Kivonat külsős felek részére az információbiztonsági szabályzatból

1. Bevezető rendelkezések

1.1. A jelen kivonat célja azon információbiztonsági követelmények rögzítése, amelyek a HungaroControl Zrt-vel (a továbbiakban: Társaság) szerződéses jogviszonyban lévő külsős felekre vonatkozik.

A kivonat a Társaság információbiztonságról szóló technológiai igazgatói szervezeti utasítás alapján készül.

1.2. A kivonat **személyi hatálya** kiterjed a Társaság IT rendszereivel kapcsolatba kerülő, vagy a Társaság tulajdonában vagy kezelésében álló adatokhoz, információkhoz hozzáférő, de nem a Társaság alkalmazásában álló természetes vagy jogi személyekre (továbbiakban: külsős személyek).

1.3. A kivonat **tárgyi hatálya** kiterjed

a. a Társaságnál alkalmazott valamennyi IT rendszerelemre (beleértve az ATM és ATM-R rendszerkörnyezetekben lévő infokommunikációs technológiai elemeket is) és az azok által nyújtott IT szolgáltatásokra, amelyek tárolják, kezelik, feldolgozzák, felügyelik, ellenőrzik, továbbítják a Társaság tulajdonában és kezelésében álló adatokat, információkat;

b. az IT rendszerelemek üzemszerű működésének biztosítására szolgáló valamennyi ingatlanra, helyiségre és épületgépészeti berendezésre függetlenül a használat jogcímétől.

1.4. Vonatkozó jogszabályok és egyéb hivatkozások, követelmények:

a. jelen kivonat az iparági szabványok és ajánlások figyelembevételével Társaság hatályos vonatkozó belső szabályozásaiban foglaltakra, az ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls-ban foglaltakra, továbbá a jelen utasítás 1.4. b pontjában felsorolt jogszabályok vonatkozó előírásainak figyelembevételével került kialakításra;

b. vonatkozó jogszabályi követelmények:

i. 1999. évi LXXVI. törvény a szerzői jogról.

ii. Az előzetes tájékoztatás, a koordinálás és a légi járatok légiforgalmi irányító egységek közötti átadása céljából a repülési adatok cseréjét biztosító automatikus rendszerekre vonatkozó követelmények megállapításáról szóló 1032/2006/EK bizottsági rendelet.

iii. Az előzetes tájékoztatás, a koordinálás és a légijáratok légiforgalmi irányító egységek közötti átadása céljára szolgáló légiforgalmi üzenettovábbítási protokoll használatára vonatkozó követelmények megállapításáról szóló 633/2007/EK bizottsági rendelet.

iv. A polgári légi közlekedés védelmének közös szabályairól és a 2320/2002/EK rendelet hatályon kívül helyezéséről szóló 300/2008/EK európai parlamenti és tanácsi rendelet.

v. Az egységes európai égbolt keretében megvalósuló adatkapcsolat-szolgáltatásokra vonatkozó követelmények megállapításáról szóló 29/2009/EK bizottsági rendelet.

vi. 2009. évi CLV. törvény a minősített adat védelméről.

vii. 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

viii. 2012. évi I. törvény a munka törvénykönyvéről.

ix. 2012. évi C. törvény a Büntető Törvénykönyvről.

x. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

xi. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

xii. 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.

xiii. A belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló 910/2014/EU európai parlamenti és tanácsi rendelet.

xiv. A légiforgalmi adatok és légiforgalmi tájékoztatások minőségével kapcsolatos követelményeknek az egységes európai égbolt keretében történő meghatározásáról szóló 73/2010/EU rendelet módosításáról szóló 1029/2014/EU bizottsági végrehajtási rendelet.

xv. 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól.

xvi. 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.

xvii. A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148/EU európai parlamenti és tanácsi irányelv.

xviii. 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 szóló 2016/679/EU európai parlamenti és tanácsi rendelet (általános adatvédelmi rendelet, GDPR).

xix. A hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148/EU európai parlamenti és tanácsi irányelv.

xx. 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól.

xxi. A légiforgalmi szolgáltatást/léginavigációs szolgálatokat és más légiforgalmi szolgáltatási hálózati funkciókat és azok felügyeletét ellátó szolgáltatókra vonatkozó közös követelmények meghatározásáról, valamint a 482/2008/EK rendelet, az 1034/2011/EU, az 1035/2011/EU és az (EU) 2016/1377 végrehajtási rendelet hatályon kívül helyezéséről, továbbá a 677/2011/EU rendelet módosításáról szóló 2017/373/EU bizottsági végrehajtási rendelet.

xxii. A nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló 2017/1584/EU bizottsági ajánlása.

xxiii. 161/2019. (VII. 4.) Korm. rendelet a közlekedési létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

xxiv. Az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről szóló 2019/881/EU európai parlamenti és tanácsi rendelet (kiberbiztonsági jogszabály).

2. Értelmező rendelkezések

2.1. **Információbiztonság:** az adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása, megőrzése.

2.2. **Bizalmasság:** annak biztosítása, hogy az adatok és információk csak az arra jogosultak számára legyen megismerhető.

2.3. **Sértetlenség (avagy integritás):** az adatok és információk, valamint a feldolgozási módszerek teljességének és pontosságának biztosítása.

2.4. **Rendelkezésre-állás:** annak biztosítása, hogy az adatok, információk és az azokat biztosító IT rendszerek a jogosultak számára igény szerint hozzáférhetőek és használhatóak legyenek.

2.5. **Kiberbiztonság és -védelem:** az adatok, információk jogosulatlan használatával és egyéb elektronikus bűncselekményekkel szembeni védelme; illetve ennek eléréséhez szükséges intézkedések.

2.6. **Infokommunikációs technológia (továbbiakban: IT):** adatok és információk tárolására, kezelésére, feldolgozására, továbbítására használt, elsősorban számítógépes és távközlési rendszerek és módszerek összefoglaló elnevezése; jelen utasítás tekintetében a Társaság vállalati, ATM és ATM-R informatikai, tele- és mobilkommunikációs rendszereit jelenti.

2.7. **Külsős személy:** a Társaság IT rendszereivel kapcsolatba kerülő, vagy a Társaság tulajdonában vagy kezelésében álló adatokhoz, információkhoz hozzáférő, de nem a Társaság alkalmazásában álló természetes vagy jogi személy.

2.8. **Felhasználó:** a Társaság munkavállalói és a Társaság IT rendszereivel kapcsolatba kerülő, vagy a Társaság tulajdonában vagy kezelésében álló adatokhoz, információkhoz hozzáférő, de nem a Társaság alkalmazásában álló természetes vagy jogi személyek együttesen.

2.9. **Információbiztonsági incidens:** olyan nem kívánatos vagy nem várt egyedi vagy sorozatos események, amelyek veszélyeztetik a Társaság működését.

2.10. **Adat:** tények, fogalmak, eligazítások megjelenése, amely alkalmas az emberi vagy az automatikus eszközök által történő értelmezésre, vagy feldolgozásra.

2.11. **Információ:** az adatnak tulajdonított jelentés; olyan tény, amely a befogadó részére új ismeretet tartalmaz, és ezáltal csökkenti bizonytalanságát.

2.12. **IT Ügyfélszolgálat:** a Társaság Infokommunikációs Szolgáltatások Osztálya (a továbbiakban: ICTS) által biztosított funkció, melynek feladata a felhasználói igények és bejelentések - beleértve az információbiztonsági hiányosságok és incidensek - egységes rendszerben történő kezelése.

2.13. **Felhasználó azonosító (avagy account):** felhasználó azonosítására és alkalmazásokba, illetve IT rendszerekbe történő bejelentkezéshez és belépéséhez használt egyedi, a felhasználó személyével egyértelműen kapcsolatba hozható karaktersorozat.

2.14. **Cserélhető adathordozó:** minden olyan hordozható adattároló eszköz, amely csatlakoztatására a felhasználó az Infokommunikációs Szolgáltatások Osztály (a továbbiakban: ICTS) támogatása nélkül képes (például: floppy lemez, CD/DVD, blu-ray lemez, pendrive, cserélhető külső adattároló egység, memóriakártya, egyéb mobilkommunikációs készülék stb.).

3. Információbiztonsági kockázatok kezelése

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

4. Összeférhetetlenség

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

5. Az információbiztonsággal kapcsolatos feladat- és hatáskörök

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

6. Az emberi erőforrással kapcsolatos információbiztonsági intézkedések

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

7. A Társaság információs vagyonának kezelése

7.1 Az Ibtv. szerinti biztonsági szintbe és osztályba sorolás

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

7.2 Az információs vagyon nyilvántartása, a vagyonelemek felelőse, információbiztonsági osztályba sorolása és védelme

A külsős személyek feladata és felelőssége a szerződés keretében átadott adatok és információk információbiztonsági osztályaira vonatkozó védelmi intézkedések alkalmazása.

A jogszabályok által minősített adatok kezelésével kapcsolatos előírásokat a Társaság biztonsági szabályzat a minősített adatok védelmére című belső szabályozása tartalmazza.

8. Az információs vagyon elfogadható használatára vonatkozó szabályok

A külsős személyek felelőssége, hogy a szerződésteljesítéshez esetlegesen átvett IT és mobil-kommunikációs eszközök (jellemzően token és cserélhető adathordozó; továbbiakban: eszközök) a ne maradjanak őrizetlenül, a használaton kívüli eszközök elzárásra kerüljenek, és nyilvános helyen történő használat során a vegyék figyelembe a nyilvános helyen történő használat kockázatait (például az azonosító és hitelesítő adatok megszerzésének megnövekedett kockázatait).

A szerződésteljesítés céljából átvett eszközök használatát tilos nem jogosult személy részére átengedni.

A külsős személy köteles a használatra átadott eszközök, valamint a Társaság által nyújtott szolgáltatások használata során jogkövető magatartást tanúsítani.

A Társaság által nyújtott szolgáltatások, beleértve az elektronikus levelezést és az internet szolgáltatást is, - információbiztonsági célból - naplózásra, a rosszindulatú programok, kódok és tevékenységek kiszűrése érdekében - automatizmusok által, emberi beavatkozás nélkül - (vírus)ellenőrzésre, (tartalom)szűrésre és szükség esetén (például lehetséges ún. zero-day támadások esetén) blokkolásra kerül.

A külsős személyeknek, a Társaság hálózatán tilos nemkívánatos tartalmú, potenciálisan veszélyt hordozó tartalmú weboldalak és nyilvánosan hozzáférhető szolgáltatások használata úgy, mint:

a. illegális tevékenységekkel, letöltésekkel és drogokkal kapcsolatos weboldalak;
b. erőszakkal és bántalmazással kapcsolatos tartalmak;
c. kiber- és internetes bűnözéssel kapcsolatos oldalak;
d. pornográfia;
e. fegyverek és fegyverkészítés;
f. peer-to-peer alapú fájlcserélők;
g. szerencsejáték és fogadás;
h. rasszizmus, gyűlöletbeszéd és

i. bármely olyan tartalom, weboldal és szolgáltatás, amely potenciális kockázatot jelent a Társaságra nézve.

A Társaság információbiztonsági okokból korlátozza, tiltja is a fenti tartalmakhoz való hozzáférést.

Tilos a szerződésteljesítéshez kapcsolódó állományokat nyilvánosan hozzáférhető, felhő alapú szolgáltatások használatával megosztani. Erre a célra kizárólag a Társaság által biztosított szolgáltatások (például SharePoint, WebShare stb.) használhatók, az érintett adatok és információk információbiztonsági osztályára vonatkozó védelmi intézkedések alkalmazása mellett.

A külsős személyek kötelesek betartani a jelszóválasztásra és -gondozására vonatkozó előírásokat.

9. Hozzáférés- és jogosultságmenedzsment

9.1 A működési követelményeknek megfelelő hozzáférésszabályozás

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

9.2 Felhasználói hozzáférések kezelése

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

9.3 Felhasználók információbiztonsági felelőssége

A külsős személyek kötelesek az információs vagyon elfogadható használatára vonatkozó követelmények, valamint a jelen utasítás előírásainak betartásával hozzájárulni a Társaság tulajdonában és kezelésében lévő adatok és információk, valamint IT rendszerek és alkalmazások információbiztonságának fenntartásához, illetve a jogosulatlan hozzáférési kísérletek megelőzéséhez.

A külsős személy felelősséggel tartozik a saját felhasználói azonosítójával (account) a Társaság IT rendszereiben és alkalmazásaiban végrehajtott minden tevékenységért és műveletért. Ezért a külsős személyek felelőssége, hogy

a. a felhasználói azonosítójukhoz tartozó és annak használatát védő jelszavak gondosan kerüljenek megválasztásra, azaz
   i. a jelszó könnyen megjegyezhető legyen, de nehéz legyen kitalálni,
   ii. a jelszó legalább 8 karakter hosszú legyen,
   iii. a jelszó tartalmazzon kis- és nagybetűkön kívül számot vagy speciális karaktert,
   iv. tilos jelszóként a felhasználói nevet, vagy a felhasználóval egyértelműen kapcsolatba hozható személyes információt (például születési dátum, saját, családtag, vagy háziállat neve stb.) használni,
   v. tilos jelszóként olyan szót, vagy kifejezést megadni, amely szótáralapú támadással szemben sérülékeny (azaz szótári formában egy az egyben fordul elő),
   vi. tilos jelszóként ismétlődő vagy periodikus karaktersorozatot választani,
   vii. a Társaság rendszerkörnyezetében használt jelszavak ne egyezzenek meg az azon kívüli környezetben használt egyéb jelszavakkal, különös tekintettel a nyilvánosan hozzáférhető internetes szolgáltatásokra;
b. biztosított legyen a megfelelő jelszógondozás, azaz
   i. a jelszót tilos bárki számára átadni, felfedni, hozzáférhetővé tenni,
   ii. a jelszót egyaránt tilos felírni és titkosítás nélkül elektronikusan tárolni, továbbítani,
   iii. az adott rendszer üzemeltetője által beállított kezdőjelszót az első bejelentkezés alkalmával mindig meg kell változtatni,

iv. minden jelszó legkevesebb 1 napig és legfeljebb 70 napig lehet érvényben és a jelszavakat az érvényességi idő lejárta előtt meg kell változtatni.

A külsős személy köteles minden olyan esemény észlelését követően haladéktalanul bejelentést tenni a kapcsolattartója vagy a Társaság IT Ügyfélszolgálata részére, amely esemény következtében fennáll a lehetősége felhasználói azonosítójával (account) történő visszaélésnek (például elhagyott, elveszett eszköz, a felhasználói azonosítóval kapcsolatos bármilyen gyanús jelenség, nem megszokott működés és/vagy funkcionalitás stb.).

9.4 Hálózati, rendszer- és alkalmazáshozzáférés ellenőrzése

A külsős személyek kizárólag olyan hálózati kapcsolatokhoz és szolgáltatásokhoz férhetnek hozzá, amelyek használata engedélyezésre került.

10. Kriptográfiai intézkedések

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

11. Fizikai és környezeti biztonsági követelmények

11.1 Fizikai biztonsági követelmények

A külsős személyek kötelesek betartani Társaság fizikai biztonsági követelményeit, a Társaság mindenkor hatályos Házirendjének megfelelően.

11.2 Informatikai eszközök és kiszolgáló berendezések környezeti biztonsága

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

11.3 Mobileszközök és cserélhető adathordozók biztonsága

A külsős személyek felelőssége a szerződésteljesítés céljából átvett eszközök használata során a vonatkozó követelmények betartása.

A külsős személy felelőssége, hogy a cserélhető adathordozók használata során, a cserélhető adathordozón tárolt adatok védelme érdekében, a rajtuk tárolt adatok információbiztonsági osztálya által meghatározott védelmi követelmények alkalmazásra kerüljenek. Amennyiben egy cserélhető adathordozó többféle információbiztonsági osztályba tartozó adatot tartalmaz, akkor mindig a legmagasabb információbiztonsági osztályba sorolt adatra vonatkozó védelmi követelmények szerint kell kezelni az adathordozót.

Cserélhető adathordozók a Társaság IT környezetében kizárólag munkavégzés és/vagy szerződésteljesítés céljából, a Társaságnál rendszeresített vírusvédelmi megoldással végzett vírusellenőrzést követően használhatók. Tilos nem megbízható forrásból származó (például talált), valószínűsíthetően nem vírusmentes cserélhető adathordozó csatlakoztatása, használata.

Cserélhető adathordozók Társaság létesítményein kívüli használata során a külsős személy feladata és felelőssége a cserélhető adathordozókon tárolt adatok védelme érdekében, az adatok információbiztonsági osztályának megfelelő kriptográfiai/védelmi intézkedések alkalmazása.

A cserélhető adathordozókon tárolt adatokat a Társaság központilag nem kezeli, ezért az esetleges elvesztésükből, megsérülésükből adódó károkért és a helyreállítás költségéért a külsős személy felelős.

12. Az üzemeltetés információbiztonsági aspektusai

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

13. Az elektronikus kommunikáció biztonsága

13.1 Hálózatbiztonsági követelmények

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

13.2 Adat- és információcserére vonatkozó biztonsági követelmények

A külsős személy köteles betartani a szerződésben az adat- és információcserére vonatkozóan meghatározott előírásokat és követelményeket.

14. IT rendszerek beszerzésének, fejlesztésének és az IT projektek információbiztonsági aspektusai

Személyes adatok tesztelés céljára csak és kizárólag anonimizált formában használhatók.

15. Külső, szerződéses felekkel történő kapcsolattartás információbiztonsági aspektusai

A külsős személy köteles betartani a szerződésben meghatározott információbiztonsági előírásokat és követelményeket.

16. Információbiztonsági incidensek kezelése

Minden külsős személynek haladéktalanul jelentene kell a kapcsolattartója vagy a Társaság IT Ügyfélszolgálata számára a tapasztalt információbiztonsági hiányosságokat és a potenciális incidenseket.

Az információbiztonsági hiányosságra és (potenciális) incidensre utalhatnak, többek között, az alábbi események, amelyek bejelentése szükséges:

a. nem hatékony, vagy nem megfelelő (információbiztonsági) szabályozás;
b. információs vagyon (adatok, információk, alkalmazások, IT szolgáltatások stb.) bizalmasságának, sértetlenségének, rendelkezésre-állásának esetleges sérülése, különös tekintettel a személyes adatokra vonatkozóan;
c. elkövetett véletlen hiba;
d. belső előírás vagy jogszabály megsértése;
e. ellenőrzés/jóváhagyás nélküli változtatás;
f. hardveres vagy szoftveres meghibásodás, üzemzavar vagy nem megfelelő működés;
g. hozzáférési jogosultságok, előírások megsértése.

17. A rendkívüli helyzetek kezelésének információbiztonsági aspektusai

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

18. Személyes adatok védelme

18.1 Általános adatvédelmi követelmények

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

18.2 A TCHI által kezelt személyes adatok

A TCHI a felhasználók személyes adatait kizárólag az üzemeltetői tevékenységéből és a Társaság IT környezetének biztonságos kialakításából, illetve védelme érdekében adódó munkafolyamatok kapcsán kezeli.

A TCHI által kezelt, a személyes adatok kezeléséről szóló részletes tájékoztatót az 1. számú melléklet tartalmazza.

18.3 Magáncélú használathoz kapcsolódó személyes adatok

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

19. Információbiztonsági felülvizsgálatok

Ez a fejezet nem tartalmaz külsős személyekre vonatkozó követelményeket.

Mellékletek

1. számú melléklet: Tájékoztató a TCHI által kezelt személyes adatok kezelésről

1. számú melléklet – Tájékoztató a TCHI által kezelt személyes adatok kezelésről

1. A Társaság IT Ügyfélszolgálatának igénybevételével kapcsolatos adatkezelési tájékoztató a Társaság internetes honlapján, a https://www.hungarocontrol.hu/download/a177be2948e29fed794c0d5a19feb94e.adatkezelesi-tajekoztato-telefonbeszelgetes-rogzitese.pdf linken érhető el (2. fejezet „*IT ügyfélszolgálat igénybevételével kapcsolatos adatkezelés*").

2. A Társaság IT rendszereinek védelmének biztosítása és magas szintű rendelkezésre állása érdekében szükséges a rendszerhasználata során keletkező felhasználói és technikai adatokban előforduló személyes adatok kezelése - az adattakarékosság elvének megfelelően -, az alábbiak szerint:

2.1. Kezelt adatok köre:

   a. a felhasználók személyével közvetetten kapcsolatba hozható technikai adatok (kliens-eszközök egyedi hálózati azonosítójuk, azaz IP címük, a klienseszközök hálózati kártyáik egyedi azonosítója, azaz MAC címük),

   b. a hálózati szolgáltatások használata során keletkező, naplózott technikai adatok (hálózat forgalomi és internethasználati adatok),

   c. a felhasználói hozzáférés- és jogosultságmenedzsment adatok (a felhasználó neve, felhasználói azonosítója, (jog)csoport tagságai),

   d. az üzemeltetési tevékenységek során készített biztonsági mentések;

2.2. az adatkezelés jogalapja: számítástechnikai vészhelyzetekre történő reagálás, hálózatbiztonsági incidenskezelés, elektronikus hírközlési hálózatok üzemeltetése és szolgáltatások nyújtása, valamint a Társaság kibervédelmének és információbiztonságának biztosítása érdekében végrehajtott olyan mértékű személyes adatkezelés, amely a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos, vagyis adott titkossági szinten az érintett hálózat vagy információs rendszer ellenálló képessége az e hálózatokon és rendszereken tárolt vagy továbbított adatok, valamint az e hálózatok és rendszerek által nyújtott vagy rajtuk keresztül elérhető kapcsolódó szolgáltatások hozzáférhetőségét, hitelességét, integritását és bizalmas jellegét sértő véletlen eseményekkel, illetve jogellenes vagy rosszhiszemű tevékenységekkel szemben, mint a Társaság érdekmérlegelési teszten alapuló jogos érdeke;

2.3. az adatkezelő személye: az ICTS és a THCS munkatársak;

2.4. az adatkezelés során érintettek köre:

   a. a Társaság munkavállalói,

   b. a Társaság IT rendszerelemeit és az azok által nyújtott szolgáltatásokat igénybe vevő, illetve a Társaság munkatársaival informatikai eszközök útján kapcsolatot tartó külső felek képviselői;

2.5. az adatok forrásai:

   a. a Társaság informatikai hálózatát és kiszolgáló eszközeit, azok forgalmát, teljesítményét naplózó és monitorozó eszközök,

   b. a biztonsági mentéseket tartalmazó rendszerelemek,

   c. Központi Címtár (Active Directory);

2.6. az adatkezelés céljai:

   a. üzemeltetési feladatok ellátása,

   b. a rendszerek magas rendelkezésre-állásának biztosítása,

   c. kiber-, informatikai- és információbiztonsági események azonosítása, megelőzése, kivizsgálása és elhárítása,

d. statisztikák és riportok készítése,
e. az üzemeltetési tevékenységek minőségbiztosítása, az IT szolgáltatások minőségének és hatékonyságának növelése,
f. felhasználói jogosultságok kezelése;

2.7. az adatkezelés időtartama:
a. az 1. számú melléklet 2.1. a-c pontokban meghatározott adatokat tartalmazó napi biztonsági adatmentések egy hétig kerülnek megőrzésre,
b. az 1. számú melléklet 2.1. a-c pontokban meghatározott adatokat tartalmazó heti biztonsági adatmentések egy évig kerülnek megőrzésre,
c. az 1. számú melléklet 2.1. a-c pontokban meghatározott adatok a munkavállaló munkaviszonyának megszűnésétől számított öt évig kerülnek megőrzésre;

2.8. az adatkezelés módja:
az adatkezelő, azaz az ICTS és a THCS jogosult az adatok:
a. felvételére és rögzítésére az 1. számú melléklet 2.1. c pont esetében,
b. gyűjtésére, rendszerezésére és tárolására az 1. számú melléklet 2.1. a-c pontok esetében,
c. informatikai biztonsági okokból lekérdezésére, elemzésre és összekapcsolásra az 1. számú melléklet 2.1. a-c pontok esetében,
d. a gyanús, kártékony és rosszindulatú programok, kódok és tevékenységek kiszűrése érdekében - automatizmusok által, emberi beavatkozás nélkül - (vírus)ellenőrzésre, (tartalom)szűrésre és szükség esetén (például lehetséges ún. zero-day támadások esetén) blokkolásra kerül az 1. számú melléklet 2.1. a-b pontok esetében,
e. jóváhagyott felhasználói igény alapján lekérdezésre, elemzésre az 1. számú melléklet 2.1. a-d pontok esetében,
f. különböző adatok összekapcsolására az 1. számú melléklet 2.1. a-d pontok esetében,
g. jóváhagyott felhasználói igény alapján megváltoztatására az 1. számú melléklet 2.1. a és c pontok esetében,
h. jóváhagyott felhasználói igény alapján visszaállítására az 1. számú melléklet 2.1. a és c-d pontok esetében,
i. hatósági megkeresés esetén továbbítására az 1. számú melléklet 2.1. a-d pontok esetében,
j. az adatkezelés határidejének lejáratát követően, valamint a felhasználó kérésére megsemmisítésére az 1. számú melléklet 2.1. a-d pontok esetében;

2.9. jogok, jogorvoslati lehetőségek:
a felhasználó jogosult a személyes adatainak
a. lekérdezésére (hozzáféréshez való jog) az 1. számú melléklet 2.1. a és c-d pontok esetében,
b. megtekintésének igénylésére (hozzáféréshez való jog) az 1. számú melléklet 2.1. a és c-d pontok esetében,
c. megváltoztatásának igénylésére (helyesbítéshez való jog) az 1. számú melléklet 2.1. a és c-d pontok esetében,
d. kötelező adatkezelés esetének kivételével törlésének igénylésére (törléshez való jog).

3. A felhasználó jogosult a Nemzeti Adatvédelmi és Információszabadság Hatósághoz, a Társaság Adatvédelmi Tisztviselőjéhez, valamint bírósághoz fordulni a jogok gyakorlásának, illetve a jogorvoslati lehetőségek igénybevételének szabályai
a. a Társaság Adatvédelmi Szabályzatában, illetve
b. az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 14-23.§-ban találhatók.