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, továbbá adatkezeléssel és adatfeldolgozással járó tevékenységekre 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 vagy 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. Partner a Szerződés teljesítése során köteles betartani az általa kezelt és feldolgozott adatokra vonatkozó Megrendelői előírásokat. Az adott Szerződés keretében érintett adatok besorolása a bizalmasság, integritás és rendelkezésre állás szerint kerül elkészítésre a Megrendelő által (továbbiakban: adatbesorolás). Az adatbesorolásra vonatkozó részletes előírásokat az ÁIF 1. számú melléklete tartalmazza. Az adatbesorolás és titoktartási kötelezettség megállapításának keretében meghatározásra kerül a „Trusted Information Security Assessment Exchange” (továbbiakban: TISAX) relevancia is. Amennyiben a megrendeléshez / szerződéses

megbízáshoz a kért dokumentumoknak megfelelő TISAX igazolásra van szükség, a Partner vállalja, hogy ezt igazolja, vagy beszerzi a TISAX igazolást. A TISAX-igazolás megszerzésének időtartama nem haladhatja meg a Szerződés elfogadását követő 12 hónapot, kivéve, ha a tárgyalási jegyzőkönyv eltérő rendelkezést határoz meg. A TISAX relevanciával rendelkező Szerződés esetében Partner köteles az AUDI konszern TISAX ellenőrzési folyamatait betartani. A Megrendelő a TISAX tanúsítási folyamat részletes lépéseiről, illetve az elvégzendő intézkedésekről – az aktuálisan fennálló TISAX tanúsítási folyamat alapján – írásban tájékoztatja a Partnert.

4.3. Megrendelő erre vonatkozó igénye esetén a Partner által fejlesztett vagy biztosított IT rendszernek meg kell felelnie az OWASP Application Security Verification Standard Project és OWASP Top Ten Project ajánlásai alapján végrehajtott penetrációs teszten. A penetrációs tesztet Megrendelő és/vagy külső partnere végzi el. Partner igénye alapján lehetőség van általa elvégeztetett penetrációs teszt eredményt bemutatni, amelyet Megrendelővel írásban köteles egyeztetni és elfogadtatni. A Partner által bemutatott Penetrációs teszt jegyzőkönyv és intézkedési terv nem lehet 1 évnél régebbi. A Megrendelő által írásban elfogadott Partner által bemutatott penetrációs teszt kiválthatja a Megrendelő és/ vagy külső Partnere által elvégzett penetrációs tesztet.
Partner köteles a penetrációs teszt által feltárt IT-biztonsági gyenge pontokat és hiányosságokat legkésőbb az üzemeltetésre történő átadásig kijavítani, és Megrendelővel a kijavítást jóváhagyatni.

4.4. 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.

4.5. Partner köteles az IT-biztonsági elvárások maradéktalanul betartása mellett 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.

4.6. Partner köteles rendszeresen (legalább évente) ellenőrizni, hogy a Partner felhasználói jogosultságai megfelelnek-e feladataiknak. A jogosultságokat szükség esetén megfelelően módosítani szükséges. A Partner a jogosultságok felülvizsgálatának eredményéről írásban tájékoztatja Megrendelőt.

4.7. 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.

4.8. Az információbiztonsági incidensek gyors, hatékony és egységes kezelése érdekében a Megrendelő információbiztonsági incidenskezelési eljárásai a Partner részéről kötelezően betartandóak az adott szolgáltatás elindulásától kezdődően. A Partner köteles a Megrendelőnek nyújtott szolgáltatásokat vagy adatait érintő információbiztonsági incidensekről minden esetben haladéktalanul írásbeli értesítést küldeni a Megrendelő részére (CERT-AudiHungaria@audi.hu). A Megrendelő az információbiztonsági incidenskezelés eljárásáról, illetve az elvégzendő intézkedésekről - az aktuálisan fennálló információbiztonsági incidens figyelembe vételével - írásban tájékoztatja a Partnert.

4.9. 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.

4.10. 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.

4.11. Valamennyi Partner köteles a jelen ÁIF 1. számú mellékletében („Információbiztonsági eljárási irányelvek külsős munkatársak, partnercégek számára”) foglaltakat betartani.

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: 2021.07.29. mely időponttal hatályát veszti a 2020.01.15. napján kiadott Általános Információtechnológiai Feltételek.

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

Általános Információtechnológiai Feltételek 1. számú melléklet - Információbiztonsági eljárási irányelvek külsős munkatársak, partnercégek számára

Verzió: 2.0 (2020.01.13.)
Kiadó: Jogi Osztály
Vállalati irányelv felelős: IT-Biztonság/Governance
Szabályozás száma: Információbiztonság Vállalati irányelv U_1.018 4. sz. melléklet

---

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 „Szolgáltató"), valamint teljesítési segédeire (a továbbiakban: közreműködők) vonatkoznak.

1 Cél

A jelen információbiztonsági eljárási irányelvek meghatározzák azokat az információbiztonságra vonatkozó szabályokat, amelyeket a szolgáltatók kötelesek betartani az információk és IT-eszközök (pl. számítógépek, munkaállomások, laptopok, okostelefonok vagy tabletek) kezelése során.

Szolgáltatónak számít minden harmadik személy, aki szerződéses jogviszonyok alapján szolgáltatást nyújt az AUDI HUNGARIA-nak, A jelen cselekvési irányelvek a szolgáltatók ügyvezetőinek, munkatársainak, valamint teljesítési segédeinek (pl. alvállalkozóinak) (a továbbiakban: közreműködők) szólnak.

Ezen információbiztonsági eljárási irányelv célja az információk bizalmasságának, integritásának és rendelkezésre állásának biztosítása, valamint a megbízó és minden olyan természetes és jogi személy jogainak és érdekeinek védelme, amelyek üzleti kapcsolatban állnak a megbízóval és/vagy tevékenységet folytatnak számára.

1.1 Rövidítések és meghatározások

Rövidítés/fogalom	Magyarázat
Az információ létrehozója	Az a személy vagy személyek csoportja, aki/amely létrehoz bizonyos információkat vagy egy dokumentumot. A létrehozó az információtulajdonos által meghatározott besorolási szint szerint köteles a dokumentumot/információt besorolni/megjelölni.
Információtulajdonos	Az a személy vagy személyek csoportja, akit/amelyet a vezetőség megbízott bizonyos bizalmas információk védelmével. Az információk élettartama során az információtulajdonos személye változhat.

2 Dokumentumszerkezet és célcsoport

A jelen dokumentum három fejezetből áll. Az alábbi táblázat bemutatja a dokumentum szerkezetét és a fejezetenkénti célcsoportokat.

Fejezet	Célcsoport	Megjegyzések
3	Minden szolgáltató	A jelen fejezet előírásait minden szolgáltató köteles betartani. A további előírásokat a 4. és 5. fejezet tartalmazza, amelyet a konszern hálózatához és rendszereihez való hozzáférési lehetőségek függvényében kell betartani.
4	Szolgáltatók, amelyek hozzáférnek a konszern hálózatához és rendszereihez	Be kell tartani továbbá az 3. fejezetben található előírásokat is.
5	Szolgáltatók, amelyek nem férnek hozzá a konszern hálózatához és rendszereihez	Be kell tartani továbbá az 3. fejezetben található előírásokat is.

3 Általános előírások

Minden szolgáltató köteles a jelen dokumentumban található meghatározások szerint az alábbi előírásokat betartani.

A megbízóra vonatkozó előírások nem képezik jelen dokumentum részét.

3.1 Szervezeti követelmények

A nem a megbízó által rendelkezésre bocsátott IT-eszközöknek a cég területére vagy a megbízó biztonsági területeire történő bevitelére az AUDI HUNGARIA szabályozásai érvényesek.

A megbízó tulajdonát képező adatok vagy szoftverek nem használhatók olyan IT-rendszereken vagy tárolóeszközökön, amelyeket nem a megbízó vagy a szolgáltató bocsátott rendelkezésre, illetve nem hagyta azokat jóvá.

Be kell tartani az U_1.018 32. mellékletben meghatározott szabályokat valamennyi olyan külső, hordozható adathordozó eszköz vonatkozásában, amelyen keresztül kártékony kód futása megvalósulhat, illetve ártó kódot tárolhat.

Az AUDI HUNGARIA tulajdonát képező adatok vagy szoftverek nem használhatók olyan fájlszolgáltatónál vagy internetes felhőalapú szolgáltatónál, amelyet a megbízó nem hagyott jóvá.

Az adatok harmadik fél felé történő továbbítása csak a megbízó adattulajdonosa által adott írásbeli jóváhagyás alapján lehetséges.

Be kell tartani a megbízó személyes adatok gyűjtésére, feldolgozására és használatára vonatkozó (lásd 7.2.1 függelék) szabályozásait.

A szolgáltató ügyvezetése köteles a munkatársait a megbízó és a szolgáltató között fennálló titoktartási megállapodás szerinti titoktartásra kötelezni. A megbízó mindenkor jogosult betekinteni ezekbe a megállapodásokba.

A megbízó mobil rendszereken vagy IT-eszközökön tárolt adatait a legkorszerűbb technológiának megfelelő hardverrel vagy szoftverrel kell titkosítani. A titkosítással és hitelesítéssel kapcsolatos további követelmények a konszern beszállítói portálján (lásd 7.2.2 függelék) találhatók.

Külföldre történő utazást megelőzően figyelembe szükséges venni az adott országban a biztonsági technológiák (pl. titkosítás) használatára vonatkozó érvényes előírásokat.

A szerződés lejártakor a megbízó adatait át kell adni a megbízónak és törölni kell a szolgáltató eszközeiről és adattárolóiról. Be kell tartani a törvényi előírásokat (pl. megőrzési határidőket).

3.2 Személyi biztonság

Azokat a felhasználói azonosítókat vagy a megbízó adataihoz való hozzáféréseket, amelyekre már nincs szükség, a megfelelő zárolás/törlés elvégzése érdekében az érintett felhasználó haladéktalanul köteles jelenteni a megbízást adó szerv (pl. a megbízó illetékes felhasználói adminisztrátora) felé.

Azokat az azonosítási médiumokat, amelyekre már nincs szükség (pl. Smartcardok, SecurID-kártyák), haladéktalanul vissza kell adni a megbízást adó szervnek.

A használatra átadott eszközöket (pl. laptopokat) és adathordozókat, illetve adattárolókat a szerződés lejártakor, vagy amennyiben azokra már nincs szükség, vissza kell adni a megbízónak.

A felhasználónak átadott IT-eszközök vagy a hitelesítésre használt médiumok elvesztését a felhasználó haladéktalanul köteles jelenteni a megbízó illetékes szerv (lásd 7.2.3 függelék) felé.

3.3 Fizikai és környezettel kapcsolatos biztonság

A megbízó adatait tároló vagy kezelő IT-eszközöket úgy kell használni, hogy az adatokba illetéktelen személy ne tekinthessen be vagy ne férhessen hozzá azokhoz. Különös elővigyázatosság szükséges a mobil rendszerek használata során.

Az illetéktelen betekintés elkerülése érdekében bizalmas vagy titkos adatokat soha nem szabad felügyelet nélkül hagyni.

3.4 A szervezeti értékek kezelése

3.4.1. A besorolásra vonatkozó szabályozások

A besorolást a három védelmi cél – a bizalmasság, az integritás és a rendelkezésre állás – alapján kell elvégezni minden információ és adatfeldolgozó IT-rendszer vonatkozásában.

A szolgáltató köteles a megbízótól beszerezni a bizalmasság, az integritás és a rendelkezésre állás alapján történő besorolást (az adott szolgáltatások köre vonatkozásában).

Az információkat (védelmi cél: bizalmasság) teljes élettartamuk alatt a bizalmassági besorolásuknak megfelelő intézkedésekkel kell védeni a jogosulatlan hozzáféréssel szemben. A bizalmassági besorolásokhoz lejárati idő adható meg.

Szükség esetén az adott folyamat tulajdonos az adatkezelés során köteles ellenőrizni és meghatározni az integritás és a rendelkezésre állás alapján történő besorolást. A jelen besorolást az információtulajdonos bevonásával rendszeresen értékelni és szükség esetén módosítani kell.

Az információtulajdonosnak igazolnia kell a helyes besorolást.

3.4.1.1. Titoktartás

A nem minden munkatársnak címzett információkat csak az arra jogosultak számára szabad hozzáférhetővé tenni (a „csak a legszükségesebb információk"-elve alapján).

Az információk létrehozóira és tulajdonosaira vonatkozó előírások:

- A létrehozó (lásd 1.1 - Az információ létrehozója) köteles megjelölni az újonnan létrehozott információkat és adatokat.
- Az információtulajdonos (lásd 1.1 - Információtulajdonos) felelős a besorolásért
- A létrehozó köteles bekérni az információtulajdonostól a helyes besorolást.
- A bizalmassági besorolást minden IT-rendszerre vonatkozóan el kell végezni.
- Ha a besorolás még nem egyértelmű, pl. újonnan létrehozott dokumentumok/IT-rendszerek esetén, akkor a „bizalmas" besorolást kell kiválasztani.
- Belső, bizalmas és titkos információk esetén az információtulajdonos (legkésőbb a következő felülvizsgálat és frissítés alkalmával) köteles ellenőrizni, hogy helyes-e a meglévő bizalmassági besorolás, és ezt köteles megfelelő módon jelölni is.

A címzettekre vonatkozó előírások:

- A nem jelölt információkat és adatokat „belső"-ként kell kezelni.
- A besorolással kapcsolatos bizonytalanság esetén fel kell venni a kapcsolatot az információtulajdonossal.

Az információk bizalmas jellegére vonatkozóan az alábbi meghatározott besorolási szintek léteznek:

Besorolás	**Meghatározás**
Nyilvános	Minden korlátozástól mentes, például a sajtóban vagy az interneten közzétehető információk. A vállalati információk nyilvános használatához az illetékes szerv hozzájárulása szükséges (lásd 7.2.4 függelék). Példák: sajtóközlemények, ügyfeleknek szánt termékkatalógusok
Belső	Olyan információk, amelyek arra nem jogosult személyek általi ismerete vagy visszaélésszerű továbbadása vagy felhasználása csak kis mértékben befolyásolja a termék- és projektcélok elérését, ezért jogosult személyek számára hozzáférhetővé tehetők. A bizalmasság megsértése negatív – akkor is, ha csak csekély mértékű – következményekkel járhat. Példa: • nem valószínű, hogy egyes személyek vagy szervezetek kártérítési igényt támasztanak Példák: üzleti kommunikációs adatok (telefonszám vagy e-mail cím), üzemi munkavédelmi előírások, munkarend

Bizalmas	Olyan információk, amelyek arra nem jogosult személyek felé történő közzététele vagy nyilvánosságra hozatala veszélyeztetheti a termék- és projektcélok elérését, ezért kizárólag feljogosított személyek zárt csoportja számára tehetők hozzáférhetővé. A bizalmasság megsértése előre láthatóan mérhető negatív következményekkel fog járni, pl.: • ügyfelek elvesztése • értékesítési számok/forgalom visszaesése • egyes személyek vagy szervezetek kártérítési igényei Példák: az üzleti kommunikációs adatokon túlmenő személyes adatok (pl. fizetés), költségvetés tervezése, felülvizsgálati jelentések
Titkos	Olyan információk, amelyek arra nem jogosult személyek számára történő közzététele vagy nyilvánosságra hozatala súlyosan veszélyeztetheti a vállalati célok elérését, ezért kizárólag korlátozott számú személyek számára tehetők hozzáférhetővé szigorú ellenőrizés mellett. A bizalmasság megsértése jelentős mértékű, negatív hatással van a vállalatról kialakult képre, illetve a vállalat megjelenésére, és gazdasági következményekkel jár, pl.: • jelentős ügyfélvesztés • értékesítési számok/forgalom erős visszaesése • különböző személyek vagy szervezetek kártérítési igényei • bizonyos piaci területekről történő kizárás • negatív hatások a nyilvános megítélés terén Példák: személyes adatok különleges típusai (pl. egészségügyi adatok), ciklustervek, stratégiai vállalati tervek, prototípusok tervrajzai

3.4.1.2. Integritás

Biztosítani kell a hibátlan információkezelést és az illetéktelen módosítások elleni védelmet.

Az információk integritására vonatkozóan az alábbi meghatározott besorolási szintek léteznek:

Besorolás	**Meghatározás**
Alacsony	Az integritás megsértése nincs előre látható hatással az üzleti tevékenységre vagy a vállalatról kialakult képre, illetve a vállalat megjelenésére.
Közepes	Az integritás megsértése csak csekély hatással van az üzleti tevékenységre és/vagy a vállalatról kialakult képre, illetve a vállalat megjelenésére. Negatív – akkor is, ha csak csekély mértékű – következményekkel járhat. Példák: • a munkafolyamatok kis mértékű elhúzódása • hibák, amelyek nincsenek hatással a munkaeredményekre (nincs kiesés a termelésben) • nincs negatív hatással a döntésekre • nem valószínű, hogy egyes személyek vagy szervezetek kártérítési igényt támasztanak Példák: telephelyi tervek, szervezeti ábrák, egyes belső telefonszámok

Magas	Az integritás megsértése érezhető hatással van az üzleti tevékenységre és/vagy a vállalatról kialakult képre, illetve a vállalat megjelenésére. Előre láthatóan mérhető negatív következményekkel fog járni, pl.: • ügyfelek valószínű elvesztése • értékesítési számok/forgalom valószínű visszaesése • a munkafolyamatok jelentős elhúzódása • hiba/hibás működés, amely látható hatással van a munkaeredményekre (komoly kiesés a termelésben) és/vagy egyes szolgáltatási folyamatok kiesése • negatív hatással a döntésekre/hibás döntések valószínűsége • valószínű, hogy egyes személyek vagy szervezetek kártérítési igényt támasztanak Példák: JIT-megbízások, sajtóközlemények, internetes megjelenés tartalma, termelésirányítási adatok
Nagyon magas	Az integritás megsértése jelentős hatással van az üzleti tevékenységre és/vagy a vállalatról kialakult képre, illetve a vállalat megjelenésére, és annak megfelelő következményekkel jár, pl.: • jelentős ügyfélvesztés • különböző személyek vagy szervezetek kártérítési igényei • értékesítési számok/forgalom erős visszaesése • bizonyos piaci területekről történő kizárás • a munkafolyamatok jelentős elhúzódása • hiba/hibás működés, amely súlyos hatással van a munkaeredményekre és/vagy több szolgáltatási folyamat kiesése (rendkívül komoly kiesés a termelésben) • jelentős negatív hatással a döntésekre/hibás döntések Példák: mérlegkészítés (pl. éves beszámoló), szabadalmak, kriptográfiai kulcsok, bérszámfejtés

3.4.1.3. Rendelkezésre állás

Az információknak rendelkezésre kell állniuk egy meghatározott időtartamban.

Az információk rendelkezésre állására vonatkozóan az alábbi meghatározott besorolási szintek léteznek:

Besorolás	Meghatározás
Alacsony	Az IT-rendszer rendelkezésre állása kiesés vagy nem elfogadható válaszidők vonatkozásában lehet kevesebb mint 95% anélkül, hogy ezáltal jelentős (anyagi vagy a vállalatról kialakított képet érintő) hátrány keletkezne. Példa: Intranet alkalmazás a munkatársaknak szóló általános információkkal
Közepes	Az IT-rendszer rendelkezésre állása kiesés vagy nem elfogadható válaszidők vonatkozásában legalább 95% kell legyen. Az alacsonyabb rendelkezésre állás jelentős (anyagi vagy a vállalatról kialakított képet érintő) hátrányhoz vezet. Példa: pályázói portál
Magas	Az IT-rendszer rendelkezésre állása kiesés vagy nem elfogadható válaszidők vonatkozásában legalább 98% kell legyen. Az alacsonyabb rendelkezésre állás jelentős (anyagi vagy a vállalatról kialakított képet érintő) hátrányhoz vezet. Példák: bérelszámolás, könyvelés

Nagyon magas	Az IT-rendszer rendelkezésre állása kiesés vagy nem elfogadható válaszidők vonatkozásában legalább 99% kell legyen. Az alacsonyabb rendelkezésre állás jelentős (anyagi vagy a vállalatról kialakított képet érintő) hátrányhoz vezet. Példa: IT-rendszer, amelynek kiesése közvetlen termeléslealláshoz vezet Jelentős hátrány lehet pl.: • ügyfelek elvesztése • különböző személyek, szervezetek vagy szövetségek kártérítési igényei • értékesítési számok/forgalom erős visszaesése • bizonyos piaci területekről történő kizárás • hiba/hibás működés, amely súlyos hatással van a munkaeredményekre és/vagy több szolgáltatási folyamat kiesése (rendkívül komoly kiesés a termelésben)

3.4.2. Információk jelölése és kezelése

Az információkat csak jogosultak bizonyos köre számára szabad hozzáférhetővé tenni a megállapodás szerinti tevékenységek céljából, a vonatkozó szabályozások betartása mellett. Mindeközben be kell tartani a „csak a legszükségesebb információk” elvét.

Az információkat a teljes élettartamuk során az aktuális bizalmassági besorolásuknak megfelelően kell védeni a jogosulatlan hozzáféréssel szemben. Az alábbi szabályozások vannak érvényben:

Besorolás	**Előírások**
Nyilvános	• Jelölés: nincs/opcionális (pl. megjegyzés az impresszumban) • Be kell tartani a besorolás jelölésének elhelyezésére vonatkozó vállalati előírásokat. • Sokszorosítás és szétosztás: nincsenek korlátozások • Tárolás: nincsenek korlátozások • Törlés: nincsenek korlátozások • Megsemmisítés: nincsenek korlátozások
Belső	• Jelölés: A bizalmassági szint megadása az adott ország nyelvén/nincs vagy „belső” jelölés van a dokumentum első oldalán • Be kell tartani a besorolás jelölésének elhelyezésére vonatkozó vállalati előírásokat. • Sokszorosítás és szétosztás: csak a konszern jogosult munkatársai és jogosult harmadik felek számára tevékenységük keretében, illetve alkalmazási területükön • Tárolás: jogosulatlan hozzáféréssel szembeni védelem • Törlés: az adatokat, amelyekre már nincs szükség, törölni kell. • Megsemmisítés: szabályszerű megsemmisítés (lásd 7.2.5 függelék)

Bizalmas	• Jelölés: A bizalmassági szint megadása az adott ország nyelvén/„bizalmas” jelölés a dokumentum minden oldalán elektronikus vagy nyomtatott formában • Be kell tartani a besorolás jelölésének elhelyezésére vonatkozó vállalati előírásokat. • Sokszorosítás és szétosztás: csak a konszern jogosult munkatársainak korlátozott köre és jogosult harmadik felek számára tevékenységük keretében, valamint alkalmazási területükön. A dokumentumokat szétosztó személy felelős a megfelelő elosztási csatornákért az információk és adatok illetéktelen hozzáféréssel és/vagy illetéktelen lehallgatással szembeni védelme érdekében (pl. titkosítás által). • Tárolás: hozzáférés csak a konszern jogosult munkatársainak korlátozott köre és jogosult harmadik felek számára tevékenységük keretében, valamint alkalmazási területükön (pl. zárt felhasználói csoportban). Megfelelő tárolási helyeket és/vagy adattárolókat kell alkalmazni. • A bizalmas dokumentumokat, ha nincs rájuk szükség, lezárt páncélszekrényben vagy olyan lezárt helyiségben kell tárolni, amelyeket csak arra jogosult személyek meghatározott csoportja nyithat fel. • Törlés: az adatokat, amelyekre már nincs szükség, törölni kell. • Megsemmisítés: szabályszerű megsemmisítés (lásd 7.2.5 függelék) • Hitelesítés: Erős hitelesítés (lásd 7.2.6 függelék) • Szállítás: A bizalmas dokumentumokat és adattárolókat zárt, semleges borítékban kell feladni; szükség esetén „személyes” jelöléssel lehet ellátni, ami azt jelenti, hogy a boríték csak közvetlenül a megjelölt címzettnek adható át.
Titkos	• Jelölés: A bizalmassági szint megadása az adott ország nyelvén/„titkos”jelölés a dokumentum minden oldalán • Be kell tartani a besorolás jelölésének elhelyezésére vonatkozó vállalati előírásokat. • Ezenkívül minden oldalt „x/y oldal” jelöléssel kell ellátni. • Sokszorosítás és szétosztás: csak a konszern jogosult munkatársainak szűk köre (pl. név szerinti lista) és jogosult harmadik felek számára tevékenységük keretében, valamint alkalmazási területükön az információtulajdonos előzetes engedélye alapján. Amennyiben műszakilag megoldható, minden adatot titkosítani kell a legkorszerűbb technológia szerint. Amennyiben ez nem lehetséges, hasonlóan erős biztonsági megoldást kell alkalmazni. Az alkalmazás függvényében további technikai, illetve szervezési óvintézkedéseket kell alkalmazni (pl. továbbítás és nyomtatás tilalma, vízjel). A kommunikációhoz megfelelő, a lehallgatást megakadályozó csatornákat kell alkalmazni (pl. titkosított videokonferencia). • Tárolás: hozzáférés csak a konszern jogosult munkatársainak szűk köre (pl. név szerinti lista) és jogosult harmadik felek számára tevékenységük keretében, valamint alkalmazási területükön (pl. zárt felhasználói csoportban). Amennyiben műszakilag megoldható, minden adatot titkosítani kell a legkorszerűbb technológia szerint. Amennyiben ez nem lehetséges, hasonlóan erős biztonsági megoldást kell alkalmazni. • A titkos dokumentumokat lezárt páncélszekrényben kell tárolni, amelyekhez külön zárakat kell használni. A titkos információkat tartalmazó mobil adathordozókat megfelelő adatszéfekben kell tárolni. • Törlés: az adatokat, amelyekre már nincs szükség, törölni kell. • Megsemmisítés: szabályszerű megsemmisítés (lásd 7.2.5 függelék) • Hitelesítés: Erős hitelesítés (lásd 7.2.6 függelék) • Szállítás: a titkos dokumentumokat és adattárolókat semleges, zárt külső borítékban („személyes”, „titkos” stb. jelölés nélkül) kell feladni, amelyben el kell helyezni egy „titkos” jelöléssel ellátott másik borítékot, amely a titkos dokumentumokat tartalmazza.

Az információk kezelésére vonatkozó előírások (jelölés, sokszorosítás, szétosztás, tárolás, törlés és megsemmisítés) az IT-rendszerekre (pl. adatbázisokra és biztonsági médiumokra) is megfelelően érvényesek.

3.4.3. Tároló és adathordozó eszközök kezelése

Az adathordozókat (pl. CD-k, DVD-k, USB-adattárolók és merevlemezek) védeni kell elvesztéssel, megsemmisítéssel és elcseréléssel, valamint jogosulatlan hozzáféréssel szemben.

A már nem használt adathordozókat biztonságos módon kell megsemmisíteni (lásd 7.2.5 függelék).

3.4.3.1. Információk cseréje

Minden bizalmas vagy titkos információt érintő vagy tartalmazó beszélgetés (beleértve a telefon-, video- és webkonferencia-beszélgetéseket is) során biztosítani kell, hogy azokat illetéktelen személyek ne tudják lehallgatni.

Az adatok rossz helyre történő továbbításának elkerülése érdekében a faxszámokat és e-mail címeket az aktuális jegyzékekből vagy a címzettől kell megszerezni.

IT-eszközök és adathordozók megbízó üzemén kívülre történő szállítása esetén be kell tartani az AUDI HUNGARIA szabályozásait (lásd 7.2.7 függelék).

Az e-mailek tartalmáért és megosztásáért a feladó, további feldolgozásukért és megosztásukért a címzett felelős.

Lánc-emailek létrehozása és küldése tilos.

3.5 Az információbiztonsági incidensek kezelése

A megbízó adatait vagy rendszereit érintő információbiztonsági incidenseket (pl. fellépő hibák vagy az információbiztonsági szabályozás megsértése) haladéktalanul jelenteni kell az illetékes szervnek (lásd 7.2.8 függelék).

Az IT-rendszer feltételezett sérülékeny pontjait és biztonsági réseit haladéktalanul jelenteni kell az illetékes szervnek (lásd 7.2.9 függelék). A sérülékeny pontok és biztonsági rések ellenőrzését (pl. behatolásvizsgálatot) csak az illetékes szerv végezheti (lásd 7.2.10 függelék).

A bizalmas vagy titkos információk feltételezett elvesztését haladéktalanul jelenteni kell az illetékes szervnek (lásd 7.2.11 függelék).

3.6 Megfelelőség és a törvényi előírások betartása

A szolgáltató köteles a jogi és vállalati előírásoknak (beleérve az erőforrások kezelését, belső ellenőrzési rendszert, IT szolgáltatásfolytonosság-menedzsmentet és az információk védelmét is) megfelelő megfelelőségi menedzsmentet (compliance management) létrehozni, amely magába foglalja a megbízó valamennyi információját, hardverét és szoftverét is.

A megfelelőségi menedzsment (compliance management) az alábbi pontokból kell álljon.

3.6.1. Korai kockázatfelismerés

Egy olyan folyamatot kell kialakítani, amely lehetővé teszi az IT-rendszereket és adatokat érintő kockázatok és lehetséges fenyegetések korai felismerését.

A felismert kockázatok kezeléséhez megelőző tevékenységeket és intézkedéseket kell megállapítani.

3.6.2. Szellemi tulajdon/licenckezelés

A szellemi tulajdonjogokkal kapcsolatos valamennyi jogot (pl. szoftverek dokumentumok és grafikák szerzői jogai, formatervezési minták, védjegy, szabadalmak és forráskódlicencek) tiszteletben kell tartani és ugyanakkor be is kell tartani őket.

Licenc nélküli szoftverek (kalózpéldányok) használata tilos.

A licenccel rendlelkező szoftverekre a szerzői jogra vonatkozó törvényi előírások érvényesek (pl. másolatok készítése, kivéve biztonsági és archiválási céllal, a szerzői jog megsértésével jár).

A jelen rendelkezések megsértése büntetőjogi következményekkel járhat, és ideiglenes intézkedést vagy kártérítési követelést vonhat maga után.

A licenccel rendelkező szoftverek csak a megállapodás szerinti célra az érvényes előírások és a gyártóval kötött licencmegállapodás betartása mellett használhatók.

3.6.3. Adatvédelem

Be kell tartani az érvényes adatvédelmi jogszabályokat és előírásokat.(lásd 7.2.12 függelék).

A szolgáltató ügyvezetése köteles a közreműködőt kötelezni a törvényben előírt adatvédelmi előírások betartására (lásd 7.2.12 függelék).

3.6.4. A szerződés rendelkezéseinek való megfelelőség

A szolgáltató IT-szervezete köteles betartani a megbízó szerződésben rögzített előírásait. A szerződéses előírások érvényesítése érdekében a szolgáltató saját szervezeti szabályozásainak ellenőrzését és mindenkori aktualizálását lehetővé tevő intézkedéseket kell alkalmazni.

3.6.5. Belső szabályozás

Az előírások betartása és a megbízó információinak, hardvereinek és szoftvereinek megfelelő kezelése érdekében a szolgáltatók kötelesek munkatársaik számára szabályozásokat és viselkedési alapelveket előírni.

3.7 Szabálysértések és a szabályok betartatása

Az információbiztonsági cselekvési irányelvek megsértése esetenként, az érvényes vállalati, szerződéses és törvényi előírások és megállapodások alapján kerül kivizsgálásra és megfelelő jogkövetkezményt von maga után.

4 A konszern belső hálózatához közvetlen hozzáféréssel rendelkező szolgáltatókra vonatkozó további követelmények

4.1 Meghatározás

Az alábbi kategóriák valamelyikéhez tartozó szolgáltatók kötelesek betartani az alábbi előírásokat:

- szolgáltatók, amelyek klienseit (felhasználói készülékeit) a Volkswagen-konszern valamely leányvállalata bocsátotta rendelkezésre
- szolgáltatók, amelyek távoli hozzáféréssel (pl. TravelX, Safe, Secure i.Do-Client) vagy más VPN-megoldással közvetlen hozzáféréssel kapcsolódnak a Volkswagen Corporate Backbone-hoz (CBB)
- szolgáltatók, amelyek közvetlenül kapcsolódnak a CBB-hez
- szolgáltatók, amelyek PFN-en (Central supplier network (CSN)) keresztül kapcsolódnak a CBB-hez

A szolgáltatók működhetnek saját cégük területén és valamely konszerntársaság területén is.

4.2 Előírások

4.2.1. Belső szervezés

A hardverek és szoftverek rendelkezésre bocsátását vagy installálását a szolgáltatók csak az esetükben illetékes szakterületen (a megbízó szakterülete) keresztül hajthatják végre vagy kezdeményezhetik.

A rendelkezésre bocsátott hardverek és szoftverek használatára az AUDI HUNGARIA szabályozásai érvényesek (lásd 7.2.13 függelék).

Az IT-eszközök felnyitása vagy hardvereken végrehajtott módosítások (pl. merevlemezek, memóriamodulok ki-/beszerelése) és a biztonsági beállítások manuális módosítása (pl. a webböngészőben) csak az illetékes szervek számára engedélyezett (lásd 7.2.14 függelék).

A megbízó programjainak használata vagy utólagos módosítása csak akkor lehetséges, ha az illetékes szerv (lásd 7.2.14 függelék) azt engedélyezte.

A rendelkezésre bocsátott IT-eszközökön tilos kezelni olyan ügyfelek adatait, akik nem a konszernhez tartoznak.

A megbízó IT-eszközeinek vagy adatainak a szolgáltató munkatársai által történő használatához a megbízó kifejezett hozzájárulása szükséges. A megbízó bármikor jogosult a hozzáférést vagy a használatot megtiltani (pl. visszaélés esetén).

4.2.2. Fizikai és környezettel kapcsolatos biztonság

A rendelkezésre bocsátott eszközöket rendeltetésszerűen kell használni, és óvni kell az elvesztéssel vagy illetéktelen módosítással szemben.

Be kell tartani a gyártó előírásait, amelyek az eszközök védelmét szolgálják.

A megbízó által rendelkezésre bocsátott eszközöket (pl. laptopok, mobiltelefonok) csak az arra vonatkozó engedély birtokában szabad kivinni a megbízó üzemi területéről.

4.2.3. Rosszindulatú szoftverek és mobil programkódok elleni védelem

Kártékony szoftverrel való fertőződés gyanúja esetén az érintett IT eszközök és adathordozók nem használhatók tovább. Haladéktalanul tájékozatni kell az illetékes szerveket (lásd 7.2.9 függelék).

4.2.4. Biztonsági mentés

Az adatok nem tárolhatók a helyi meghajtókon, csak a megadott hálózati meghajtókon, mert a biztonsági másolatok központi és automatikus előállítása csak a hálózaton biztosított.

A felhasználó felelős azon adatok biztonsági másolatainak elkészítéséért, amelyek nem a központi hálózati meghajtókon (pl. helyi merevlemez, mobil adathordozó) vagy hasonló funkciójú rendszereken (pl. eRoom, SharePoint) találhatók.

A biztonsági mentéseket és médiumokat ugyanúgy kell kezelni, mint az eredeti adatokat.

4.2.5. A hozzáférés ellenőrzése

4.2.5.1. A hozzáférések ellenőrzésének üzleti követelményei

Az alábbi előírásokat minden felhasználó köteles betartani:

Általános előírások

- Más személy felhasználói azonosítójának vagy fiókjának használata tilos.
- Azonosító eszközök (pl. SmartCardok vagy SecurID-kártyák) továbbadása tilos.
- Személyes használatra szánt felhasználói azonosítóhoz tartozó jelszavakat vagy PIN-kódokat („személyes felhasználói azonosítók”) titokban kell tartani, továbbadásuk tilos.
- Jelszavak tárolása vagy felírása (pl. papíron, mobilkészüléken vagy fájlban történő rögzítése) tilos, amennyiben nem ezt határozták meg biztonságos módszerként (lásd 7.2.15 függelék).
- Amennyiben feltételezhető, hogy a jelszó vagy a PIN-kód biztonsága sérült, vagy valaki hozzáfért a jelszóhoz vagy a PIN-kódhoz, ezeket az adatokat azonnal módosítani kell.
- Az ideiglenes jelszavakat (pl. új fiók esetén) az első bejelentkezéskor meg kell változtatni.
- Minden jelszót vagy PIN-kódot meg kell változtatni az első használat során, és legkésőbb egy év elteltével (ez utóbbi előírás csak a jelszavakra vonatkozik).
- Jelszavak kikémlelése tilos.
- A jelszavakat legalább bizalmasként kell besorolni.
- Ha a jelszavakat írásos formában kell tárolni, azt a munkatárs köteles megfelelő, jogosulatlan hozzáféréssel szemben védett helyen (pl. páncélszekrényben), lezárt borítékban tárolni. Az így őrzött jelszót minden módosítást követően aktualizálni kell. A lezárt borítékot az érintett munkatárs köteles aláírni. Miután kivételes esetekben (pl. betegség esetén) szükség lehet a jelszó használatára, név szerint meg kell jelölni azokat a személyeket, akik jogosultak a borítékot felbontani. Ennek során be kell tartani a „két személyes”-szabályt. Minden felbontást dokumentálni kell a munkatárs tájékoztatása mellett. A munkatárs köteles minden felbontás után azonnal módosítani és biztonságba helyezni a jelszót. Alternatív megoldásként alkalmazhatók hasonló funkciót ellátó IT-rendszerek (pl. elektronikus jelszótároló) is.
- A képernyős munkavégzés megszakítása esetén (pl. szünet vagy megbeszélés céljából) a rendszert zárolni kell (pl. jelszóval védett képernyővédővel).
- Azon felhasználók, akik multifunkciós igazolványukat az IT-rendszerekbe való bejelentkezésre használják, a rendszer elhagyásakor kötelesek eltávolítani az igazolványukat az olvasóból.

4.2.5.2. Jelszavak generálása

A jelszavak generálása során be kell tartani a következő előírásokat:

- A (szolgáltatóhoz tartozó) munkatársak a megbízó rendszereihez való hozzáféréskor nem használhatják ugyanazt a jelszót munkahelyi és privát célokra.

- A (szolgáltatóhoz tartozó) munkatársak nem használhatják ugyanazt a jelszót a Volkswagen-konszern által rendelkezésre bocsátott rendszerekhez és a harmadik felek által rendelkezésre bocsátott rendszerekhez (pl. alkalmazások, internetes regisztrációk).
- A rendszerek által megkövetelt minimális jelszóhosszúságot be kell tartani. Ezek az adott szabályozásban előírtakhoz igazodnak (lásd 7.1.2 függelék).
- Triviális jelszavak (pl.: „Test123456“) vagy személyes vonatkozást tartalmazó jelszavak (pl.: nevek, születési dátum) nem használhatók.
- Ha a rendszer vagy az alkalmazás komplex jelszóválasztást vár el (lásd 7.1.2 függelék), követni kell az előírásokat.
  Megjegyzés: a biztonságos jelszóválasztáshoz használhat emlékeztető hívószavakat vagy rövidítéseket, illetve ferdítéseket (például: „Minden reggel bemegyek a fürdőbe és alaposan megmosakszom”, a jelszó: „Mrbaf&am”). Emellett négy szó kombinációja (pl. „NapFaTeaVaj”) is biztonságos, de könnyen megjegyezhető jelszó lehet. Az itt megadott példákat nem szabad tényleges jelszóként használni.

4.2.5.3. Okostelefonok és tabletek zárolására használt PIN-kódok

Be kell tartani a 4.2.5.2 fejezetben foglalt előírásokat.

4.2.5.4. PIN-kódok hitelesítő SmartCardokhoz

Be kell tartani a 4.2.5.2 fejezetben foglalt előírásokat.

4.2.5.5. Csoportos azonosítók

Bizonyos csoportos azonosítók több személy által történő többszöri használata (pl. képzési osztály, gyakornokok, felsőoktatásban tanulók) az alábbi feltételek betartása mellett megengedett:

- A felhasználói azonosítót az illetékes személy adja ki, aki írásos jegyzőkönyvet készít arról, ki mely időpontban milyen felhasználói azonosítót használ, és archiválja a vonatkozó jegyzőkönyvet.
- A felhasználói azonosító átvételét az érintett felhasználó írásban köteles igazolni. Az igazolást a felhasználói azonosítóért felelős személy megőrzi.
- A felhasználói azonosító átvételét követően az érintett felhasználó köteles azt olyan jelszóval módosítani, amelyet csak ő ismer.
- A felhasználói azonosító visszaadását követően az illetékes személy köteles azt olyan jelszóval módosítani, amelyet csak ő ismer.
- A jegyzőkönyvek archiválására a vállalatnál meghatározott archiválási határidők érvényesek.

Az egyidejűleg több személy által használható felhasználói azonosítók (úgynevezett „csoportos azonosítók”) alkalmazása csak akkor megengedett, ha azok kizárólag olyan alkalmazások futtatását teszik lehetővé, amelyek saját felhasználókezeléssel rendelkeznek, beleértve a személyes hitelesítést is, és csak olvasásra biztosítanak hozzáférést.

4.2.6. A hálózatokhoz való hozzáférés ellenőrzése

4.2.6.1. Hálózati szolgáltatók igénybe vételére vonatkozó szabályozás

A megbízó által rendelkezésre bocsátott IT-eszközt csak akkor és annyi ideig szabad külső hálózatokkal (pl. hotspot, privát WIFI, kivéve mobilhálózatok) összekapcsolni, ha és ameddig az a konszern hálózatával való kapcsolat létrehozása érdekében történik (távoli hozzáféréssel/VPN-en keresztül). Közvetlen „szörfölés” stb. nem engedélyezett (kivéve a mobilhálózatokhoz kapcsolódó okostelefonokkal és tabletekkel).

A már nem szükséges kapcsolatot meg kell szakítani.

4.2.6.2. Eszközazonosítás a hálózaton belül

A kommunikációs eszközök és a belső hálózat (intranet) közötti korlátlan kapcsolat (pl. tűzfal nélkül) csak akkor megengedett, ha azokat a konszern vagy olyan társaság bocsátja rendelkezésre, amelyben a konszern vagy egyik társasága többségi részesedéssel bír.

5 A konszern belső hálózatához közvetlen hozzáféréssel nem rendelkező szolgáltatókra vonatkozó további követelmények

5.1 Meghatározás

Az alábbi kategóriák valamelyikéhez tartozó szolgáltatók kötelesek betartani az 5. fejezet szerinti előírásokat:

- szolgáltatók, amelyek nem rendelkeznek közvetlen hozzáféréssel valamely konszerntársaság hálózatához
- szolgáltatók, amelyek részére nem bocsátanak rendelkezésre olyan felhasználói készülékeket, melyek a Volkswagen-konszern tulajdonában vannak, és csak a szolgáltató cége tulajdonában lévő felhasználói készülékeket használják
- szolgáltatók, amelyekkel nem áll fenn kapcsolat Secure Partner, remote access vagy más VPN-megoldáson keresztül

- A csak képernyőtartalmak és hozzájuk tartozó vezérlőadatok továbbítását lehetővé tevő virtuális desktop megoldásokra a jelen fejezet szerinti előírások érvényesek.
- Ezek a szolgáltatók adatokat cserélnek az AUDI HUNGARIA-val.

Ezek a szolgáltatók saját vállalatuk telephelyén működnek és a vállalatuk szabályozásait kötelesek betartani.

5.2 Előírások

5.2.1. Belső szervezés

A konszerntársaságok adatait külön kell választani harmadik felek adataitól, különösen a szolgáltatók más ügyfeleinek adataitól (pl. a jogok kezelése által). Az adatok nem lehetnek harmadik fél számára hozzáférhetők (pl. titkosítással kell védeni őket).

Az összes szükséges biztonsági intézkedés megvalósítása érdekében az AUDI HUNGARIA besorolását alkalmazni kell a szolgáltató besorolási sémájában is.

A szolgáltatók kötelesek a feladataik elvégzéséhez megfelelő biztonsági intézkedéseket kialakítani saját vállalatuknál, a részükre átadott szabályozásban szereplő információbiztonsági előírások alapján.

A szolgáltató munkatársainak a megbízó adataihoz való hozzáférést csak a „szükséges ismeret” („need-to-know”) elve alapján szabad biztosítani.

6 Felelősségek

A jelen szabályozást a jelen dokumentumban található meghatározás szerint minden szolgáltató köteles betartani.
A jelen cselekvési irányelvektől való eltérések, amelyek a biztonsági szint csökkenését okozzák, csak időszakosan és az illetékes szervekkel (lásd 7.2.16 függelék) és a megbízóval egyeztetve megengedettek.

7 Függelék

7.1 Együtt érvényes dokumentumok

7.1.1. Vállalati irányelv U_1.018: 6. sz. melléklet– Információbiztonsági cselekvési irányelv rendszerüzemeltetők és adminisztrátorok számára

7.1.2. Vállalati irányelv U_1.018: 11. sz. melléklet– Hitelesítés és IAM

7.2 Vállalatspecifikus definíciók

7.2.1. Személyes adatok (pl. név, telefonszám, e-mail cím, születési dátum) gyűjtése, kezelése vagy használata csak a törvényi és vállalati személyes adatvédelmi előírásoknak megfelelően történhet.

Az AUDI HUNGARIA-nál tárolt személyes adatok csak munkavégzés céljából használhatóak, amikor a személyes adatok szakmai cél elérését szolgálják. A személyes adatok továbbadása jogosulatlan harmadik félnek (pl. ügyfelek, partnercégek alkalmazottai, vállalati munkatársak) tilos.

A személyes adatok osztályozásához szükséges információk megtalálhatóak az Audi Myneten a következő elérhetőségen: Társaságok / Audi Hungaria / Szervezet / Központi funkciók / IT-biztonság / IT-biztonsági folyamatok / Üzletkritikusság besorolás (BKE) / Dokumentumok / Adatosztályozás Template

Azok az IT-eszközök és adathordozók, melyeken személyes, bizalmas vagy titkos adatok kerültek tárolásra, kizárólag titkosított állapotban hagyhatják el az AUDI HUNGÁRIA területét.

7.2.2. http://www.vwgroupsupply.com

7.2.3. AUDI HUNGARIA ServiceDesk, Tel. 1400.

7.2.4. Felelősség: AUDI HUNGARIA Külső kommunikáció/PR (G/GP-1) szervezeti egysége

7.2.5. A személyes, bizalmas és titkos, papír alapú dokumentumokat biztonságos módon (pl. adatvédelmi konténerekben) kell eltávolítani. A már nem használt adathordozókat megbízható módon, felülírással kell törölni vagy fizikailag megsemmisíteni.

7.2.6. A megbízó titoktartás hatálya alá eső valamennyi adatára vonatkozóan a „Vállalati irányelv U_1.018 – 6. sz. melléklet - – Információbiztonsági cselekvési irányelv rendszerüzemeltetők és adminisztrátorok részére 8.1” pontjában található hitelesítési eljárások engedélyezettek besorolásuk függvényében.

7.2.7. Azok az IT eszközök és adathordozók, amelyeken az AUDI HUNGARIA személyes, bizalmas vagy titkos adatait tárolják, alapszabály szerint csak titkosítva hagyhatják el az AUDI HUNGARIA üzemi területét.

7.2.8. AUDI HUNGARIA Service Desk, Tel. 1400

7.2.9. IT-Biztonság / Governance terület

7.2.10. IT-Biztonság / Governance terület

7.2.11. IT-Biztonság / Governance terület, Know-how Védelem terület, az Audi Hungaria adatvédelmi tisztviselője.

7.2.12. AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet - "GDPR”. Továbbá a „2011. évi CXII. törvény - az információs önrendelkezési jogról és az információszabadságról“ illetve egyéb, vonatkozó jogszabályok.

7.2.13. Minden szolgáltató felelős azért, hogy az információkat, programokat és IT-eszközöket csak vállalati célokra és az adott feladatra vonatkozó megbízás keretében, szabályszerűen használják és alkalmazzák.

7.2.14. Felelősség: IT Infrastructure / Workplace Services terület.

7.2.15. Jelszó széfek, pl. KeePass használata ajánlott.

7.2.16. It-Sicherheit@audi.hu