcsolatban Megrendelő licenc-auditot folytat le (a felhasználási jogra vonatkozó szabályok betartásának megvizsgálása), és írásban tájékoztatja Megrendelő a Partnert a licenc-audit eredményéről.

4. IT-biztonsági elvárások

4.1. Partner a Szerződés teljesítése során a legfrissebb ISO 9001 szabványnak és az ISO 27000 szabványcsaládnak, ill. a tudomány és a technika jelen állásának megfelelő adat- és rendszervédelmi követelményeket biztosít, így különösen biztosítja Megrendelő rendszereit a technika jelen állásának megfelelően, harmadik személy illetéktelen hozzáférése (pl.: hacker támadások), valamint nem kívánatos adatátvitel (pl.: spam) ellen.

4.2. A szolgáltatások teljesítése során Partner köteles betartani Megrendelő információbiztonsági elvárásait, melyek megtalálhatóak a jelen ÁIF törzsszövegében és mellékleteiben, ill. az adott Szerződésre vonatkozó speciális dokumentumokban.

4.3. Partner köteles az IT-biztonsági elvárások maradéktalanul betartása mellett köteles a teljesítésbe bevont közreműködőket (ideértve különösen, de nem kizárólagosan: munkavállalók, alvállalkozók, megbízottak, egyéb harmadik személyek) a Megrendelő rendszereihez való hozzáférést megelőzően tartalmukról tájékoztatni. A Partner által a teljesítésbe bevont, információkkal dolgozó személyeknek az AH biztonsági oktatásokat és tudatossági képzéseket biztosít, melyeken ezen személyeknek kötelezően részt kell venniük. Az AH

információit is kezelő szolgáltatások esetén Partnernek dokumentáltan ki kell jelölnie egy információbiztonsági kérdésekkel foglalkozó kapcsolattartó személyt (a szolgáltatás volumenétől függően dedikált vagy nem dedikált). A szállítóknak ki kell jelölniük, dokumentálniuk kell, és dokumentáltan meg kell küldeniük az AH számára az adott szolgáltatásban részt vevő, és AH információkhoz hozzáférő személyek nevét és adatait (figyelembe véve a vonatkozó adatvédelmi szabályokat is), akik időszakosan vagy folyamatosan ezen adatokkal kapcsolatba kerülhetnek.

4.4. A szolgáltatások átmeneti időszakának (pl. tranzíciós időszak) biztonsági követelményeit Megrendelő külön kezeli a folyamatos szolgáltatási időszaktól; ezen időszakokban eltérő biztonsági intézkedéseknek, ellenőrzési módszereknek kell Partnernek megfelelnie.

4.5. A biztonsági incidensek gyors, hatékony és egységes kezelése érdekében Megrendelő eseménykezelési eljárásai Partner részéről kötelezően betartandóak az adott szolgáltatás elindulásától kezdődően. Partner köteles az információbiztonsági incidensekről minden esetben haladéktalanul írásbeli értesítést küldeni Megrendelő részére.

4.6. Partner köteles dokumentálni és haladéktalanul írásban értesíteni Megrendelőt valamennyi olyan változásról, mely a Megrendelőnek nyújtott szolgáltatást érintheti, így különösen, de nem kizárólagosan:

- változás a Partner közreműködőinek körében;
- új technológia, termék vagy verzió használata;
- a szolgáltatásnyújtás helyének megváltoztatása, fizikai környezetben történő egyéb változás;
- szolgáltatásnyújtás harmadik személynek, mely érintheti a Megrendelőnek nyújtott szolgáltatást.

4.7. Megrendelő erre vonatkozó igénye esetén Partner köteles benyújtani a nála elvégzett olyan információbiztonsági ellenőrzésekről szóló írásbeli jelentéseket, melyek összefüggésben vannak a Megrendelőnek nyújtott szolgáltatások biztonsági aspektusaival.

4.8. Valamennyi Partner köteles a jelen ÁIF 1. számú mellékletében (IT-Biztonsági eljárási irányelvek külsős munkatársak, partnercégek számára) foglaltakat betartani.

4.9. Minden IT-üzemeltetői szolgáltatást nyújtó Partner köteles a jelen ÁIF 2. számú mellékletében (IT-biztonsági irányelvek rendszerüzemeltetők és adminisztrátorok részére) foglaltakat betartani.

4.10. Minden szoftverfejlesztési szolgáltatást nyújtó Partner köteles a jelen ÁIF 3. számú mellékletében (IT biztonsági eljárási irányelvek rendszerfejlesztők részére) foglaltakat.

5. Revíziós klauzula

5.1. Partner Megrendelőnek és/vagy külső partnereinek és/vagy a VOLKSWAGEN AG konszernrevíziójának bármikor gyakorolható jogot biztosít, amely alapján előzetes bejelentést követően:

- **a Partner és Megrendelő között történt üzleti eseményekre vonatkozó valamennyi adatot;**
- **Partner és/vagy közreműködői IT-biztonsági dokumentumait (szabályzatok, munkautasítások stb.) és folyamatait a Megrendelő IT-biztonsági elvárásainak betartását;**

Partnernél, ill. közreműködőinél megtekinthetik és megvizsgálhatják.

6. Egyéb

6.1. Amennyiben jelen ÁIF valamely rendelkezése ellentétes az ÁBF-el, a jelen ÁIF-ben foglaltak elsőbbséget élveznek.

6.2. Hatálybalépés időpontja: 2019.05.01. mely időponttal hatályát veszti a 2018.09.24. napján kiadott Általános IT Előírások.

AUDI HUNGARIA Zrt.
Székhely: 9027 Győr, Audi Hungária út 1.
Győri Törvényszék Cégbírósága
Cg. 08-10-001840

Adószámok:
Magyar adószám: 23391475-2-08
Magyar közösségi adószám: HU23391475

Bankszámlaszámok:
Commerzbank Budapest
HUF: 14220108-42431006-00000000
IBAN: HU47 14220108 42431006 00000000
(SWIFT: COBAHUHXXXX)

Commerzbank Ingolstadt
EUR: 72140052-192247500
IBAN: DE31 7214 0052 0192 2475 00
(SWIFT: COBADEFF721)

IT-biztonsági eljárási irányelvek külső partnerek számára

Verzió: 5.0 (2018.05.11.)
Kiadó: IT-biztonság
Szabályozás száma: 08 Felsőszintű szabályozás

Érvényességi kör

Az eljárási irányelvek az AUDI HUNGARIA Zrt. (továbbiakban úgy is, mint „Audi Hungaria”, ill. „Megbízó”) számára szolgáltatást végző partnerekre (továbbiakban úgy is mint „Megbízott”) vonatkoznak.

Tartalom

1. Cél 5
2. Szabályozások 5
2.1. Az információbiztonság szervezése 5
2.1.1. Belső szervezés 5
2.1.2. Külső kapcsolatok 6
2.2. A szervezet saját értékeinek a kezelése 6
2.2.1. Szabályozások az osztályozásra 6
2.2.2. Bizalmasság 6
2.2.3. Integritás 8
2.2.4. Visszakövethetőség 9
2.2.5. Rendelkezésre állás 9
2.2.6. Információk azonosítása és kezelése 10
2.3. Személyes biztonság 12
2.4. Fizikai és környezeti biztonság 12
2.5. Üzemi- és kommunikációmanagement 12
2.5.1. Rosszindulatú szoftverek és mobil programkódok elleni védelem 12
2.5.2. Biztonsági mentés 13
2.5.3. Tároló és adathordozó médiák kezelése 13
2.5.4. Információcsere 13
2.6. Hozzáférések ellenőrzése 13
2.6.1. Üzleti követelmények a hozzáférések ellenőrzésére 13
2.6.2. A felhasználók felelőssége 14
2.6.3. Hozzáférések ellenőrzése hálózatok esetén 15
2.6.3.1. A hálózati szolgáltatások használatára vonatkozó szabályok 15
2.6.3.2. Az eszközök azonosítása a hálózaton 16
2.7. Információbiztonsági események kezelése 16
2.8. Előírások betartása 16
2.9. Eltérések 16
3. További dokumentációk, mellékletek 17
3.1. Hivatkozások 17

1. Cél

A Megbízó információinak és/vagy IT eszközeinek (személyi számítógép, munkaállomások ideértve a mobil számítógépeket, mint Notebook, okostelefon, Tablet PC-k, stb.) kezelésével kapcsolatos, a külsős partnerekre érvényes IT biztonsági szabályozásokat ezen eljárási irányelvben fogalmazza meg. Megbízott a teljesítés során köteles betartani, ill. a munkavállalóival, közreműködőivel, teljesítési segédeivel betartatni a jelen irányelvben foglalt előírásokat.

Az IT-biztonsági eljárási irányelvek az információk bizalmasságának, integritásának, rendelkezésre állásának és követhetőségének védelmét, valamint a vállalat és minden olyan természetes és jogi személy jogainak és érdekeinek védelmét szolgálja, akik üzleti kapcsolatban állnak az AUDI HUNGARIA Zrt-vel, illetve a társaságnál dolgozókkal.

2. Szabályozások

2.1. Az információbiztonság szervezése

2.1.1. Belső szervezés

A rendelkezésre bocsátott hardverek és szoftverek beszerzése és installálása kizárólag a Megbízó érintett területeivel [Ld. 3.1. sz. fejezet 1.] együttműködve történik, az érvényben lévő engedélyezési eljárások alapján.

A rendelkezésre bocsátott hardverek és szoftverek használatával kapcsolatban az Audi Hungaria szabályozásai és üzemi megállapodásai érvényesek [Ld. 3.1. sz. fejezet 2.].

Az IT eszközök kinyitását és a hardver elemek módosítását (pl. merevlemezek, memóriaelemek ki-/beszerelése), valamint a biztonsági beállítások (pl. böngésző-beállítások) kézi módosítását kizárólag Megbízó felelős területei [Ld. 3.1. sz. fejezet 3.] végezhetik. (Az okostelefonok használatára vonatkozó korlátozásokat tilos eltávolítani (jailbreak)).

A Megbízó programjainak használata vagy utólagos módosítása csak akkor megengedett, ha azt a felelős területek engedélyezték [Ld. 3.1. sz. fejezet 3.].

A rendelkezésre bocsátott IT eszközökön tilos olyan további ügyfelek adatait feldolgozni, akik nem tartoznak a Megbízóhoz.

A saját használatú, azaz privát IT eszközöknek a vállalat területére való bevitelének engedélyezésére az Audi Hungaria szabályai vonatkoznak.

Az Audi Hungaria adatait el kell választani a nem az Audi Hungariához tartozó további ügyfelek adataitól.

A személyes és a titoktartás alá eső adatok tárolására, valamint egyéb feldolgozására és felhasználására az Audi Hungaria szabályozásai és üzemi megállapodásai érvényesek [Ld. 3.1. sz. fejezet 4.].

Tilos a magáncélra vásárolt programok és adatok szolgálati célokra történő felhasználása.

Nem megengedett a vállalat saját szoftvereinek és adatainak privát IT eszközökön és adathordozókon történő használata.

Tilos Megbízó saját szoftvereinek és adatkezelésében lévő személyes és más adatok nem engedélyezett tárolóeszközökön (pl. nem engedélyezett fájlszolgáltatások / Internetes cloud) történő használata. (pl.: SkyDrive, Google drive, Dropbox, stb.) Ezzel kapcsolatban további egyeztetést az alábbi email címen kezdeményezhet: it-sicherheit kukac audi pont hu

2.1.2. Külső kapcsolatok

A Megbízó IT eszközeinek és adatainak partnercégek munkatársai általi használatához Megbízó illetékes szakterületének kifejezett hozzájárulása szükséges. A szakterületnek jogában áll bármikor megtiltani a használatot (különösen visszaélés, jogszabályi előírások be nem tartása esetén).

A partnercégek engedéllyel rendelkező munkatársainak körét a Megbízó illetékes szakterületének kell meghatároznia, és törekedni kell annak minimalizálására.

A partnercégek munkatársait az ügyvezetésüknek kötelezniük kell a titoktartásra. Ez megfelelő módon érvényes a partnercégek alvállalkozóinak munkatársaira is. A megbízást adó szakterület számára betekintést kell biztosítani ezekbe a megállapodásokba.

Az adatok harmadik személy számára történő átadása alapértelmezetten tilos, kivéve, ha ezt a Megbízó illetékes szakterülete írásban engedélyezi.

2.2. A szervezet saját értékeinek a kezelése

2.2.1. Szabályozások az osztályozásra

Az adatgazda felelős az információk bizalmasságának, rendelkezésre állásának, integritásának és visszakövethetőségének besorolásáért.

Az adatok besorolásáról a Megbízó terület IT Biztonsági megbízottjánál kaphat információkat.

2.2.2. Bizalmasság

Azokat az információkat, melyeket a Megbízó nem a nyilvánosság számára szánt, csak az erre jogosultak számára szabad hozzáférhetővé tenni.

Az információk csoportosításának alábbi szintjeit határozzuk meg a bizalmassággal kapcsolatos követelmények alapján:

Besorolás	Definíció
Nyilvános	Semmilyen korlátozás alá nem eső információk, amelyeket pl. a vállalat jelentet meg újságokban vagy az Interneten. A vállalati információk nyilvános felhasználásához az illetékes területek [Ld. 3.1. sz. fejezet 5.] hozzájárulása szükséges.

	Példák: sajtóközlemények, ügyfeleknek szánt termékkatalógusok
Belső	Csak belső használatra és nem a nyilvánosságnak szánt információk. A bizalmasság elvesztése következményekkel járhat, de ezek csak kisebb mértékűek, pl.: • kevésbé valószínű egyes személyek vagy szervezetek kártérítési igénye. Példák: szolgálati kommunikációs adatok (pl.: telefonszámok, email-címek), munkavédelmi előírások, munkarend.
Bizalmas	Olyan információk, amelyek erre fel nem jogosított személyek általi ismerete vagy visszaélésszerű továbbadása, illetve felhasználása veszélyeztetheti a termék- és projektcélokat, éppen ezért ezeket csak korlátozott, erre feljogosított személyek köre számára szabad hozzáférhetővé tenni. A bizalmasság elvesztése valószínűsíthetően következményekkel jár, és ezek mérhetők is, pl.: • ügyfelek elvesztése, • értékesítési mutatók / forgalom csökkenése, • egyes személyek vagy szervezetek kártérítési igénye. Példák: a szolgálati kommunikációs adatokon túlmenő, személyes adatok (pl. béradatok), költségvetési tervezetek, revíziós jelentések.
Titkos	Olyan információk, amelyek erre fel nem jogosított személyek általi ismerete vagy visszaélésszerű továbbadása vagy felhasználása tartósan veszélyeztetheti a vállalati célok elérését, ezért ezeket csak nagyon korlátozott formában szabad továbbadni és szigorúan ellenőrizni kell. A bizalmasság megsértése jelentős kihatással van a vállalat külső megítélésére / megjelenésére és / vagy gazdasági következményekkel jár(hat), pl.: • jelentős számú ügyfél elvesztése, • értékesítési mutatók / forgalom jelentős csökkenése, • számos személy vagy szervezet jelentős mértékű kártérítési igénye, • kizárás bizonyos piacokról, • negatív hatások a hírnévre. Példák: személyes adatok speciális típusai, ciklus-tervek, igazgatósági előterjesztések, vállalati stratégiával kapcsolatos tervek, új prototípusok design-képei.

2.2.3. Integritás

Biztosítani kell az információk hibátlan feldolgozását, és meg kell óvni őket az illetéktelen módosítástól.

Az információk csoportosításának alábbi szintjeit határozzuk meg az integritással kapcsolatos követelmények alapján:

Besorolás	Definíció
Alacsony	Az integritás megsértése nincs belátható hatással a vállalat üzleti tevékenységére vagy külső hatására / megjelenésére.
Közepes	Az integritás megsértése csak minimális hatással van a vállalat üzleti tevékenységére és / vagy csak minimális hatással van a vállalat külső megítélésére. Következmények lehetségesek, de ezek csak kisebb mértékűek, pl.: • minimális késedelem a munkafolyamatokban, • a hibák / zavarok nincsenek hatással a munkaeredményekre (nincs termeléskiesés), • a döntések nem szenvednek hátrányt, • kevésbé valószínű egyes személyek vagy szervezetek kártérítési igénye. Példák: telephelytervek, szervezeti diagramok, egyes belső telefonszámok.
Magas	Az integritás megsértése érezhető hatással van a vállalat üzleti tevékenységére és / vagy külső hatására / megjelenésére. Valószínűsíthetően következményekkel jár, és ezek mérhetők is, pl.: • ügyfelek elvesztésének lehetősége, • az értékesítési mutatók romlásának és a forgalom csökkenésének valószínűsége, • jelentős késedelem a munkafolyamatokban, • a hibák / zavarok érezhető hatással vannak a munkaeredményekre (nagyfokú termeléskiesés), illetve néhány szolgáltatási folyamat kiesik, • hátrányos / hibás döntések valószínűsége, • egyes személyek vagy szervezetek kártérítési igényének valószínűségének megnövekedése. Példák: JIT-megrendelések, sajtóközlemények, az Internetes megjelenés tartalmai, a termelésirányításra vonatkozó adatok
Nagyon magas	Az integritás megsértése jelentős hatással van a vállalat üzleti tevékenységére és / vagy külső megítélésére, és megfelelő gazdasági következményekkel is jár, pl.: • jelentős számú ügyfél elvesztése, • számos személy vagy szervezet kártérítési igénye, • értékesítési mutatók / forgalom jelentős csökkenése,

	• kizárás bizonyos piacokról, • jelentős késedelem a munkafolyamatokban, • a hibák / zavarok jelentős hatással vannak a munkaeredményekre (nagyon nagyfokú termeléskiesés), illetve több szolgáltatási folyamat kiesik, • hátrányos/ hibás döntések. Példák: pénzügyi jelentéskészítés (pl. éves mérleg), szabadalmi dokumentumok, kriptográfiai kulcsok, bérelszámolás.

2.2.4. Visszakövethetőség

A védett információkhoz való hozzáférésnek és a tranzakciók végrehajtásának visszakövethetőnek kell lennie.

Az információk csoportosításának alábbi szintjeit határozzuk meg a visszakövethetőséggel kapcsolatos követelmények alapján:

Besorolás	Definíció
Alacsony	Nincsenek követelmények a valódisággal, ellenőrizhetőséggel és bizalmassággal kapcsolatban.
Közepes	A módosítási hozzáférések esetén nyomon követhetőnek kell lennie a módosítás típusának (hozzáadás, törlés, módosítás), a végrehajtó személyeknek és az időpontoknak.
Magas	A módosítási hozzáférés esetén nyomon követhetőnek kell lennie a módosításoknak (beleértve a módosítások előtti állapotot), a végrehajtó személyeknek és az időpontoknak.
Nagyon magas	Az olvasási és módosítási hozzáférések esetén nyomon követhetőnek kell lennie a módosításoknak (beleértve a módosítások előtti állapotot), a végrehajtó személyeknek és az időpontoknak.

2.2.5. Rendelkezésre állás

Az információkat egy megállapodás szerinti időtartam során rendelkezésre kell bocsátani.

Az információk csoportosításának az alábbi szintjeit határozzuk meg a rendelkezésre állással kapcsolatos követelmények alapján:

Besorolás	Definíció
Alacsony	Az IT rendszer kiesés, vagy nem megfelelő válaszidő miatt 95%-nál kisebb mértékben lehet elérhető anélkül, hogy szignifikáns kár keletkezne (anyagi kár, vagy a vállalat image-ét érintő kár). Példa: Intranetes alkalmazás a munkatársaknak szóló általános információkkal

Közepes	Az IT rendszernek a kiesésre vagy nem megfelelő válaszidőre vonatkozóan 95%-ban elérhetőnek kell lennie. Ezt követően szignifikáns kár keletkezik (anyagi kár, vagy a vállalat image-ét érintő kár). Példa: pályázói portál.
Magas	Az IT rendszernek a kiesésre vagy nem megfelelő válaszidőre vonatkozóan 98%-ban elérhetőnek kell lennie, egyéb esetben szignifikáns kár keletkezik (anyagi kár, vagy a vállalat image-ét érintő kár). Példák: bérelszámolás, könyvelés.
Nagyon magas	Az IT-rendszernek a kiesésre vagy nem megfelelő válaszidőre vonatkozóan 99%-ban elérhetőnek kell lennie, egyéb esetben szignifikáns kár keletkezik (anyagi kár, vagy a vállalat image-ét érintő kár). Példák: olyan IT rendszer, amelynek kiesése azonnali termelésleállást von maga után. Szignifikáns kárnak számít például: • ügyfelek elvesztése, • számos személy vagy szervezet kártérítési igénye, • értékesítési mutatók / forgalom jelentős csökkenése, • kizárás bizonyos piacokról, • a hibák / zavarok jelentős hatással vannak a munkaeredményekre, illetve több szolgáltatási folyamat kiesik (nagyon nagyfokú termeléskiesés).

2.2.6. Információk azonosítása és kezelése

Az információkhoz csak a jogosult személyek körének szabad hozzáférni. Ez csak a megállapodás szerinti feladat keretében, valamint a meglévő szabályozások betartásával lehetséges. Ennek során a „szükséges ismeret” („need-to-know”) alapelvét kell követni.

Az információkat teljes élettartamuk során aktuális bizalmassági besorolásuknak megfelelően kell védeni az illetéktelen hozzáférésektől. Az alábbi szabályozások érvényesek:

Besorolás	Előírások a kezeléssel kapcsolatban
Nyilvános	• Jelölés: nincs. • Sokszorosítás és továbbadás: nincsenek korlátozások. • Tárolás: nincsenek korlátozások. • Törlés: nincsenek korlátozások. • Selejtezés: nincsenek korlátozások.
Belső	• Jelölés: nincs (vagy „Belső”).

	• Sokszorosítás és továbbadás: csak a jogosult konszern munkatársak és a munka- vagy alkalmazási területen jogosult harmadik személyek részére. • Tárolás: illetéktelen betekintéstől óvni kell. • Törlés: a rendszeroldalon meglévő, illetve a rendelkezésre bocsátott törlési funkció használata. • Selejtezés: szabályszerű selejtezés [Ld.3.1. sz. fejezet 6.].
Bizalmas	• Jelölés: „Bizalmas”. Jelölés a dokumentum első oldalán elektronikus és nyomtatott formában. • Sokszorosítás és továbbadás: a jogosult konszern munkatársak és a munka- vagy alkalmazási területen jogosult harmadik személyek korlátozott köre. Ennek során a továbbadó viseli a felelősséget, hogy alkalmas megosztási útvonalakat használjon annak érdekében, hogy megóvja az információkat és adatokat az illetéktelen betekintéstől, illetve illetéktelen lehallgatástól (pl. titkosítás révén). • Tárolás: a jogosult konszern munkatársak és a munka- vagy alkalmazási területen jogosult harmadik személyek korlátozott köre részére hozzáférhető (pl. zárt felhasználói csoportok révén). Ehhez megfelelő tárolási helyeket, illetve tárolási médiumokat kell használni. • Törlés: a már nem szükséges adatok törlendők. • Selejtezés: szabályszerű selejtezés [Ld. 3.1. sz. fejezet 6.].
Titkos	• Jelölés: „Titkos”. Jelölés a dokumentum valamennyi oldalán. • Sokszorosítás és továbbadás: a jogosult konszern munkatársak és a munka- vagy alkalmazási területen jogosult harmadik személyek erősen korlátozott köre részére (pl. név szerinti lista), az adatgazdának előzetes engedélye alapján. Ennek során az adatokat a technikai lehetőségeknek megfelelően kódolni kell. Amennyiben ez technikailag nem lehetséges, úgy hasonló óvintézkedéseket kell alkalmazni és emellett a további technikai vagy szervezeti óvintézkedéseket is meg kell vizsgálni (pl. továbbadás vagy nyomtatás tilalma, vízjel). Megfelelő óvintézkedéseket kell tenni, hogy megakadályozzák a lehallgatást (pl. kódolt videokonferencia). • Tárolás: a jogosult konszern munkatársak és a munka- vagy alkalmazási területen jogosult harmadik személyek erősen korlátozott köre részére hozzáférhető (pl. név szerinti lista). Ennek során az adatokat a technikai lehetőségeknek megfelelően kódolni kell. Amennyiben ez technikailag nem lehetséges, úgy hasonló óvintézkedéseket kell alkalmazni. • Törlés: a már nem szükséges adatok törlendők. • Selejtezés: szabályszerű selejtezés [Ld. 3.1. sz. fejezet 6.]

A megjelölésért az információ létrehozója a felelős.

Ha egy információ nincs jelölve, úgy azt „Belső” információként kell kezelni, kivéve, ha rendelkezésre áll az illetékes terület [Ld. 3.1. sz. fejezet 5.] nyilvánossá tételhez való hozzájárulása. Ebben az esetben az információt nyilvánosként kell kezelni.

Az információk kezelésére vonatkozó szabályozások (jelölés, sokszorosítás, továbbadás, törlés, selejtezés) az IT rendszerekre is vonatkoznak (pl. adatbázisokra, biztonsági mentésre használt médiumokra).

Az információk besorolása az integritás, visszakövethetőség és rendelkezésre állás tekintetében elsődlegesen azt a célt szolgálja, hogy ezek alapján biztonsági követelményeket lehessen meghatározni azon információs rendszerek számára, amelyek feldolgozzák ezeket.

2.3. Személyes biztonság

A már szükségtelen felhasználónevet vagy a már nem szükséges hozzáférési jogot az adott felhasználónak haladéktalanul jelentenie kell az adott, illetékes területeknél annak érdekében, hogy megtörténhessen a megfelelő zárolás / törlés.

A már szükségtelen, azonosításra szolgáló médiumokat (pl. Smart kártyák, SecurID kártyák) haladéktalanul vissza kell adni az illetékes szerveknek.

Az átadott készülékeket (pl. laptopok) és adathordozókat, illetve tárolási médiumokat vissza kell szolgáltatni.

A felhasználónak átadott IT eszközök, valamint az azonosítást szolgáló médiumok elvesztését a felhasználónak haladéktalanul jelentenie kell a Megbízó területeknek.

2.4. Fizikai és környezeti biztonság

A rendelkezésre bocsátott eszközöket rendeltetésszerűen kell használni, és óvni kell az elvesztéssel vagy illetéktelen módosítással szemben, valamint be kell tartani a gyártó előírásait a készülékek megóvására vonatkozóan.

A bizalmas vagy titkos adatokat tároló vagy feldolgozó IT eszközöket úgy kell kialakítani, hogy az illetéktelenek általi hozzáférés vagy betekintés kockázata minimalizálható legyen.

A Megbízó által rendelkezésre bocsátott készülékeket (pl. laptopok, mobiltelefonok, stb.) csak a Megbízó illetékes szakterületének engedélyével szabad kivinni a gyár területéről. Ezen IT eszközök elvesztését haladéktalanul jelenteni kell az illetékes területeknek [Ld. 3.1. sz. fejezet 7.].

2.5. Üzemi- és kommunikációmanagement

2.5.1. Rosszindulatú szoftverek és mobil programkódok elleni védelem

Kártékony szoftverrel való megfertőződés gyanúja esetén az érintett IT eszközök és adathordozók nem használhatók tovább. Haladéktalanul értesíteni kell az illetékes területeket [Ld. 3.1. sz. fejezet 8.].

2.5.2. Biztonsági mentés

Az adatokat lehetőség szerint a hozzárendelt hálózati meghajtókon kell tárolni, nem pedig a helyi merevlemezen, mivel csak a hálózatban biztosított a központi automatikus adatmentés.

Azon adatok biztonságáért, melyeket nem a központi hálózati meghajtókon tárolnak (pl. helyi merevlemez, mobil adathordozók) a felhasználó tartozik felelősséggel.

2.5.3. Tároló és adathordozó médiák kezelése

Az adathordozókat (pl. CD-k, DVD-k, USB-tárak, merevlemezek) védeni kell az elvesztéssel, megsemmisüléssel és felcseréléssel, valamint az illetéktelen hozzáféréssel szemben.

A már nem szükséges adathordozókat biztonságosan le kell selejtezni. [Ld. 3.1. sz. fejezet 6.]

2.5.4. Információcsere

Valamennyi, bizalmas vagy titkos információról szóló beszélgetés során, beleértve a telefonbeszélgetéseket is, ügyelni kell arra, hogy azokat ne hallgathassák le illetéktelenek.

A külső faxszámokat és e-mail címeket az aktuális kommunikációs jegyzékekből kell kikeresni, vagy a címzettől kell megkérdezni annak érdekében, hogy elkerülhető legyen a megküldött adatok rossz helyre történő továbbítása.

Bizalmas adatok faxon történő küldése előtt telefonon jelezni kell a kommunikációs félnek az átvitelt. Az átvitelt követően telefonon ellenőrizni kell a fax szabályszerű megérkezését. A feladónak az átvitelt követően ki kell vennie a faxról szóló visszaigazolást a faxkészülékből.

Ügyelni kell arra, hogy meghozzanak valamennyi szükséges óvintézkedést (pl. tikosítás) amelyek megakadályozzák, hogy a szállítás közben illetéktelenek (ide tartoznak a családhoz és a baráti körhöz tartozó személyek is) betekinthessenek bizonyos információkba, módosítsák vagy töröljék azokat.

IT eszközök és adathordozók üzemen kívülre történő kivitele esetén be kell tartani az Audi Hungaria szabályozásait és üzemi megállapodásait. Ezzel kapcsolatban Megbízó terület ad további útmutatást.

A létrehozó az e-mail szerzőjeként felel annak tartalmáért és kiküldéséért, a címzett pedig az e-mail további feldolgozásáért és továbbításáért.

Elektronikus lánclevelek készítése és kiküldése tilos.

2.6. Hozzáférések ellenőrzése

2.6.1. Üzleti követelmények a hozzáférések ellenőrzésére

Tilos az idegen felhasználói azonosító használata.

Tilos az azonosítást szolgáló médiumok (pl. Smart-kártyák, SecurID-kártyák) továbbadása.

Tilos egy személyes felhasználásra hozzárendelt felhasználói azonosítás jelszavának vagy PIN-kódjának (ún. „személyre vonatkozó felhasználói azonosítás”) továbbadása.

A személyes felhasználói azonosítások újbóli, különböző személyek általi használata (pl. képzésben résztvevők, gyakornokok, végzős hallgatók) az alábbi intézkedések betartásával minősül megengedettnek:

- A felhasználói azonosítás kiosztását egy felelős személynek kell kezelnie. Ennek a személynek írásos jegyzéket kell vezetnie arról, ki mikor melyik felhasználói azonosítót használta. Ennek igazolását ennél a személynél kell elhelyezni.
- A felhasználói azonosító átvételét az adott felhasználónak írásban kell visszaigazolnia. Az igazolás a felhasználói azonosításért felelős személynél marad.
- Az adott felhasználói azonosító átadásakor az új felhasználónak módosítania kell a jelszót egy olyanra, amelyet kizárólag ő ismer.
- Az adott felhasználói azonosító visszaadásakor az illetékes kezelőnek módosítania kell a jelszót egy olyanra, amelyet kizárólag ő ismer.
- Az igazolások megőrzésére vonatkozóan figyelembe kell venni a társaság-specifikus megőrzési határidőket.
- Tilos több személy által egyszerre használt felhasználói azonosítások használata (ún. „csoportos azonosítások”), kivéve, ha ezen felhasználói azonosítással kizárólag olyan alkalmazások tölthetők be, amelyek olyan saját felhasználó kezeléssel rendelkeznek, amely szükségessé teszi a személyre vonatkozó vizsgálatot, vagy csupán olvasásra való hozzáférést engedélyez.

2.6.2. A felhasználók felelőssége

A jelszó meghatározásakor az alábbi minimális követelményeket kell figyelembe venni:

- Az alábbi 4 kritériumból legalább 3 alkalmazásával legalább 8 karakterből álló kombinációt kell alkalmazni:
    - nagybetűk,
    - kisbetűk,
    - számok,
    - különleges írásjelek,
- Nem használhatók triviális kombinációk (pl. „AAAAAAAA”) vagy a személyes körülményekre vonatkozó szempontok (pl. nevek, születési dátumok).

A Windows-bejelentkezés jelszavainak meghatározásakor a fenti 4 kritériumból legalább 3 alkalmazásával legalább 10 karakterből álló kombinációt kell alkalmazni. Ezek lehetnek könnyen megjegyezhető mondatok (jelszó: „Fő a biztonság!”), vagy könnyen megjegyezhető mondatok rövidítései és átírásai (könnyen megjegyezhető

mondat: „Reggel korán fel fogok kelni és egyből megmosom a fogam.” Az ebből képzett jelszó: „Rkffk&1maf”.) (Az itt megadott példákat ne használja saját jelszóként.)

Az azonosítást szolgáló médiumok (pl. Smart kártyák, SecurID kártyák) PIN kódjának megadásakor az alábbi minimális követelményeket kell figyelembe venni:

- A SecurID kártyák esetében legalább 4 karakterből álló kombinációt, az egyéb médiumok esetében (pl. Smart kártyák) pedig legalább 6 karakterből álló kombinációt kell használni. Nem használhatók triviális kombinációk (pl. „111111”) vagy a személyes körülményekre vonatkozó szempontok (pl. születési dátumok).

A személyes jelszavak, illetve PIN kódok (a továbbiakban: jelszavak) kezelésekor az alábbi minimális követelményeket kell figyelembe venni:

- A jelszavak tárolása csak biztonságos kódolás mellett megengedett.
- A jelszót az első használatkor, majd ezt követően 90 naponként módosítani kell. (Ez nem vonatkozik a PIN kódokra.)
- A jelszót haladéktalanul meg kell változtatni, ha fennáll annak gyanúja, hogy harmadik személy megismerhette azt.
- Tilos a jelszavak kifigyelése.
- Amennyiben a jelszavakat írásban letétbe kell helyezni, úgy azt a munkatársnak lezárt borítékban, erre alkalmas helyen (illetéktelen hozzájutásától megóvva /pl. páncélszekrényben/) kell elhelyeznie, amit a jelszó minden egyes módosításakor aktualizálnia kell. A lezárt borítékot az adott munkatársnak alá kell írnia. A felnyitásra jogosult személyeket név szerint rá kell vezetni a borítékra. Amennyiben rendkívüli, illetve kivételes esetben szükségessé válik a letétbe helyezett jelszó használata (pl. betegség esetén), úgy ennek a „több szem elve” alapján kell történnie. Minden egyes felnyitást dokumentálni kell és közölni kell a munkatárssal. Minden egyes felnyitás után a munkatársnak haladéktalanul meg kell változtatnia a jelszót, és ismét letétbe kell helyeznie azt. (Megengedettek azok az IT rendszerek is, amelyek megfelelnek ezeknek a követelményeknek (pl. jelszó-széf)).

A rendszerből üzem közben történő kilépéskor (pl. szünet, megbeszélés) a felhasználónak aktiválnia kell egy rendszergátat (pl. jelszóval védett képernyővédő).

Azon munkatársaknak, akik multifunkciós igazolványukat az IT rendszerekbe való bejelentkezésre használják, a rendszer elhagyásakor el kell távolítaniuk az igazolványukat az olvasóból.

2.6.3. Hozzáférések ellenőrzése hálózatok esetén

2.6.3.1. A hálózati szolgáltatások használatára vonatkozó szabályok

A vállalat által rendelkezésre bocsátott IT eszközt csak akkor és addig szabad összekötni a vállalattól idegen hálózatokkal (pl. hotspotok, privát WLAN), ha ez a Megbízó hálózatával történő kapcsolat létesítését szolgálja.

2.6.3.2. Az eszközök azonosítása a hálózaton

Az IT-eszközök belső hálózathoz történő korlátlan (pl. tűzfalon keresztül) csatlakoztatása csak abban az esetben megengedett, ha ezen eszközöket a Megbízó bocsátja rendelkezésre.

Amennyiben a megbízott IT eszközein vagy mobil rendszerein a Megbízó adatai vannak elmentve, úgy azokat a technika mindenkori állása szerinti hardver és szoftver segítségével kell kódolni.

Külföldi utazás előtt figyelembe kell venni a biztonsági technikák (pl. kódolás) alkalmazásával kapcsolatos ország specifikus szabályozásokat.

2.7. Információbiztonsági események kezelése

Az IT biztonsággal kapcsolatos eseményeket (pl. fellépő zavarok, az IT biztonsági szabályzat megsértése) azonnal jelenteni kell az illetékes területeknek [Ld. 3.1. sz. fejezet 8.]

Az IT rendszerek vélt sérülékenységeit és gyenge pontjait jelenteni kell az illetékes területeknek [Ld. 3.1. sz. fejezet 9.].

2.8. Előírások betartása

Meg kell óvni a szellemi tulajdonhoz fűződő jogokat (pl. szoftverek, dokumentumok, idegen képanyag szerzői jogai, tervek, márkajelzések, szabadalmak és forráskód-licencek jogai).

Különösen tilos az érvényben lévő jogszabályi rendelkezések értelmében a licenccel nem rendelkező szoftverek (kalózmásolatok) használata.

A licenc-szoftverre a szerzői jogi védelemmel kapcsolatos jogszabályi rendelkezések vonatkoznak (pl. a szoftverek sokszorosítása, kivéve a biztonsági és archiválási célokat, a szerzői jog megsértésének minősül). A fenti rendelkezések megsértése büntetőjogi intézkedéseket, valamint a jogsértés megszüntetését célzó, illetve kártérítési igényeket vonhat maga után.

A licenc-szoftver csak a megállapodás szerinti célokra, és kizárólag az érvényben lévő rendelkezéseknek és a gyártóval kötött licenc-megállapodásoknak megfelelően használható.

Be kell tartani az adatvédelemre vonatkozó nemzeti törvényeket és egyéb szabályozásokat

A megbízottakat a partnercég ügyvezetésének köteleznie kell az adatvédelemre vonatkozó jogszabályi szabályozások betartására.

2.9. Eltérések

Az eljárási irányelvtől való olyan eltérés, amely csökkenti a biztonsági szintet, csak az illetékes területekkel [Ld. 3.1. sz. fejezet 9.] való egyeztetés alapján és kizárólag időben korlátozott módon megengedett.

3. További dokumentációk, mellékletek

Hivatkozások

	Leírás
1.	Beszerzés, IT, Kontrolling.
2.	Megbízott felelős azért, hogy az információkat, programokat és IT-eszközöket csak Megbízó vállalati céljaira és csak az adott feladat keretében használja és alkalmazza, az érvényben lévő megbízásnak megfelelően. Nem megengedett a privát szoftver installálása és a privát adatok tárolása és használata Megbízó IT-eszközein és adathordozóin.
3.	IT érintett területei.
4.	Az AUDI HUNGARIA Zrt adatkezelésében lévő személyes adatok csak a szolgálati tevékenységek keretében dolgozhatók fel és használhatók. Nem megengedett ezen adatok illetéktelen harmadik személynek (pl. ügyfelek, partnercégek munkatársai, munkatársak) történő továbbítása. Azon IT eszközök és adathordozók, amelyeken személyre vonatkozó vagy más egyéb bizalmas vagy titkos adatokat tárolnak, alapvetően csak titkosítva hagyhatják el az AUDI HUNGARIA területét.
5.	Vállalati kommunikáció és kormánykapcsolatok
6.	A személyre vonatkozó illetve egyéb bizalmas és titkos, papír alapú dokumentumokat az adatvédelmi konténerekben kell leselejtezni. A már nem szükséges adathordozókat megbízható módon, átírással kell törölni vagy fizikai módon megsemmisíteni.
7.	Biztonságpolitika és adatvédelem
8.	IT Biztonság: it-sicherheit@audi.hu
9.	IT Biztonság: it-sicherheit@audi.hu

IT-biztonsági eljárási irányelvek rendszerüzemeltetők és adminisztrátorok részére

Verzió: 4.0 (2018.05.11.)
Kiadó: IT-biztonság
Szabályozás száma: 10 Felsőszintű szabályozás

Érvényességi kör

Az eljárási irányelvek az AUDI HUNGARIA Zrt. (továbbiakban úgy is mint „Audi Hungaria”, ill. „Megbízó”) számára szolgáltatást végző partnerekre (továbbiakban úgy is mint „Megbízott”) vonatkoznak.

Tartalom

1. Cél 20
2. Szabályozások 20
2.1. Az információbiztonság szervezése 20
2.2. A szervezet saját értékeinek a kezelése 20
2.3. Fizikai és környezettel kapcsolatos biztonság 20
2.4. Üzemi és kommunikációmenedzsment 21
2.4.1. Eljárások és felelősségek 21
2.4.2. Harmadik személy szolgáltatásnyújtásának szervezése 22
2.4.3. Rendszertervezés és átadás 23
2.4.4. Kártékony szoftverek és mobil programkódok elleni védelem 23
2.4.5. Biztonsági mentés 23
2.4.6. A hálózat biztonságának kezelése 23
2.4.7. Elektronikus közlemények/ hírek (Messaging) 24
2.4.8. Nyilvánosan elérhető információk 24
2.4.9. Ellenőrzés 24
2.5. Hozzáférések ellenőrzése 25
2.5.1. A hozzáférések ellenőrzésének üzleti követelményei 25
2.5.2. Felhasználók kezelése 26
2.5.3. A felhasználók felelőssége 27
2.5.4. Hozzáférés ellenőrzése a hálózaton 27
2.5.5. Jogosultság ellenőrzése operációs rendszeren 27
2.5.6. Mobile Computing és távmunka 28
2.6. IT-rendszerek beszerzése, fejlesztése és karbantartása 28
2.6.1. IT-rendszerek biztonsági követelményei 28
2.6.2. Titkosító intézkedések 31
2.6.3. Rendszeradatok biztonsága 32
2.6.4. Fejlesztési- és támogatófolyamatok biztonsága 32
2.6.5. Sebezhetőség kezelése 32
2.7. Az üzletfolytonosság biztosítása (Business Continuity Management) 32
2.8. Az előírások betartása 33
3. További dokumentációk, mellékletek 35

3.1. Eltérések..... 34

1. Cél

Az információk és az IT készülékek (pl.: személyi számítógépek, munkaállomások, hordozható számítógépek, mint pl.: notebook-ok, smartphone-ok, Tablet-ek) használatakor figyelembe veendő rendszerüzemeltetőknek és adminisztrátoroknak szóló IT biztonsági szabályok ebben az eljárási irányelvben kerültek megfogalmazásra. A programozható logikai vezérlők (SPS) és a robotvezérlők védelmére kizárólag ezen eljárási irányelvben [3. sz. fejezet 1.] olvasható szabályozás érvényes.

Az IT biztonsági eljárási irányelvek az információk bizalmasságának, integritásának, rendelkezésre állásának és követhetőségének védelmét, valamint a vállalat és minden olyan természetes és jogi személy jogainak és érdekeinek védelmét szolgálja, akik üzleti kapcsolatban állnak az AUDI HUNGARIA Zrt-vel, illetve a társaságnál dolgozókkal.

2. Szabályozások

2.1. Az információbiztonság szervezése

Egy külsős partnercég konszernhálózatba való bekötése csak titoktartási szerződés aláírása után (ld. [3. sz. fejezet 3.]) és egy meghatározott biztonsági szint bizonyítása (pl. a VDA alapján az Information Security Assessment-en (ISA) alapuló Self Assessment) után lehetséges.

2.2. A szervezet saját értékeinek a kezelése

A működéshez szükséges IT rendszereket (ld. [3. sz. fejezet 4.]) egy listába kell összefoglalni. Az IT rendszerek működéséért egy szervezeti egységet vagy egy személyt kell felelősként rendelni.

2.3. Fizikai és környezettel kapcsolatos biztonság

A működéshez szükséges IT rendszereket osztályozni kell az alapján, hogy a működési zavara esetén a vállalat további működését veszélyeztetik, ill. amelyek helyreállítása vagy újra beszerzése sok időbe telik és / vagy magas költséggel jár.

Az IT rendszerek összefoglaló listája legalább az alábbi információkat kell, hogy tartalmazza:

- Az IT rendszerek leírása a többi IT rendszerhez való kapcsolatok leírásával együtt.
- Felelős munkakör vagy személy.
- Az IT rendszerek üzleti folyamatokhoz való hozzárendelése.

- Az üzemelés helye (pl. számítógépközpont).
- Üzleti folyamathoz való tartozás.
- Adatok osztályozása és adott esetben a különleges védelemre vonatkozó követelmények és intézkedések megjegyzései.
- Személyes adatok megléte.
- Az adatgazda megnevezése.

Az információkért a felelősség a mindenkori információtulajdonost terheli és ez akkor is érvényes, ha az információ IT rendszeren keresztül biztosított. Az egyes feladatok delegálása engedélyezett.

A működéshez szükséges IT-rendszereket az áramkiesés hatásaitól védeni kell (pl.: szünetmentes áramellátás).

Az áramot és a telekommunikációs kapcsolatot biztosító ellátó kábeleket, amelyek adatokat szállítanak, illetve információs rendszereket látnak el, lehallgatás és károsodás ellen a megfelelő intézkedésekkel (pl. az elosztó központokba történő ellenőrzött bejárás) kell védeni.

Az üzemeltetőnek a készülék karbantartása alatt is biztosítania kell, hogy az adatok elérhetőek legyenek az alábbiak szerint:

- a készülékek karbantartásának meg kell felelnie az előállító előírásainak,
- a készülék üzemelésének meg kell felelnie az előállító által megadott üzemi paramétereknek (hőmérséklet-, nedvességtartalom ellenőrzése, stb.)
- a készüléket jogosulatlan hozzáféréstől, illetve manipulációtól védett és a káros környezeti hatásoktól óvni kell (tűz /víz / szennyeződések).

2.4. Üzemi és kommunikációmenedzsment

2.4.1. Eljárások és felelősségek

2.4.1.1. Dokumentált üzleti folyamatok

Azon utasításokat, amelyeket az IT-rendszerek üzeménél figyelembe kell venni, az üzemeltetőnek kell elkészítenie és naprakészen tartania, pl. üzemeltetési kézikönyvek, működési és karbantartási leírások formájában. Nyilvánosságra hozatalkor arra kell figyelni, hogy a biztonsági szempontból fontos adatok (pl. tűzfal konfigurációk) jogosulatlan harmadik fél számára ne legyenek elérhetőek. A dokumentációkat a vállalati szabályozások alapján kell archiválni (ld. [3. sz. fejezet 5.]). A rendszerüzemeltetőnek a meghatározott folyamatokhoz kell tartania magát (pl.: Change folyamat).

2.4.1.2. Változások kezelése

A produktív IT rendszereken tervezett változtatásokat meghatározott eljárás alapján tervezni, tesztelni, engedélyezni és dokumentálni kell, mielőtt azok éles üzembe kerülnek.

Változtatási igényeket (Change requests) írásban dokumentálni kell (pl. IT rendszereken történő változtatásokat az adatgazda által, az infrastrukturális vagy a

berendezésen történő változtatásokat az üzemeltető által) és a felelős területtel engedélyeztetni.

A tervezett változtatások hatásait tesztrendszerben kell megvizsgálni és a bevezetésénél mérlegelni kell a lehetséges rizikókat, valamint az azokhoz szükséges ráfordításokkal is tervezni kell. Vészhelyzetben az üzemeltető egy IT vészhelyzeti tervben meghatározhat gyorsított eljárást is (ld. az „Üzletfolytonosság biztosítása“ Business Continuity Management c. fejezetben). Emellett biztosítani kell azt is, hogy a változtatásokkal a biztonsági intézkedések ne sérüljenek.

A biztonsági szintet a változtatás ideje alatt és után meg kell tartani. Ha a rizikókat nem lehet kizárni, a tervezésnek a visszaállás lehetőségét is biztosítani kell és meg kell adni azon kritériumokat, amikor ez a lehetőség bekövetkezik. Az IT-rendszerekben történő változtatásokat naplózni kell.

Minden, a változásban érintett személyt a megfelelő időben informálni kell.

2.4.1.3. A felelősségek felosztása

A végrehajtó (pl. programozás, fejlesztés) és az ellenőrző (pl. audit, átadás) feladatokat szét kell választani egymástól, a végrehajtó és az ellenőrzést végző személyek nem lehetnek ugyanazok. Egyedi esetben ezt szervezetileg is szabályozni kell.

A tevékenységeket abban az esetben is szét kell választani, ha szétválasztás nélkül szándékos vagy akaratlan károkozás történik / történhet a konszern terhére. („több-szem-elv“)

2.4.1.4. A fejlesztői-, teszt- és produktív rendszerek elkülönítése

A fejlesztői és a tesztkörnyezetet, valamint az éles rendszert el kell különíteni egymástól. Kivételt képeznek ez alól a gyártási környezetben lévő berendezések, amelyeknél ez aránytalanul nagy többletmunkát eredményez.

Szoftverek fejlesztése és tesztelése csak az arra tervezett fejlesztő, illetve tesztkörnyezetben engedélyezett és biztosítani kell, hogy a produktív működést ne zavarja.

Amennyiben lehetséges a tesztadatokat elő kell állítani. (pl. teszt adatgenerátor segítségével)

A személyes, bizalmas és titkos adatokat az éles rendszerből történő átvétel előtt úgy át kell alakítani, hogy az eredeti adatokra ne lehessen visszakövetkeztetni.

Az éles IT-rendszerekből történő információk másolása vagy használata csak az adatgazdának az előzetes jóváhagyásával lehetséges. A másolt adatokra ugyanazok az IT biztonsági előírások vonatkoznak, mint az eredeti adatokra.

Az éles rendszerből használt információkat a teszt elvégzése után törölni kell.

Az éles rendszerben érvényes hozzáférési szabályozásokat a tesztfelhasználás során is figyelembe kell venni.

2.4.2. Harmadik személy szolgáltatásnyújtásának szervezése

Az IT biztonságra vonatkozó tevékenységeket alapvetően belső munkatársnak kell végeznie. Amennyiben ez nem lehetséges, a harmadik fél tevékenységét ellenőrző

intézkedésekkel kell kísérni. Az adminisztratív vagy operatív tevékenységek outsourcingja vagy outtaskingja esetén a harmadik fél tevékenységét ellenőrző intézkedésekkel kell kísérni.

2.4.3. Rendszertervezés és átadás

Az IT rendszer kapacitásigényeit a tervezés során kell megállapítani.

Az IT rendszerek biztonsági követelményeit a tervezés során az adatgazdával kell megállapítani és dokumentálni. Egy új rendszer bevezetése tartalmaz a rendszerüzemeltető által dokumentált és átadott üzemátvételt.

A rendszertervezést (szakmai koncepció, rendszertervezés, rendszermegvalósítás) és –átadást (rendszerbevezetés) az Audi Hungariánál érvényes rendszerfejlesztési előírás alapján kell megvalósítani.

2.4.4. Kártékony szoftverek és mobil programkódok elleni védelem

A kártékony szoftverekkel fertőzött IT eszközöket, a lehetséges további hatások (pl. sormegállás) figyelembe vételével le kell választani a hálózatról.

Az IT eszközöket és IT rendszereket védeni kell a támadásoktól, illetve a kártékony szoftverektől, pl. egy, az illetékes munkakör által jóváhagyott vírusirtó szoftverrel (ld. [3. sz. fejezet 6.]). A megfelelő víruslenyomatokat rendszeresen aktualizálni kell.

2.4.5. Biztonsági mentés

Minden IT rendszerért felelős személynek biztosítania kell, hogy az adatok biztonsági mentésével az információk meghatározott visszaállíthatósági időpontig elérhetőek legyenek.

A mentési eljárásokat tervezni, megvalósítani, ellenőrizni és dokumentálni kell.

A Backup médiákra ugyanazok a biztonsági követelmények vonatkoznak, mint az eredeti adatokra. (pl. lopás és jogosulatlan hozzáférés elleni védelem). Ezeket az IT-rendszertől elkülönítve, egy tűzálló helyen kell tárolni. A védelmi követelmény függvényében egy másik telephelyen külső biztosítást kell nyújtani.

Az adatok megőrzésének idejére az információk olvashatóságát és használhatóságát biztosítani kell.

Az adatok archiválásánál a vállalati és a törvényi előírások szerinti megőrzési határidőket be kell tartani (ld. [3. sz. fejezet 5.]). Az archivált adathordozók olvashatóságát meghatározott időközönként meg kell vizsgálni.

A mentett adatok visszaállításának működőképességét rendszeresen ellenőrizni kell.

2.4.6. A hálózat biztonságának kezelése

Közvetlenül egy hálózati komponens telepítése után (pl. Router) aktiválni kell a rendszerspecifikus védelmi mechanizmusokat (pl. jelszavas védelem). A különböző aktív hálózati komponenseket egy megfelelő managementrendszer segítségével, központilag kell ellenőrizni, hogy a hibás állapotokat vagy a kritikus események bekövetkezését időben felismerhetőek legyenek.

2.4.7. Elektronikus közlemények/ hírek (Messaging)

A rendszerfelelős felelős a kommunikációs szolgáltatások (pl. e-mail) megbízhatóságáért. Az e-mail szolgáltatásoknál a következőkre kell figyelni:

- Visszakövethetőnek kell lennie, hogy ki küldte az emailt.
- A rendszer által generált email üzeneteket egy felelős személyhez kell rendelni.
- A postaládákat jogosulatlan hozzáférés ellen védeni kell.

2.4.8. Nyilvánosan elérhető információk

A nyilvánosan elérhető IT-rendszerekből csak biztonságos hálózati kapcsolatokon keresztül szabad a belső hálózatot elérni.

Azokat az információkat, amelyeket nyilvánosan elérhető IT rendszereken kerülnek rendelkezésre bocsátásra, megfelelő biztonsági intézkedésekkel (pl. az azonosítási információ titkosított kapcsolaton keresztül) kell óvni a jogosulatlan hozzáféréstől.

2.4.9. Ellenőrzés

2.4.9.1. Auditprotokollok

A titkos adatokat tartalmazó rendszerek felhasználói hozzáféréseit naplózni kell. A naplóállományokat (logokat) a vállalati szabályozásoknak megfelelően meg kell megőrizni.

A logoknak legalább a következőket kell tartalmaznia:

- a logokban szereplő személy egyértelmű azonosítását (pl. név vagy felhasználó),
- a rendszerhez való sikeres vagy sikertelen hozzáférések,
- az adatokhoz és egyéb erőforrásokhoz való hozzáférés rögzítése.

2.4.9.2. A rendszer használatának ellenőrzése

A logok kiértékelése rendszeresen, audit keretein belül és IT biztonsági esemény gyanúja esetén kerül elvégzésre.

Az audit / aktivitáslogok kiértékelésénél a szükséges engedélyezési eljárásokat be kell tartani [lásd 7.1. fejezet 7.].

2.4.9.3. A naplóinformációk védelme

A naplóállományokat úgy kell menteni, hogy a naplózott személyeknek ne legyen jogosultsága a logokat változtatni vagy törölni. A logokat nem szabad manipulálni vagy a naplózó rendszert deaktiválni, a rendszeradminisztrátorok nem törölhetik észrevétlenül a listákat. Amennyiben a napló titkos információkat tartalmaznak (pl.: az adatok listája a változtatás előtt és után, vagy átadott adatok stb.), biztosítani kell, hogy a logokat olyan személy tekinthesse meg vagy értékelje, aki az adatgazdától megfelelő felhatalmazással rendelkezik.

2.4.9.4. Adminisztrátori és üzemeltetői protokollok

A rendszerüzemeltetők IT-rendszereken végzett tevékenységeit bizalmas, és / vagy titkos információként kell naplózni.

A rendszerüzemeltetők legalább az IT rendszereken végzett titkos információkkal történő tevékenységeit úgy kell tárolni, hogy a bővített jogosultsággal rendelkező naplózott személyeknek ne legyen a logok adataira vonatkozó változtatási vagy törlési jogosultságuk.

A naplóknak legalább a következőket kell tartalmazniuk:

- a naplózott személy egyértelmű azonosítása (pl. név vagy felhasználó),
- az IT rendszeren történő tevékenység kezdete és vége
- a tevékenység oka (pl. rendszerhiba, change, update)
- elvégzett intézkedések.

2.4.9.5. Hibaprotokollok

A felhasználók által jelzett hibákat és a hibás működést naplózni kell. Az üzemeltető által végzett, a hiba elhárítását szolgáló intézkedéseket dokumentálni kell.

2.4.9.6. Időszinkronizálás

Az információs rendszerek, amelyek naplózási adatait gyűjteni kell, egy pontosan meghatározott referenciaidővel kell szinkronizálni.

2.5. Hozzáférések ellenőrzése

2.5.1. A hozzáférések ellenőrzésének üzleti követelményei

Az információkhoz való hozzáférésre az adatgazdának a kockázatértékelésétől függően kell az azonosításra és engedélyezésére mechanizmusokat bevezetni. Emellett az adatgazda által megállapított jogosultsági koncepciót meg kell valósítani.

Egy IT-rendszerhez való hozzáférés vagy jogosultság igénylése írásban, felhasználói igényléssel, egy ezen tevékenység céljából létrehozott IT rendszeren keresztül kell történnie úgy, hogy azt a szervezeti egység vezetőjének és az adatgazdának is engedélyeznie kell. Minden személyt, aki egy IT rendszert vagy alkalmazást használatára jogosult hivatalosan rögzíteni kell.

A jogosultság és hozzáférés beállításához a szervezeti egység vezetőjének és az információ mindenkori tulajdonosának, a központi szolgáltatások kivételével (pl. Intranet) az engedélyezése szükséges (több-szem-elv).

A felhasználói azonosítókat mindig egy személyhez kell hozzárendelni.

A karbantartási hozzáféréshez használt azonosítási médiákat (pl. Smartcards, SecureID-kártyák) csak az alábbi intézkedések betartásával lehet továbbadni:

- A továbbadást egy felelős személynek dokumentálnia kell. Gondoskodni kell arról, hogy egy írásban rögzítve legyen, hogy ki, mikor és kinek adta át a médiát.
- A dokumentáció megőrzésére ugyanaz az időszak vonatkozik, mint a jogosultság igénylésekre.

- Az átadásra és a jelszavak visszaállítására eljárást kell meghatározni és azt nyilvánossá kell tenni.

2.5.2. Felhasználók kezelése

Adminisztrátori felhasználókat csak adminisztrátori feladatok végrehajtására szabad használni. A rutinfeladatok, amelyekhez nem kell adminisztrátori jogosultság, egy korlátozott hozzáférésű felhasználói azonosítóval kell elvégezni.

A jelszavak és az azonosítási médiák (pl.: Smartcards, SecurID-kártyák) megadására eljárásokat kell meghatározni és azokat nyilvánossá kell tenni.

Az előállító sztenderd jelszavait közvetlenül a rendszer vagy szoftver telepítése után az érvényben lévő jelszóirányelveknek megfelelően meg kell változtatni.

A felhasználói jogosultságok rendszeres felülvizsgálatához a szervezeti egység vezetőjének a saját hatáskörébe tartozó adatokat rendelkezésére kell bocsájtani.

A külsős partnerek jogosultságait amennyiben a rendszerekben technikailag lehetséges, a megbízás időtartamára kell korlátozni (max. 1 év).

A következő minimum követelményeket kell figyelembe venni a jelszómegadásnál (ez a bekezdés nem vonatkozik a PIN-ekre):

- A jelszócsere alapvetően a rendszer első használatakor és aztán 90 naponta kötelező kell, hogy legyen.
- A felhasználói azonosítás és jelszavak próbája megfelelő intézkedésekkel lehetséges (pl. a hibás próbálkozás utáni várakozási idő megnövelése és / vagy meghatározott számú hibás próbálkozás után a felhasználó zárolása).
- A bizalmas vagy titkos adatokat tároló rendszereken történő azonosításnál a jelszavakat alapvetően titkosítva kell megadni. Amennyiben ez nem lehetséges, akkor egyszeri jelszavakat kell használni.

A következő minimumkövetelményeket a jelszavak kezelésénél figyelembe kell venni:

- Azokat a felhasználói azonosítókat, amelyeket 400 napig nem használtak, zárolni kell.
- Azon jelszavakat, amelyek a rendszerekben előre be vannak állítva, egyéni jelszavakkal kell pótolni.
- A jelszavak fájlokban történő mentése csak titkosítva engedélyezett.
- Amennyiben technikailag lehetséges, 5 hibás próbálkozás után zárolni kell a fiókot,
- Biztosítani kell, hogy a felhasználók bármikor meg tudják változtatni a jelszavukat.
- A jelszavak beadásakor a képernyőn nem szabad azt szövegesen megjeleníteni.

2.5.3. A felhasználók felelőssége

Azoknak az adminisztrátori felhasználóknak, akik IT rendszerek kezelésére személyétől függően összefoglaló jogosultságokat használnak, legalább 15 jegyű kombinációból álló jelszavakat kell meghatározni és a következő 4 kritériumból legalább 3-nak teljesülnie kell:

- Nagybetűk.
- Kisbetűk.
- Számok.
- Különleges karakterek.

A rendszerfüggő felhasználói azonosítók, amelyeket automatikus bejelentkezésre és feldolgozásra a rendszer használ, legalább 16 karakter hosszú jelszavakat kell használni, amelyke a következő 4 kritériumok közül legalább 3-nak megfelelnek:

- Nagybetűk.
- Kisbetűk.
- Számok.
- Különleges karakterek.

A fent leírtak mellett a jelszót évente legalább egyszer meg kell változtatni. A rendszerfüggő felhasználói jelszavak rendelkezésre állását a rendszerfelelősnek kell biztosítania (pl. jelszóletét által). Ha a megkövetelt beállításokat egy rendszerben nem lehet megvalósítani, akkor a jelszószabályozás az érvényes.

2.5.4. Hozzáférés ellenőrzése a hálózaton

Csak azonosított és jogosult személyek kaphatnak hozzáférést a konszern hálózatához. A távoli hozzáférést a konszern belső hálózatához (Intranet) a „Tudni és birtokolni“ (pl. PKI kártya: a „Tudni“ a PIN-kód ismeretét jelenti, a „birtokolni“ pedig magának a kártyának a birtoklását) útján kell védeni. Az adattovábbítást biztonságos titkosítással kell védeni.

A hálózatban megfelelő intézkedéseket kell megtenni a végfelhasználói készülékek azonosítására.

A nem szükséges szolgáltatásokat és portokat ki kell kapcsolni.

A rizikók figyelembevétele alapján hálózati szegmentálást kell végezni és az engedélyezett kommunikációs kapcsolatokat meg kell állapítani.

A különböző védelmi igényekkel rendelkező hálózatokat az átvitelnél megfelelő hálózati biztonsági komponensekkel (pl.: Intrusion Prevention System, Firewall) kell védeni.

2.5.5. Jogosultság ellenőrzése operációs rendszeren

2.5.5.1. Eljárás a biztonságos bejelentkezéshez

A nem nyilvános adatokat tartalmazó IT-rendszerekhez való hozzáférést egy megfelelő eljárással (pl. azonosítás) a jogosult felhasználók számára kell korlátozni.

A rendszerfelelős kötelessége, hogy az irányelvnek megfelelő, biztonságos bejelentkezési eljárást (pl. PKI kártyával történő azonosítás) valósítson meg.

A felhasználói azonosítók és a jelszavak kipróbálása ellen megfelelő intézkedéseket kell bevezetni. (pl. a várakozási idő meghosszabbítása minden hibás próbálkozás után és / vagy a felhasználói azonosító meghatározott számú próbálkozás utáni zárolása).

2.5.5.2. Felhasználók azonosítása és hitelesítése

Az adminisztrációs tevékenységeket, amennyiben technikailag lehetséges, erősen kell hitelesíteni (2-szintű-hitelesítés a Tudni és birtokolni alapján). Ha ez technikailag nem lehetséges, akkor alternatív védelmi mechanizmusokat (pl. hosszú jelszó) kell bevezetni és ezeket az illetékes szakterülettel egyeztetni (ld. [3. sz. fejezet 8.]). A jelszó megadásánál / változtatásánál meg kell vizsgálni, hogy a jelszavak a jelszószabályozásnak megfelelően vannak-e képezve.

2.5.5.3. Jelszavak kezeléséhez használt rendszerek

A rendszerfelelősnek a jelszavak meghatározására vonatkozó minimum követelményeket (ld.: IT-biztonsági eljárási irányelvek partnercégek számára) megfelelő rendszerbeállítások segítségével támogatnia kell.

A jelszavakat legalább bizalmas csoportba kell sorolni és megfelelően kell kezelni őket, kivéve, ha az adatgazda az adatokat, amelyekhez ezzel a jelszóval hozzá lehet férni, titkosként sorolta be. Ilyenkor a jelszavakra magasabb a védelmi igény (személyiséglopás), ezért a tárolási hely titkosítása szükséges.

2.5.5.4. Rendszereszközök használata

A rendszer vagy alkalmazás beállításain végzett nem jogosult változtatás, például rendszereszközök segítségével, és megfelelő intézkedések útján (pl. a megfelelő jogosultságok elvétele) megakadályozandó.

2.5.5.5. Session Time-out

A kapcsolatokat, amelyeket hosszabb időn keresztül aktívan nem használtak, deaktiválni kell vagy megfelelő intézkedésekkel kell védeni.

2.5.6. Mobile Computing és távmunka

Egy, a vállalat által rendelkezésre bocsájtott IT eszközt csak akkor és annyi időre szabad a vállalaton kívüli hálózattal (pl. Hot Spot, privát WLAN) összekapcsolni, amíg a kapcsolat felépítése a konszern hálózatával szükséges.

2.6. IT-rendszerek beszerzése, fejlesztése és karbantartása

2.6.1. IT-rendszerek biztonsági követelményei

IT-rendszerek fejlesztése és bevezetése előtt a kötelező IT biztonsági intézkedéseket meg kell határozni és be kell vezetni.

Az információk kezelésére vonatkozó szabályozások érvényesek az IT-rendszerekre is.(Pl.: adatbázisok, háttérmentésekre szolgáló médiák).

2.6.1.1. A bizalmasság védelme

Az információkat jogosulatlan hozzáférésektől az osztályozásuknak megfelelően kell védeni. A bizalmasságra vonatkozó osztályozásnál a következő védelmi intézkedéseket kell levezetni:

Besorolás	Definíció
Nyilvános	• Rendszer erősítés (csak szükséges szolgáltatások, aktuális biztonsági patch-ek).
Belső	A „nyilvános“ intézkedései, továbbá: • Hozzáférés védelme a „felimerés, ha szükséges“ szerint. (incidens esetén történő ellenőrzés) • 1-szintű-azonosítás (pl. User-ID és jelszó).
Bizalmas	A „belső“ intézkedései, továbbá: • 2-szintű-azonosítás (pl. Smartcard PIN-kóddal), különösen alkalmazásokhoz való hozzáférés esetén vagy további biztosítás, mint kiegészítő hitelesített tárolási titkosítás (pl. titkosított fájlok a fileshare-en, titkosított USB-Stick). • Adatcsatorna titkosítás
Titkos	A „bizalmas“ intézkedései, továbbá: • 2-szintű-azonosítás (pl. Smartcard PIN-kóddal), különösen alkalmazásokhoz való hozzáférés esetén. • Adatcsatorna titkosítás • Tárolási hely titkosítás.

2.6.1.2. Az integritás védelme

Az információkat az osztályozásuknak megfelelően a vétlen változtatások elől és jogosulatlan manipulációtól védeni kell. Az integritásra vonatkozó osztályozás alapján a következő védelmi intézkedéseket kell levezetni:

Besorolás	Definíció
Alacsony	• Rendszer erősítés (csak szükséges szolgáltatások, aktuális biztonsági patch-ek)

Közepes	Az „alacsony“ intézkedései, továbbá: • Hozzáférés védelme a „need to know“ elv szerint. • 1-szintű-azonosítás (pl. User-ID és jelszó).
Magas	A „közepes“ intézkedései, továbbá: • A bementi és a kimeneti adatok ellenőrzése, úgymint a belső feldolgozás hibáinak a csökkentése és a sztenderd támadások, mint Buffer-Owerlows és a végrehajtó kódok beszivárgása (pl. mezőhatárérték vizsgálat, a mezők korlátozása speciális területekre
Nagyon magas	A „magas“ intézkedései, továbbá: • 2-szintű-azonosítás (pl. Smartcard és PIN-kód) a változtatási jogosultságokhoz. • A digitális aláírások képzése és átvizsgálása a tártolt adatokra (vagy össszehasonlítható védelmi mechanizmusok használata).

2.6.1.3. A visszakövethetőség védelme

A jogosultságok nyilvántartásához való hozzáférési jogosultságoknak és az információkban történő változtatásoknak a visszakövethetőségét besorolásának megfelelően kell biztosítani. A visszakövethetőség szerinti osztályozásnál a következő védelmi intézkedéseket kell levezetni:

Besorolás	Definíció
Alacsony	• Rendszer erősítés (csak szükséges szolgáltatások, aktuális biztonsági patch-ek). • az előforduló hibák, bejelentkezési próbák stb. sztenderd rendszernaplózása.
Közepes	Az „alacsony“ intézkedései, továbbá: • A módosítási jogosultságoknál a „USER ID”, a változtatás rendszeridejének és módjának (aktiválás, törlés, változtatás) naplózása • A módosítási jogosultságok 1-szintű-azonosítása (pl. User-ID és jelszó)
Magas	A „közepes“ intézkedései, továbbá:

	• A módosítási jogosultságoknál a „USER ID”, a változtatás rendszeridejének a naplózása, olyan módon, hogy a változtatás előtti állapot is megismerhető legyen.
Nagyon magas	A „magas“ intézkedései, továbbá: • Az olvasási jogosultságoknál a „USER ID” és a rendszeridő naplózása. • Az olvasási és a változtatási jogosultságok részére 2 szintű azonosítás (Pl. Smartcard PIN-kóddal)

2.6.1.4. A rendelkezésre állás védelme

Az IT-rendszerek rendelkezésre állását a besorolásuknak megfelelően kell biztosítani. A rendelkezésre állás alapján történő besorolásból a következő védelmi intézkedéseket kell levezetni:

Besorolás	Definíció
Alacsony	• Rendszer erősítés (csak a szükséges szolgáltatások, aktuális biztonsági patch-ek). • A kiesési idő lehet 72 óránál több. Ehhez a kötelező intézkedéseket be kell vezetni.
Közepes	• Rendszer erősítés (csak a szükséges szolgáltatások, aktuális biztonsági patch-ek). • A kiesési idő maximum 72 óra lehet. Ehhez a kötelező intézkedéseket be kell vezetni.
Magas	• Rendszer erősítés (csak a szükséges szolgáltatások, aktuális biztonsági patch-ek) • A kiesési idő maximum 24 óra lehet. Ehhez a kötelező intézkedéseket be kell vezetni.
Nagyon magas	• Rendszer erősítés (csak a szükséges szolgáltatások, aktuális biztonsági patch-ek) • A kiesési idő maximum 1 óra lehet. Ehhez a kötelező intézkedéseket be kell vezetni.

2.6.2. Titkosító intézkedések

A titkosító kulcsokat a módosítás és a megsemmisítés ellen megfelelően védeni kell. Amint a kulcs jogosulatlan számára ismerté vált, azt ki kell cserélni. Azon személyek körét, akik hozzáférhetnek ezen kulcsokhoz, a lehető legkevesebb

létszámon kell tartani és egy listában meghatározni. Biztosítani kell, hogy használt kulcsot legalább olyan hosszan megőrizzék, amíg az általa titkosított adatokat archiválni kell, amennyiben ezt nem a központi kulcsmenedzsment (pl. PKI) biztosítja. Amennyiben a kulcsot már nem használják, egy biztonságos eljárással meg kell semmisíteni.

2.6.3. Rendszeradatok biztonsága

2.6.3.1. Üzemben lévő szoftverek ellenőrzése

Az éles rendszerek új vagy változtatott programjait csak sikeres tesztek, mint az adatgazda és a rendszerüzemeltető jóváhagyása után lehet bevezetni. A bevezetett szoftverek verzió-/korrektúraállapotait dokumentálni kell és a vállalati szabályozásoknak (ld. [3. sz. fejezet 10.]) megfelelően archiválni kell.

2.6.3.2. A forráskódok hozzáféréseinek az ellenőrzése

A program forráskódokat a bizalmasság, integritás, rendelkezésre állás és nyomon követhetőség szempontjai alapján osztályozni kell, és megfelelően védeni.

2.6.4. Fejlesztési- és támogatófolyamatok biztonsága

Az alkalmazások biztonságát adminisztrátori eszközök és –naplózás bevezetésével nem szabad veszélyeztetni. Egy új szoftververzió telepítése vagy patch-elés előtt tesztekkel kell biztosítani, hogy sem az üzem sem a biztonság, a változtatások által nincs veszélyeztetve.

A változtatások esetén a felhasználói útmutató érintett leírásait és az üzemi dokumentációt aktualizálni kell.

Ha a szoftvercsomagon változtatások kerülne végrehajtásra, a meglévő szabályozásokra, szerződésekre és biztonsági intézkedésekre gyakorolt hatást tisztázni kell. Csak akkor lehet változtatásokat végrehajtani, ha licencjogilag és a karbantartási szerződés alapján engedélyezett.

2.6.5. Sebezhetőség kezelése

Biztonsági frissítéseket és javításokat a lehetséges kockázatok mérlegelése után, a nyilvánosságra hozataluk után közvetlenül tesztelni kell, majd bevezetni.

2.7. Az üzletfolytonosság biztosítása (Business Continuity Management)

Az előre nem látható és váratlan események, amelyek az IT rendszerek egy nem tolerálható időn túli kiesését okozzák és az üzleti folyamatban kárt okozhatnak, (a továbbiakban) IT vészhelyzetként említjük.

Az üzletfolytonosság fenntartása érdekében intézkedéseket kell bevezetni, hogy a kritikus IT üzleti folyamatok azonosításra és értékelésre kerüljenek.

Elővigyázatossági intézkedéseket kell meghatározni, hogy a váratlan eseményeknek (pl. kiesések) ne legyen IT vészhelyzeti következménye. Továbbá

olyan intézkedéseket kell meghatározni, amelyeket IT vészhelyzet bekövetkezése esetén végre kell hajtani.

Az intézkedéseknek az üzleti folyamatok követelményein kell alapulnia. A kockázatelemzés segítségével a lehetséges káreseményeket az előfordulási valószínűségükre vonatkoztatva és a kár nagyságának figyelembe vételével kell értékelni. Minden üzleti folyamatot figyelembe kell venni, nem kizárólag az információfeldolgozó berendezésekre kell korlátozódni. Emellett egy Business Impact Analysis-t (Üzleti hatáselemzés) kell végrehajtani.

Az üzleti szempontból kritikus információfeldolgozó IT rendszerek maximálisan elfogadható kiesési idejét és a maximálisan engedélyezett adatvesztését meg kell határozni és dokumentálni kell.

IT vészhelyzeti terveket kell készíteni, amelyek meghatározzák, hogy mikor jelentkezik IT vészhelyzet és szabályozzák az ITvészhelyzeti eljárásokat. Tömörített formában tartalmazniuk kell minden döntési szempontból lényeges adatot. Emellett azon intézkedéseket is le kell írni, melyek egy vészhelyzeti üzemből a normál üzembe való visszatéréshez szükségesek. (Az intézkedéseket érthetően kell leírni.)

Az IT vészhelyzeti terveket úgy kell elkészíteni, hogy segítségével gyorsan el tudják dönteni, mely intézkedéseket mely felelősökkel milyen sorrendben kell végrehajtani.

Az IT vészhelyzeti intézkedésekért felelős munkatársat és a helyettesét név szerint és funkció alapján is bele kell írni az IT vészhelyzeti tervekbe és biztosítani kell az elérhetőségüket is. (Fel kell sorolni azokat is, akik az IT-vészhelyzetről értesítendők)

Az üzletmenet folytonosságának biztosítását a következő intézkedésekkel és technikákkal rendszeresen (évente) meg kell vizsgálni, amennyiben az IT rendszer üzleti szempontból kritikusként határozták meg:

- IT vészhelyzetek szcenáriói.
- A személyek a krízismenedzsmentben betöltött szerepének szimulálása oktatás céljából
- Technikai tesztek az információs rendszerek visszaállítására.
- Az üzemelés visszaállításának a tesztelése.
- A külső szolgáltatók szerződéseinek vizsgálata.
- Rendszeres IT-vészhelyzeti gyakorlatok.

2.8. Az előírások betartása

A titkosítás és / vagy az elektronikus aláírás bevezetésénél (ld. [3. sz. fejezet 11.]) különösen a határokon túl az importra/exportra/jogosultságra vonatkozó hardverre, szoftverre és információkra érvényes országspecifikus szabályozásokat figyelembe kell venni.

Az országban érvényben lévő szabályozásokra vonatkozó kérdésekkel az illetékes szakterületet kell megkeresni (ld. [3. sz. fejezet 12.].).

Minden IT rendszerüzemeltetőnek szúrópróbaszerűen meg kell vizsgálnia és dokumentálnia kell, hogy a felelősségi körébe tartozó IT rendszerek megfelelnek-e a biztonsági szempontból fontos előírásoknak és irányelveknek.

A rendszer ellenőrzésére mechanizmusokat és tool-okat kell bevezetni és használni. Az ehhez szükséges engedélyezési eljárást figyelembe kell venni. (ld. [3. sz. fejezet 7.]).

Az IT rendszerüzemeltetők kötelessége, hogy az ismertté vált IT sebezhetőségeket a megfelelő intézkedésekkel kiküszöböljék.

Az audit követelményeit és aktivitásait alaposan meg kell tervezni (különösen az éles rendszerekre vonatkozóan), hogy az üzleti folyamatokra hatással lévő kockázatokat minimalizálják.

A következő pontokat kell betartani:

- A vizsgálatok alkalmazási területében meg kell egyezni és ellenőrizni kell.
- A vizsgálatokat csak a szoftverek és adatok olvasási jogosultságára kell korlátozni.
- IT erőforrásokat kell a vizsgálat idejére azonosítani és rendelkezésre bocsájtani.
- Minden eljárást, követelményt és jogosultságot dokumentálni kell.

Azért, hogy az auditáló eszköz helytelen használatát vagy kompromittálását elkerüljük, az auditáló eszközhöz való hozzáférést csak a korábban jóváhagyott személyeknek lehet engedélyezni.

2.9. Eltérések

Az eljárási irányelvtől való olyan eltérés, amely csökkenti a biztonsági szintet, csak az illetékes területekkel [Ld. 3.1. sz. fejezet 8.] való egyeztetés alapján és kizárólag időben korlátozott módon megengedett.

3. További dokumentációk, mellékletek

Dokumentum	Leírás
1.	A programozható logikai vezérlőket (SPS) és a robotvezérlőket zárható szekrényben kell megőrizni vagy más megfelelő, alkalmas intézkedésekkel kell biztosítani. A hozzáférést csak jogosultaknak szabad engedélyezni. A programozható logikai vezérlőket (SPS) és a robotvezérlőket csak olyan hálózatokon lehet üzemeltetni, amelyeken csak az a kommunikáció engedélyezett, ami az üzlet számára feltétlenül kötelező.
2.	A változtatásokra és az aktualizálásokra vonatkozó információk közzététele kizárólag az Audi Hungaria mynet-en keresztül történik.
3.	Az ebből a szempontból lényeges dokumentumok és információk az *Audi Hungaria Jogi és Compliance Osztály intranetes oldalán találhatóak.*
4.	Az IT rendszer egy olyan átfogó rendszer, ami magában foglal minden hardver és szoftver komponenst, a kommunikációs kapcsolatokat is beleértve
5.	A dokumentumokat az AUDI HUNGARIA Zrt. igazgatóságának 022. számú irányelve - Dokumentumok megőrzése szerint kell archiválni.
6.	A vírusvédelmi szoftverek kiválasztását, validálását a Vírus Competence Center (VCC) végzi.
7.	A személyre vonatkozó auditokat az adatvédelmi testületnek kell írásban engedélyeznie. Az illetékes személyügyi vezetés és az üzemi tanács bevonását is biztosítani kell.
8.	Felelősség: IT-biztonság szervezeti egység.
9.	Felelősség: Azon munkatársak, akik meghatározott feladat alapján telepítési jogosultsággal rendelkeznek pl. IT Infrastruktúra, kulcsfelhasználó.
10.	A verziók és a javítási állapotokat az AUDI HUNGARIA Zrt. igazgatóságának 022. számú irányelve - Dokumentumok megőrzése szerint kell archiválni.
11.	A nemzeti törvények az elektronikus aláírás elismerésére: Magyarországon az elektronikus aláírásról szóló törvény érvényes. Ebben határozták meg a nemzeti törvényes keretfeltételeket az elektronikus aláírások bevezetése esetén. Az elektronikus aláírásról szóló 2001. évi XXXV. törvényünk (Eat.) alapja az elektronikus aláírásra vonatkozó közösségi keretfeltételekről

	szóló 1999. december 13-i 1999/93/EK Európai Parlament és Tanács irányelve, amely 2001. június 12-én lépett hatályba. A törvény olyan keretfeltételeket teremt meg, amelyek betartásával egy minősített elektronikus aláírást minimum a sajátkezű aláírással egyenértékűnek ismernek el. Olyan követelményeket tartalmaz, hogy mikor egyenértékű az elektronikus aláírás az elektronikus aláírási törvény alapján sajátkezű aláírással. Ennek eredményeként az elektronikus aláírásról szóló törvény alapján készült elektronikus aláírások magas szintű biztonságát a bíróság is elismeri.
12.	Felelősség: Jogi és Compliance osztály.

IT-biztonsági eljárási irányelvek rendszerfejlesztők részére

Verzió: 4.0 (2018.05.11.)
Kiadó: IT-biztonság
Szabályozás száma: 10 Felsőszintű szabályozás

Érvényességi kör

Az eljárási irányelvek az AUDI HUNGARIA Zrt. (továbbiakban úgy is mint „Audi Hungaria”, ill. „Megbízó”) számára szolgáltatást végző partnerekre (továbbiakban úgy is mint „Megbízott”) vonatkoznak.

Tartalom

1. Cél 39
2. Szabályozások 39
2.1. A szervezet saját értékeinek menedzsmentje 39
2.2. Üzem- és kommunikációmenedzsment 39
2.3. Hozzáférés engedélyezés 39
2.4. IT rendszerek beszerzése, fejlesztése és karbantartása 40
2.4.1. IT rendszerek biztonsági követelményei 40
2.4.2. Alkalmazások helyes kidolgozása 42
2.4.3. Titkosítási eljárások 42
2.4.4. Rendszeradatok biztonsága 43
2.4.5. Fejlesztési és támogatási folyamatok biztonsága 43
2.5. Az előírások betartása 44
2.6. Felelősség ..... **Hiba! A könyvjelző nem létezik.**
3. További dokumentációk, mellékletek 44

1. Cél

Ebben a munkautasításban definiáljuk az információk és IT eszközök használatára (pl.: személyi számítógépek, workstation-ök, notebookok, smartphone-ok, tablet pc-k) vonatkozó, rendszerfejlesztők által betartandó IT biztonsági szabályokat.

Az IT biztonsági eljárási irányelvek az információk bizalmasságának, integritásának, rendelkezésre állásának és követhetőségének védelmét, valamint a vállalat és minden olyan természetes és jogi személy jogainak és érdekeinek védelmét szolgálja, akik üzleti kapcsolatban állnak az AUDI HUNGARIA Zrt-vel, illetve a társaságnál dolgozókkal.

2. Szabályozások

2.1. A szervezet saját értékeinek menedzsmentje

Az információkért mindenkor azok tulajdonosa, adatgazdája viseli a felelősséget. Ez akkor is érvényes, ha az információkat IT rendszerek állítják elő. (Egyes feladatok delegálása természetesen ennek ellenére lehetséges.)

2.2. Üzem- és kommunikációmenedzsment

Az IT-biztonságot érintő tevékenységeket alapvetően az AH belső személyeinek kell ellátniuk. Ha ez nem lehetséges, akkor követő ellenőrző intézkedéseket kell a külső szolgáltató tevékenységéhez előirányozni:

- Egy IT rendszer erőforrás igényeit a tervezés alatt meg kell határozni.
- Egy IT rendszer biztonsági követelményeit a tervezés alatt az információtulajdonossal kell definiálni és dokumentálni.
- A rendszertervezést (Szakmai koncepció, Rendszertervezés, Rendszermegvalósítás) és –átvételt (Rendszerbevezetés) a konszern érvényes rendszerfejlesztési standardja (pl.: (IT-PEP) Rendszerfejlesztési folyamat) alapján kell végrehajtani.
- Azokat az információkat, melyeket nyilvánosan hozzáférhető IT rendszerek hoznak létre, a megfelelő biztonsági intézkedésekkel (pl.: azonosítási információk titkosított átvitele) kell a jogosulatlan változtatástól védeni.

2.3. Hozzáférés engedélyezés

Jogosultsági mechanizmusokat kell bevezetni és az információtulajdonos által meghatározott szerep és jogosultsági koncepciót kell követni.

A rendszerfelelősök kötelezettsége, az irányelveknek megfelelő, biztonságos bejelentkezési eljárás bevezetése. (pl.: erős authentikáció PKI kártya segítségével).

Megfelelő intézkedésekkel kell megakadályozni a felhasználói azonosítók és jelszavak próbálgatását. (pl.: minden téves próbálkozás után hosszabb várakozási idő és/vagy bizonyos számú téves próbálkozás után zárolás).

A rendszerfelelősöknek a megfelelő rendszerek bevezetésével kell támogatni a jelszóképzés minimális elvárásait.

A jelszavakat tikosként kell besorolni és ennek megfelelően kezelni.

A párbeszéd-kapcsolatokat, melyeket hosszabb ideje már nem használnak aktívan, ki kell kapcsolni vagy a megfelelő intézkedésekkel kell védeni.

2.4. IT rendszerek beszerzése, fejlesztése és karbantartása

2.4.1. IT rendszerek biztonsági követelményei

IT rendszerek fejlesztése és bevezetése előtt a szükséges IT biztonsági követelményeket (pl.: patch menedzsment) azonosítani és implementálni kell.

Az információk kezelésére vonatkozó szabályozások az IT rendszerekre (pl.: adatbázisok, háttértárak) is vonatkoznak.

2.4.1.1. Dokumentált üzleti folyamatok

Az információkat a besorolásuk alapján kell védeni a jogosulatlan hozzáféréstől. A besorolási bizalmasságra vonatkozó óvintézkedések:

Besorolás	Definíció
Nyilvános	• Rendszererősítés (csak a szükséges szolgáltatások, aktuális biztonsági patchek)
Belső	További intézkedések a „Nyilvános”-hoz: • Hozzáférési védelem („Ismeret, csak ha szükséges” elv alapján) • 1- lépcsős-azonosítás (pl.: User-ID és jelszó)
Bizalmas	További intézkedések a „Belső”-höz: • 2-lépcsős-azonosítás (pl.: smartcard PIN kóddal) – különösen az alkalmazások elérésekor vagy egy további biztosítás, mint a járulékos azonosított tároló titkosítás. (pl.: titkosított adatok a megosztáson vagy titkos usb-stick) • Adatcsatorna titkosítás
Titkos	További intézkedések a „Bizalmas”-hoz: • 2-lépcsős-azonosítás (pl.: smartcard PIN kóddal) – különösen alkalmazások eléréséhez • Adatcsatorna titkosítás • Tároló titkosítás

2.4.1.2. Adatok egységének védelme

Az információkat védeni kell besorolásuk szerint az akaratlan változtatástól és a jogosulatlan manipulációktól. A besorolt integritásra vonatkozó óvintézkedések:

Besorolás	Definíció
Alacsony	• Rendszererősítés (csak a szükséges szolgáltatások, aktuális biztonsági patchek)
Közepes	További intézkedések a „Alacsony”-hoz: • Hozzáférési védelem („Ismeret, csak ha szükséges” elv alapján) • 1- lépcsős-azonosítás (pl.: User-ID és jelszó)
Magas	További intézkedések a „Közepes”-hez: • A bemenő és kijövő adatok ellenőrzése, úgymint hibacsökkentése irányuló belső feldolgozások ellenőrzése és standard támadások, mint a Buffer-Overflow és a végrehajtható kódok becsempészésének megelőzése. (pl.: határok ellenőrzése, területek korlátozása speciális körre)
Nagyon magas	További intézkedések a „Magas”-hoz: • 2-lépcsős-azonosítás (pl.: smartcard PIN kóddal) a módosítási hozzáférésekhez. • Az elhelyezett adatokhoz vagy digitális aláírások képzése és ellenőrzése vagy hasonló védelmi mechanizmusok.

2.4.1.3. A követhetőség védelme

Az információkhoz való hozzáférés és az információkon történt változtatások követhetőségét besorolásuk szerint kell biztosítani. A besorolt követhetőségre vonatkozó óvintézkedések:

Besorolás	Definíció
Alacsony	• Rendszererősítés (csak a szükséges szolgáltatások, aktuális biztonsági patchek) • Fellépő hibák, bejelentkezési próbálkozások, standard rendszer dokumentálása, stb.
Közepes	További intézkedések a „Alacsony”-hoz: • A módosítási hozzáférések esetén User-ID, rendszeridő és változtatás módjának (hozzáadás, törlés, változtatás) naplózása. • 1-lépcsős-azonosítás (pl.: User-ID és jelszót) a módosítási hozzáférések esetén.
Magas	További intézkedések a „Közepes”-hez:

	• A módosítási hozzáférések esetén User-ID, rendszeridő és változtatás olyan naplózása, ami lehetővé teszi a változás állapotának felismerését.
Nagyon magas	További intézkedések a „Magas”-hoz: • Olvasási hozzáférésekhez User-ID és rendszeridő naplózása. • 2-lépcsős-azonosítás (pl.: smartcard PIN kóddal) olvasási és módosítási hozzáférésekhez.

2.4.1.4. A rendelkezésre állás védelme

Az IT rendszerek rendelkezésre állását a besorolásuknak megfelelően kell biztosítani. A besorolt rendelkezésre állásra vonatkozó óvintézkedések:

Besorolás	Definíció
Alacsony	• Rendszererősítés (csak a szükséges szolgáltatások, aktuális biztonsági patchek) • A kiesési idő több lehet, mint 72 óra. (Ehhez be kell vezetni a szükséges intézkedéseket.)
Közepes	• Rendszererősítés (csak a szükséges szolgáltatások, aktuális biztonsági patchek) • A kiesési idő nem lehet több 72 óránál. (Ehhez be kell vezetni a szükséges intézkedéseket.)
Magas	• Rendszererősítés (csak a szükséges szolgáltatások, aktuális biztonsági patchek) • A kiesési idő nem lehet több 24 óránál. (Ehhez be kell vezetni a szükséges intézkedéseket.)
Nagyon magas	• Rendszererősítés (csak a szükséges szolgáltatások, aktuális biztonsági patchek) • A kiesési idő nem lehet több 1 óránál. (Ehhez be kell vezetni a szükséges intézkedéseket.)

2.4.2. Alkalmazások helyes kidolgozása

Az IT rendszerek biztonságát olyan intézkedések bevezetésével kell garantálni, melyek a konszern érvényes rendszerfejlesztési standardját (pl.: IT-PEP) követelik meg.

IT rendszerek bevezetésekor a tanácsadást illetően az adott konszernvállalat üzemeltetési megállapodásai és szabályozásai érvényesek. [lásd 3. fejezet 1.]

2.4.3. Titkosítási eljárások

Titkosítási eljárások stratégiájára, bevetésére és kezelésére vonatkozó alapvető döntéseket az erre illetékeseknek kell meghozniuk. [lásd 3. fejezet 2.]

Titkosítási termékek kiválasztásakor a figyelembe kell venni a „Book of standards”-ot.

Alkalmazás specifikus titkosítási szoftver használata esetén a kibontáshoz szükséges eszközöket át kell adni.

A tanúsítványoknak időben korlátozott az érvényessége. Egy aláírási tanúsítvány érvényességének lejárata előtt ("content commitment" ill. "non repudiation" kulcshasználat) az azzal aláírt adatokat egy hosszabb érvényességű kulccsal kell átírni.

2.4.4. Rendszeradatok biztonsága

2.4.4.1. Teszt adatok védelme

A fejlesztési- és tesztkörnyezeteket, valamint a produktív IT rendszereket, a berendezések kivételével, szét kell választani egymástól.

A tesztekhez lehetőség szerint tesztadatokat kell létrehozni. (pl.: tesztadat generátorok segítségével).

A szoftver tesztelése csak az erre a célra szolgáló tesztkörnyezetben engedélyezett. Itt meg kell győződni arról, hogy az éles üzem nem sérülhet.

Személyekre vonatkozó, bizalmas vagy titkos adatokat az éles IT rendszerből a tesztrendszerekbe történő átvétel előtt úgy kell módosítani, hogy az eredeti adatokra lehetetlen legyen visszakövetkeztetni, (ezekhez az adatokhoz olyan személyek is hozzáférést kapnak, akiknek a szerződésben foglalt munkájuk teljesítéséhez ezekre nincs szükségük).

Futó IT rendszerekből nyert információk másolása és használata csak az adatgazda előzetes beleegyezése után engedélyezett. A másolt adatokra ugyanazon IT biztonsági szabályozások vonatkoznak, mint az eredeti adatokra.

A futó IT alkalmazásokból nyert felhasznált információkat a tesztek elvégzése után törölni kell.

A működő IT rendszerekre vonatkozó hozzáférési jogokat a tesztalkalmazásoknál is figyelembe kell venni.

2.4.4.2. Forráskódok hozzáférés-ellenőrzése

A program forráskódokat osztályozni kell, és ennek megfelelően is kell védeni.

2.4.5. Fejlesztési és támogatási folyamatok biztonsága

Minden IT rendszert érintő folyamatot és eljárást úgy kell kialakítani, hogy az elérhető legmagasabb IT biztonsági szintet érjük el és azt tartsuk is meg.

Változásellenőrzési eljárást (Change Management) kell alkalmazni és biztosítani kell, hogy az IT rendszerek biztonsága és ellenőrzési eljárásai a változtatások miatt nem sérülnek.

Ha a megvásárolt szoftvercsomagokon változtatásokat hajtunk végre, akkor vizsgálni kell a meglévő szabályozásokra és biztonsági intézkedésekre gyakorolt hatásait. A változtatások csak akkor engedélyezettek, ha ez licencjogilag és a karbantartási szerződések alapján is megengedett.

2.5. Az előírások betartása

Titkosítás és/vagy elektronikus aláírás használatakor, különös tekintettel országhatáron túl, figyelembe kell venni az adott ország Importra/Exportra/Hozzáférésre illetve Hardverre/Szoftverre/Információkra vonatkozó szabályozásait.

Az ország specifikus szabályozásokkal kapcsolatos kérdésekben az illetékesekkel kell felvenni a kapcsolatot [lásd 3. sz. fejezet 3.].

2.6. Eltérések

Az eljárási irányelvtől való olyan eltérés, amely csökkenti a biztonsági szintet, csak az illetékes területekkel [Ld. 3.1. sz. fejezet 2.] való egyeztetés alapján és kizárólag időben korlátozott módon megengedett.

3. További dokumentációk, mellékletek

Dokumentum	Leírás
1.	A közös döntést igénylő IT rendszerekkel kapcsolatban az Üzemi tanács – IT közös bizottsága hozhat döntést.
2.	IT-biztonság szervezeti egység.
3.	Jogi és Compliance Osztály szervezeti egység
4.	AH Adatvédelmi Testület