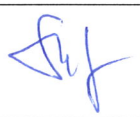
Nitrogénművek Zrt.

Informatikai Biztonsági Szabályzat (IBSz)

Hatálybalépés időpontja:	2018.05.25.
Érvényesség:	visszavonásig
Hatályon kívül helyezett szabályozások:	Informatikai Biztonsági Szabályzat 2016.04.08.
Jóváhagyó:	Szilágyi János vezérigazgató
Aláírás:	
Dátum:	Pétfürdő, 2018. május 25.

Tartalomjegyzék

1. Általános rendelkezések

1.1. A szabályzat célja

Az Informatikai Biztonsági Szabályzat (röviden: IBSz) célja a jogszabályi előírások és a szakmai ajánlások alapján a Nitrogénművek Zrt. információbiztonsági követelményjegyzékének meghatározása.

A követelményjegyzék magában foglalja a szervezetre vonatkozó információbiztonsági feladatok és felelősségi körök meghatározását, valamint a szervezet által kezelt, feldolgozott, továbbított, valamint tárolt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának kockázatokkal arányos védelmét, a törvényi előírásokkal összhangban.

1.2. A szabályzat hatálya

1.2.1. Személyi hatály

A szabályzat személyi hatálya kiterjed a Nitrogénművek Zrt-vel munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló valamennyi természetes személyre, továbbá – a velük kötött szerződés alapján – minden olyan személyre, akik munkavégzésük során a Nitrogénművek Zrt. által biztosított, a szabályzat tárgyi hatálya alá tartozó infokommunikációs eszközt vagy szolgáltatást vesz igénybe, vagy szerez be.

1.2.2. Tárgyi hatály

A szabályzat tárgyi hatálya kiterjed a Nitrogénművek Zrt. tulajdonában és/vagy használatában álló, valamint az általa üzemeltetett valamennyi informatikai (számítástechnikai) és kommunikációs eszközre, alkalmazásra, szolgáltatásra.

1.3. A szabályzattal kapcsolatos feladatok

A szabályzattal kapcsolatos feladatokat és felelősségeket az alábbi táblázat (ún. RACI) szemlélteti:

Feladat	Vezérigazgató	Információ-biztonsági Felelős	Informatikai osztályvezető	VMA üzemvezető
IBSz elkészítése, módosítása	T	V; Sz	K	K
IBSz elfogadása és kihirdetése	V; Sz	T	T	T
IBSz rendszeres felülvizsgálata	T	V; Sz	K	K
IBSz betartásának ellenőrzése	Sz	V	V	V
V=Végrehajtó; Sz=Számonkérhető; K=Konzulens; T=Tájékoztatandó				

1.3.1. IBSz elkészítése, módosítása

A szabályzat elkészítése és szükség szerinti módosítása az Információbiztonsági Felelős feladata és felelőssége, melyről tájékoztatni köteles a Vezérigazgatót. Konzultációs célból ajánlott az Informatikai osztályvezető valamint a Villamos és Műszer-Automatika üzemvezető bevonása.

1.3.2. IBSz elfogadása és kihirdetése

A szabályzat elfogadása és kihirdetése a személyi hatályban meghatározott érintett kör részére a Vezérigazgató feladata és felelőssége, melyről tájékoztatnia kell az érintetteket.

A szabályzatot az Interneten kell közzétenni PDF formátumban, hogy az jogosulatlanok számára ne legyen módosítható, de minden érintett megismerhesse.

1.3.3. IBSz rendszeres felülvizsgálata

Az Információbiztonsági Felelős feladata és felelőssége a szabályzatot felülvizsgálni minden olyan esetben –de legalább évente egyszer–, amikor azt szervezeti, műszaki, jogszabályi vagy egyéb változások indokolttá teszik.

A felülvizsgálatnak a legutolsó kiadás óta bekövetkezett jogszabályi, funkcionális, biztonsági, technológiai vagy egyéb változásokra is ki kell terjednie.

A felülvizsgálat eredményéről tájékoztatni kell a Vezérigazgatót, továbbá konzultációs célból szükség esetén be kell vonni az érintett terület irányításáért felelős vezetőt, az Informatikai osztályvezetőt és a Villamos és Műszer-Automatika üzemvezetőt.

1.3.4. IBSz betartásának ellenőrzése

A szabályzatban foglaltak szervezeti szintű betartatása és ellenőrzése az Információbiztonsági Felelős, az Informatikai osztályvezető és a Villamos és Műszer-Automatika üzemvezető feladata –eseti ellenőrzések végrehajtásán keresztül–, de a Vezérigazgató felelőssége.

2. Az információbiztonság szervezete

2.1. Információbiztonsági szerepek és felelősségek

2.1.1. Vezérigazgató

Felelőssége: mint a szervezet vezetője, felelős az Információbiztonsági Politika (IBP) és az Informatikai Biztonsági Szabályzat (IBSz) elfogadásáért és kihirdetéséért, valamint az információbiztonsági szabályok betartatásáért. A kockázatelemzés során feltárt hiányosságokat és az azok megszüntetésére vonatkozó, valamint a további védelmi intézkedéseket –cselekvési tervet– jóvá kell hagynia.

Hatásköre: jóváhagyási joga van a szabályzatok és belső utasítások, továbbá a kockázatok felmérése, a védelmi intézkedések megtétele, illetve azok végrehajtása tekintetében.

2.1.2. Információbiztonsági Felelős (IBF)

Felelőssége: a szervezet információbiztonságának fenntartása és folyamatos fejlesztése, az IBP és az IBSz eseti és rendszeres karbantartása. Feladata a jogszabályban előírt adatszolgáltatási és jelentési kötelezettség teljesítése más szervezetek és szakmai csoportok irányába, illetve a folyamatos szakmai kapcsolat fenntartása.

Hatásköre: véleményezési joga van minden olyan beszerzés esetében, amelynek közvetlen vagy közvetett hatása lehet az információbiztonságra, továbbá valamennyi releváns szabályzat tekintetében. Információbiztonsági szakmai kérdésekben döntéshozó.

2.1.3. Informatikai osztály osztályvezető

Felelőssége: irányítási jogkörének megfelelően az Informatikai osztály és az információs rendszerek szabályzatoknak és előírásoknak megfelelő működtetése.

Hatásköre: utasítási joggal rendelkezik az osztály beosztottjai felé, valamint véleményezési, tájékoztatási jogkörrel az informatikai üzemeltetést és fejlesztést érintő stratégiai és koncepcionális kérdésekben. Jogosult továbbá a számítógépes adatvédelem és adatbiztonság megszervezésére és ellenőrzésére.

2.1.4. Villamos és Műszer-Automatika üzemvezető (VMA üzemvezető)

Felelőssége: irányítási jogkörének megfelelően felelős a gyártásvezérlési és irányítási rendszerek üzemeltetése tekintetében az Informatikai Biztonsági Szabályzatnak és az egyéb szabályzatoknak történő betartásáért, betartatásáért.

Hatásköre: a gyártásvezérlési és irányítási rendszerek üzemeltetése tekintetében utasítási joggal rendelkezik, valamint javaslattal élhet az egyes rendszerek üzemeltetési környezete

tekintetében. Gondoskodik továbbá arról, hogy az adatvédelmi és adatbiztonsági megfontolások az üzemeltetés során érvényesítésre kerüljenek.

2.1.5. Területi vezetők (adatgazdák)

Felelősségük: a közvetlen munkatársaik körében az információbiztonsági követelményeket betartatása és az információbiztonsági kontrollok működtetése. Felelősségük továbbá a területükhöz tartozó adatok elvárásoknak megfelelő kezelése, valamint az ezekhez kapcsolódó hozzáférési jogosultságok szabályozása.

Hatáskörük: a területükhöz tartozó rendszerek és adatok tekintetében a hozzáférési – igénylés, módosítás, visszavonás – jogosultságok elbírálása.

2.1.6. Rendszerüzemeltetést végző munkatársak

Felelősségük: a szabályzatokban és eljárási rendekben megfogalmazott követelményeknek megfelelően fejleszteni, üzembe helyezni, üzemeltetni, kivonni az információs eszközöket, rendszereket, szolgáltatásokat.

Hatáskörük: a területi vezetőkön keresztül szakmai véleményt és javaslatot fogalmazhatnak meg a szabályozásokkal és eljárásrendekkel kapcsolatban.

2.1.7. Felhasználók

Felelősségük: valamennyi felhasználó felelős a szabályzatban meghatározott biztonsági követelmények betartásáért azon adatok és információs rendszerek tekintetében, amelyeket használnak, vagy bármilyen módon kapcsolatba kerülnek velük. Az esetleges rendellenességeket a szabályzatban meghatározottak szerint haladéktalanul jelenteniük kell.

Hatáskörük: jogosultak a munkavégzésükhöz szükséges és elégséges mértékű hozzáférést kapni az információs rendszerekhez, eszközökhöz, szolgáltatásokhoz.

2.2. Az Ibtv.-ben meghatározott feladatok

Feladat	Vezérigazgató	Információ-biztonsági Felelős	Informatikai osztályvezető	VMA üzemvezető
Biztonsági szintbe és osztályba sorolás	Sz	V	-	-
Cselekvési terv készítése	Sz	V	K	K
Kapcsolat a hatóságokkal	T	V; Sz	K	K
V=Végrehajtó; Sz=Számonkérhető; K=Konzulens; T=Tájékoztatandó				

2.2.1. Biztonsági szintbe és osztályba sorolás

A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a törvény hatálya alá tartozó elektronikus információs rendszereket – vagy a rendszer által kezelt adatokat – be

kell sorolni egy-egy biztonsági osztályba a bizalmasságuk, a sértetlenségük, valamint a rendelkezésre állásuk szempontjából. A biztonsági osztályba sorolás alkalmával az érintett rendszernek – vagy az általa kezelt adatoknak – a szervezet üzletmenetére gyakorolt hatása alapján egy 1-től 5-ig számozott fokozatot kell alkalmazni, mely a számozás emelkedésével arányosan szigorodó védelmi előírásokkal jár együtt.

A szervezet elvárt biztonsági szintbe, valamint az elektronikus információs rendszerek elvárt biztonsági osztályba sorolását az 1. számú mellékletet tartalmazza, melyet a Vezérigazgató jelen szabályzat kihirdetésével elfogad.

A biztonsági szintbe és osztályba sorolást a szervezet vagy az elektronikus információs rendszer – illetve az abban kezelt adatok – jelentős megváltozása esetén, de legalább 2 évente felül kell vizsgálni.

2.2.2. Cselekvési terv készítése

Ha a vizsgálat – vagy felülvizsgálat – alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre vagy szervezeti egységre jogszabályban meghatározott biztonsági szint, vagy ha a szervezet az adott elektronikus információs rendszerére vonatkozó biztonsági osztály meghatározásánál hiányosságot állapít meg, akkor a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére vagy hiányosságok megszüntetésére.

A cselekvési terv elkészítése és folyamatos nyomon követése az Információbiztonsági Felelős feladata, annak elfogadása és betartatása a Vezérigazgató felelőssége.

2.2.3. Kapcsolattartás a hatóságokkal

A jogszabályokban meghatározott hatóságokat az Információbiztonsági Felelős tájékoztatja az elektronikus információs rendszerek biztonsági eseményeiről és adatvédelmi incidenseiről, valamint teljesíti a Nitrogénművek Zrt. jogszabályi előírásként megfogalmazott információbiztonsággal összefüggő adatszolgáltatási kötelezettségeit is.

A Kormányzati Eseménykezelő Központtal és az információbiztonsági kérdésekben eljáró hatóságokkal szintén az Információbiztonsági Felelős tartja a kapcsolatot, mely eseményekről beszámolási kötelezettsége van a Vezérigazgató felé.

2.3. Szállítói kapcsolatok

Feladat	Területi vezető (Adat-gazda)	Információ-biztonsági Felelős	Beszerzési osztályvezető	Informatikai osztályvezető	VMA üzem-vezető
Általános szabályok érvényesítése	V, Sz	K	V	K	K
Harmadik féllel kötött megállapodások	V, Sz	K	V	K	K

2.3.1. Általános szabályok

Az informatikai rendszerekkel, illetve a szervezet által kezelt adatokkal kapcsolatba kerülő, vagy az információbiztonságra közvetlen módon hatást gyakorló külső felekkel olyan írásbeli megállapodást kell kötni, amely tartalmaz vagy utal minden olyan információbiztonsági követelményre, mely az IBSz-ben vagy egyéb dokumentumban szabályozásra került.

A külső felhasználóknak rendelkezniük kell egy, a szervezeten belüli kapcsolattartóval, aki a számukra szükséges jogosultságokat megigényli, felügyeli, szükség esetén a visszavonásukat kezdeményezi.

A külső felhasználók hozzáférését a hozzáférés indokának megszűnte után azonnal meg kell szüntetni, illetve a szerződés lejártakor automatikusan megszűnik.

A külső felhasználók információs eszközeire vonatkozó biztonsági követelmények megegyeznek a szervezeten belüli eszközök követelményeivel.

Az elektronikus információs rendszer létrehozásában, üzemeltetésében, auditálásában, karbantartásában vagy javításában közreműködők esetében gondoskodni kell arról, hogy az Ibtv.-ben foglaltak szerződéses kötelemként teljesüljenek.

Ha a szervezet az adatkezelési vagy az adatfeldolgozási tevékenységhez közreműködőt vesz igénybe, akkor azt a GDPR (Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete) rendelkezéseivel összhangban kell tennie.

2.3.2. Külső felekkel kötött megállapodások

A külső felekkel történő megállapodások során a következő témaköröket –ahol azok értelmezhetőek– kell minimálisan a szerződésekbe foglalni, amennyiben az elektronikus információs rendszert érint:

- a megállapodásban résztvevő felek kötelezettségeit;
- valamennyi teljesítendő szolgáltatás és termék leírását, definícióját;
- az IBSz-ben és egyéb szabályzatokban foglaltak betartatását;
- a hozzáférés szabályozás és ellenőrzés módját, részletes feltételeit;
- az információ másolásának és nyilvánosságra hozatalának korlátozásait;
- a szellemi tulajdonjogokat és a szerzői jogi feltételeket;
- a személyes adatok kezelésének, feldolgozásának, továbbításának célját, jogalapját, időtartamát;
- a titoktartásra vonatkozó megállapodásokat;
- az alvállalkozók bevonásának feltételeit;
- a szerződésben foglaltak ellenőrzésének jogát;

3. Az emberi erőforrások biztonsága

3.1. A munkaviszony kezdetekor

Feladat	Informatikai osztály-vezető	VMA üzem-vezető	Humán igazgató	Területi vezetők (adatgazdák)	Információ-biztonsági Felelős
Dolgozói Felelősségvállalási Nyilatkozat	-	-	V, Sz	-	-
Kezdeti jogosultságok és eszközök	V	V	-	V, Sz	-
Információbiztonsági oktatások	-	-	V	T	V, Sz
V=Végrehajtó; Sz=Számonkérhető; K=Konzulens; T=Tájékoztatandó					

3.1.1. Dolgozói Felelősségvállalási Nyilatkozat

A munkavállalók belépéskor a munkaszerződéshez kapcsolódó – 2. számú mellékletet képező – nyilatkozatban ismerik el, hogy az Informatikai Biztonsági Szabályzatban meghatározott biztonsági elvárásoknak, előírásoknak eleget tesznek.

A munkaszerződésnek és a Dolgozói Felelősségvállalási Nyilatkozatnak a belépő munkatárssal történő aláíratása és adminisztrálása a Humán igazgatóság feladata és felelőssége.

3.1.2. Kezdeti jogosultságok és eszközök

Felvételhez szükséges az informatikai és egyéb feladatkörök azonosítása, főleg a kulcsfontosságú IT alkalmazottak esetében. Ennek felelőse az új kolléga közvetlen felettese, vagy a területi vezetője.

A folyamat indításáért a Jogosultság igénylése, módosítása, visszavonása formanyomtatvány – 3. sz. melléklet – papír alapú kitöltésével az adott területi vezető – osztályvezető, üzemvezető, igazgató – a felelős. Külső szolgáltató esetén a Nitrogénművek Zrt.-n belüli kapcsolattartó – területi vezető – a felelős, engedélyezésért a szintén a területi vezető (adatgazda), végrehajtásért pedig az igényelt jogosultságtól függően az Informatikai osztályvezető és/vagy a VMA üzemvezető felelős.

3.1.3. Információbiztonsági oktatások

Az új belépők számára az IBSz-ben foglalt előírások tudatosítása érdekében az Információbiztonsági Felelős biztonsági alapképzést biztosít a belépéstől számított 5 munkanapon belül. Az oktatás szakmai lebonyolítása az Információbiztonsági Felelős feladata és felelőssége, melyet a Humán igazgatóság tájékoztatása alapján tud elvégezni.

3.2. A munkaviszony fennállása során

Feladat	Informatikai osztály-vezető	VMA üzem-vezető	Humán igazgató	Területi vezetők (adatgazdák)	Információ-biztonsági Felelős
Az információ-biztonság tudatosítása	-	-	T	V	V, Sz
Viselkedési szabályok betartatása	V	V	-	V, Sz	V
Szoftverhasználati szabályok betartatása	V	V	-	V, Sz	V
Fegyelmi eljárások	-	-	T, V, Sz	K, T	K, T
V=Végrehajtó; Sz=Számonkérhető; K=Konzulens; T=Tájékoztatandó					

3.2.1. Az információbiztonság tudatosítása

Az Információbiztonsági Felelős indokolt esetben, de legalább évente egyszer ismételt képzést tart a biztonságtudatosság növelése érdekében, mely során a legfontosabb változásokról részletes tájékoztatást ad az érintetteknek

Az oktatáson való részvétel minden munkavállaló számára kötelező, aki a munkavégzése során informatikai rendszert használ – a részvételt jelenléti íven kell igazolni – a részvétel biztosítása pedig a szervezeti egységek vezetőnek a feladata.

A felhasználók a szabályzatokat érintő változásokról, valamint a legfontosabb információbiztonsági eseményekről és trendekről az oktatások mellett időszakosan az Intraneten, illetve e-mail-en kapnak tájékoztatást, mely az Információbiztonsági Felelős feladata és felelőssége.

3.2.2. Viselkedési szabályok

Az elektronikus levelezésre és az Internetes böngészésre vonatkozó szabályok:

- A vállalati levelező rendszer a munkavégzéssel kapcsolatos ügyintézést szolgálja. A levelező rendszer tárterülete korlátozott;
- Felhasználók nem használhatják más azonosítóját vagy hamis azonosító adatokat;
- A vállalati levelező kliens beállításait nem szabad módosítani pl. a Thunderbirdben gmail, freemail, stb. fiókot beállítani;
- Ismeretlen helyről származó, gyanús e-mail megnyitását a felhasználó köteles mérlegelni, mert a levél vagy csatolmánya vírust tartalmazhat. A mérlegelés során az IT osztály valamelyik kollégájának a véleményét ki kell kérni. Az ilyen leveleket célszerű olvasatlanul, másnap törölni – ezáltal a víruskeresőnek nagyobb esélye van a vírus kiszűrésére.
- A Nitrogénművek Zrt. fenntartja a jogot, hogy a vállalati levelezést és Internet használatot ellenőrizhesse abból a célból, hogy az üzleti célú kommunikációs csatornák magán vagy üzleti célú használatával okozott-e hátrányt a Nitrogénművek Zrt. üzletvitele vagy hírneve tekintetében, illetőleg veszélyeztette-e ezeket.
- Vállalati e-mail címet magáncélra – online regisztrációhoz, hírlevél feliratkozáshoz, fórum feliratkozáshoz – nem szabad használni, ennek betartását a Nitrogénművek Zrt. rendszeresen ellenőrizheti.

Nem megengedett az alábbiakban bemutatásra kerülő viselkedési módok és tevékenységek:

- Az Internetet használóknak bármilyen anyagot továbbítani vagy letölteni, amely nem szolgál közvetlenül üzleti célokat;
- Automatikusan továbbítani – forwarding – egy levelet a belső hálózatból egy külső levelező (például gmail, freemail vagy bármely egyéb) hálózatba;
- Az üzleti kommunikációra nyilvános levelező hálózatot (például gmail, freemail, vagy bármely egyéb) használni;
- Zavaró, indokolatlanul nagyméretű, félreinformáló és lánc levelek küldése;
- Másokra nézve sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység;
- Profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése.

- A hálózati forgalom lehallgatása, megfigyelése, kivéve, ha az az IT osztályhoz vagy megbízottjához kapcsoló, üzemeltetési feladat ellátásához szükséges tevékenységet végez.
- Az Internet segítségével üzleti tevékenységi-, vagy érdekkörbe tartozó állományok, adatok kijuttatása, külső kiszolgálókra való feltöltése, illetve bármilyen módon történő megosztása.
- Automatizált letöltő alkalmazások, kliensek használata csak az Informatika számára megengedett a rendszerek frissítéséhez.
- Minden olyan alkalmazás letöltése/telepítése/használata, amely alkalmas Interneten keresztül történő erőforrás megosztásra.

A fenti szabályok betartatása és állandó jellegű ellenőrzése a Területi vezetők feladata és felelőssége, mely feladatuk elvégzésében az Információbiztonsági Felelős és az Informatikai vagy VMA üzem munkatársai is segítik őket.

3.2.3. Szoftverhasználati szabályok

Kizárólag olyan szoftvereket és dokumentációkat szabad használni, amelyek megfelelnek a vonatkozó szerződésbeli, szerzői jogi, vagy más jogszabályi elvárásoknak.

A számítógépek és a fájlmegosztások folyamatos ellenőrzésével biztosítani kell a mennyiségi licencekkel védett szoftverek és a kapcsolódó dokumentációk jogszerű használatát, vagyis: hogy ezt a lehetőséget nem használják szerzői joggal védett munka jogosulatlan megosztására, megjelenítésére, végrehajtására vagy reprodukálására.

A számítógépeken csak és kizárólag az Informatikai vagy a VMA üzem arra jogosult munkatársai telepíthetnek, módosíthatnak, vagy távolíthatnak el bármilyen fajta szoftvert.

A fenti szabályok betartatása és állandó jellegű ellenőrzése a Területi vezetők feladata és felelőssége, mely feladatuk elvégzésében az Információbiztonsági Felelős és az Informatikai vagy VMA üzem munkatársai is segítik őket.

3.2.4. Fegyelmi eljárások

Munkáltatói fegyelmi eljárást kell kezdeményezni azokkal a munkavállalókkal és külső partnerekkel szemben, akik a biztonsági előírásokat súlyosan vagy következetesen megsértve fegyelmi vétséget követnek el, mint például:

- biztonsági előírások megsértése vagy gondatlan munkavégzés következtében nagy vagyoni kár, többletköltség keletkezik;
- bizalmas adatok, információk gondatlan vagy szándékos kiszivárogtatása;
- a személyes adatok védelmére vonatkozó jogszabályok sérelme;
- sorozatos, kismértékű szabályszegések esetén;

- jogszabálysértés történt, vagy bűncselekmény gyanúja esetén;

Fegyelmi vétség esetén az Információbiztonsági Felelősnek vagy a munkavállaló közvetlen felettesének, illetve területi vezetőjének kötelessége jeleznie azt a Humán igazgatóság felé, akik kezdeményezhetik a fegyelmi eljárást. Külső partner esetében a szerződés szerinti kapcsolattartó hivatott eljárni.

3.3. A munkaviszony megváltozásakor

Feladat	Informatikai osztály-vezető	VMA üzem-vezető	Humán igazgató	Területi vezetők (adatgazdák)	Információ-biztonsági Felelős
Munkavégzés tartós szünetelése	V	V	Sz	K	-
Áthelyezések, átirányítások, kirendelések	V	V	-	V, Sz	-
V=Végrehajtó; Sz=Számonkérhető; K=Konzulens; T=Tájékoztatandó					

3.3.1. Munkavégzés tartós szünetelése

A munkavégzés várhatóan 1 hónapnál hosszabb szünetelése – GYES, GYED hosszantartó betegség – esetén a felhasználó jogosultságait a távollét időszakára le kell tiltani, de törölni nem szabad. A folyamat indításáért a Jogosultság igénylése, módosítása, visszavonása formanyomtatvány – 3. sz. melléklet – papír alapú kitöltésével a Humán igazgatóság felelős, a végrehajtása pedig az adott jogosultságtól függően az Informatikai osztályvezető vagy a VMA üzemvezető feladata. A szüneteltetés alól kivételes esetekben el lehet tekinteni, de ilyenkor a felettes területi vezető köteles azt írásban indokolni a Humán igazgatóság felé.

3.3.2. Áthelyezések, átirányítások, kirendelések

A korábbi jogosultságokat felül kell vizsgálni, szükség esetén gondoskodni azok módosításáról vagy visszavonásáról. A folyamat indításáért a Jogosultság igénylése, módosítása, visszavonása formanyomtatvány – 3. sz. melléklet – papír alapú kitöltésével az adott területi vezető a felelős, külső szolgáltató esetén a Nitrogénművek Zrt.-n belüli kapcsolattartó – területi vezető – a felelős, engedélyezésért a szintén a területi vezető – adatgazda – végrehajtásért pedig az igényelt jogosultságtól függően az Informatikai osztályvezető és/vagy a VMA üzemvezető felelős.

3.4. A munkaviszony megszűnésekor

Feladat	Informatikai osztály-vezető	VMA üzem-vezető	Humán igazgató	Területi vezetők (adatgazdák)	Információ-biztonsági Felelős
Hozzáférési jogosultságok visszavonása	V	V	-	V, Sz	-
Infokommunikációs eszközök visszaszolgáltatása	V, Sz	-	-	-	-
Tájékoztatás a jogokról és a kötelezettségről	-	-	V, Sz	-	-
V=Végrehajtó; Sz=Számonkérhető; K=Konzulens; T=Tájékoztatandó					

3.4.1. Hozzáférési jogosultságok visszavonása

Valamennyi munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban álló valamennyi természetes személynek az információkhoz és információfeldolgozó eszközökhöz való hozzáférési jogosultságát meg kell szüntetni, amikor alkalmazásuk megszűnik, szerződésük, illetve megállapodásuk lejár. A folyamat indításáért a Jogosultság igénylése, módosítása, visszavonása formanyomtatvány – 3. sz. melléklet – papír alapú kitöltésével az adott területi vezető a felelős, külső szolgáltató esetén a Nitrogénművek Zrt.-n belüli kapcsolattartó – területi vezető – a felelős, engedélyezésért a szintén a területi vezető (adatgazda), végrehajtásért pedig az adott jogosultságtól függően az Informatikai osztályvezető és/vagy a VMA üzemvezető felelős.

Ha az érintett részéről fennállhat az üzletmenetet vagy információbiztonságot sértő magatartás veszélye, a jogosultságokat még az érintett tájékoztatását megelőzően vissza kell vonni!

3.4.2. Infokommunikációs eszközök visszaszolgáltatása

Valamennyi alkalmazottnak, a szerződő félnek vissza kell szolgáltatnia a Nitrogénművek Zrt. valamennyi használatra átvett vagyontárgyát, amikor alkalmazásuk, szerződésük, illetve megállapodásuk lejár, illetve megszűnik.

Az infokommunikációs eszközök kihelyezésére és visszaszolgáltatására vonatkozó szabályok és formanyomtatványok a 3/2017 (VII.01.) gazdasági igazgatói rendelkezésben találhatóak.

3.4.3. Tájékoztatás a jogokról és kötelezettségekről

A Humán igazgatóság feladata tájékoztatni a kilépőt az esetleg reá vonatkozó, jogi úton is kikényszeríthető, a jogviszony megszűnése után is fennálló kötelezettségekről, valamint arról, hogy a szervezet fenntartja magának a hozzáférés jogát a kilépő személy által korábban használt, kezelt elektronikus információs rendszerekhez és szervezeti információkhoz.

4. Hozzáférés-felügyelet

Feladat	Területi vezetők (adatgazdák)	Informatikai osztályvezető	VMA üzemvezető	Információ-biztonsági Felelős
Azonosítás	K	V,SZ	V,SZ	-
Hitelesítés	K	V,SZ	V,SZ	-
Engedélyezés	V, SZ	V	V	K
Felügyelet	K	V,SZ	V,SZ	T
V=Végrehajtó; Sz=Számonkérhető; K=Konzulens; T=Tájékoztatandó				

4.1. Azonosítás

4.1.1. Felhasználói fiókok

Az elektronikus információs rendszereknek minden belső és külső felhasználót egyedileg kell azonosítaniuk annak érdekében, hogy:

- minden egy adott időpontban végzett tevékenység összerendelhető legyen egy természetes személlyel;
- az összerendelés egyértelmű, megváltoztathatatlan, később is visszakereshető legyen.

A beépített (ún. built-in) fiókokat (User, Guest, Admin, root, stb.) is vagy nevesíteni kell – átnevezéssel –, vagy le kell tiltani. Amennyiben erre nincs mód, úgy technikai fiókként kell kezelni azokat.

Korábban már felhasznált azonosítókat a megszüntetésüktől számított 6 hónapig nem lehet ismételten kiadni, vagy egyéb módon használatba venni.

4.1.1.1. Kivételek

Ha a rendszer által nem lehetséges az egyedi azonosítás, akkor azzal egyenrangú védelmi intézkedésként a papír alapú nyilvántartás – pl. szakmány napló – is elfogadható, ha abból egyértelműen kiderül, hogy egy adott időpontban mely természetes személy használta az adott fiókot.

4.1.2. Privilegizált fiókok

A privilegizált funkciók eléréséhez erre a célra dedikált –szintén nevesített– fiókokat kell létrehozni az információs rendszerekben. A privilegizált – kiemelt jogosultságú – fiókokat egységes névkonvenció alapján javasolt elnevezni, mely alapján megkülönböztethetőek az általános – felhasználói – fiókoktól.

A privilegizált fiókokkal általános – nem rendszergazdai – tevékenységet végezni tilos!

Minden más követelmény – beleértve a kivételek kezelését is – megegyezik a felhasználói fiókoknál ismertetettekkel.

4.1.3. Technikai fiókok

A nem nevesített – technikai vagy szolgáltatás – fiókot nem személyhez, hanem szervezeti egységhez kell rendelni, mely esetben mindig az adott szervezeti egység vezetője felelős a fiókért és annak használatával elvégzett módosításokért. Technikai fiók a jogosultsági szintjétől függően lehet felhasználó vagy privilegizált.

4.2. Hitelesítés

A Nitrogénművek Zrt. tulajdonában vagy használatában lévő valamennyi elektronikus információs rendszer esetében az azonosítást legalább egy hitelesítő mechanizmussal is ki kell egészíteni. A hitelesítés mechanizmus általános módszere a felhasználói azonosítóhoz tartozó jelszó alkalmazása.

4.2.1. Felhasználói fiókok jelszavai

A jelszavakkal kapcsolatos minimális elvárások – melyeknél csak szigorúbbakat szabad alkalmazni – minden rendszer esetében:

- a jelszavak hossza legalább 8 karakter kell, hogy legyen;
- sem részben, sem egészében nem tartalmazhatja a fiókazonosítót;

A felhasználói fiókok esetében a jelszavak megváltoztatásának gyakoriságára vonatkozóan – az információs rendszerek eltérő célja, használati és technikai feltételei miatt – nincs egységes követelmény, azokat az Informatikai osztály vagy a VMA üzem munkatársai a legjobb gyakorlat alapján határozzák meg és állítják be a rendszereken.

A kezdeti jelszavakat a rendszerüzemeltetést végző munkatársak személyesen vagy a munkavállaló mobiltelefonjára küldött SMS üzenetben adhatják át. E-mail-ben küldeni tilos!

A jelszavak bizalmasságát minden felhasználónak meg kell őriznie, azokat más személy tudomására hozni szigorúan tilos! A jelszavakat azok kompromitálódása – vagy annak gyanúja – esetén haladéktalanul meg kell változtatni, vagy a hozzá kapcsolódó fiókot le kell tiltani.

4.2.2. Privilegizált fiókok jelszavai

A privilegizált – kiemelt jogosultságú – fiókok jelszavaira az alábbi – szigorúbb – követelményeket kell alkalmazni:

- a jelszavak hossza legalább 8 karakter kell, hogy legyen;
- sem részben, sem egészében nem tartalmazhatja a fiókazonosítót;
- az alábbi négyféle karaktertípus közül legalább hármat tartalmaznia kell:
  - kisbetű (a..z)
  - nagybetű (A..Z)
  - számjegy (0..9)

- speciális (!,$,#,%, stb.)
- a jelszavakat legalább 90 naponként meg kell változtatni;
- az új jelszó nem lehet azonos a legutóbb használt 4 bármelyikével.

Minden más követelmény megegyezik a felhasználói fiókok jelszavainál ismertetettekkel.

4.2.3. Technikai fiókok

A nem nevesített – technikai vagy szolgáltatás – fiókok jelszavát csak elzárt borítékban vagy jelszókezelő rendszerben lehet tárolni, és az ahhoz való hozzáféréseket naplózni kell.

Továbbá a nem nevesített – technikai vagy szolgáltatás – fiókokhoz tartozó jelszavakkal kapcsolatos követelmények – legyenek azok felhasználói vagy privilegizált fiókok – az alábbiak szerint módosulnak:

- a jelszavak hossza legalább 14 karakter kell, hogy legyen;
- a technikai fiókok jelszavát minden megismerést követően, vagy minimum évente egyszer meg kell változtatni, és ismételten elzárni azt borítékba vagy felvinni a jelszókezelő rendszerbe.

A fenti módosítások együttesen értelmezendők és alkalmazandók a felhasználói vagy privilegizált fiókok jelszavaira vonatkozó követelményekkel (függően attól, hogy a technikai fiók felhasználóinak vagy privilegizáltnak minősül-e).

4.2.3.1. Kivételek

Kivételt képeznek a munkaállomások operációs rendszerének beépített technikai fiókjaihoz – built-in administrator – tartozó jelszavak, melyek megváltoztatására csak akkor van szükség, ha a jelszó kitudódik vagy a jelszót ismerő valamely személy munkaviszonya megváltozik, megszűnik.

4.3. Engedélyezés

Az elektronikus információbiztonsággal kapcsolatos engedélyezés kiterjed minden, az érintett szervezet hatókörébe tartozó:

- emberi, fizikai és logikai erőforrásra;
- eljárási és védelmi követelményszintre és folyamatra.

4.3.1. Legkisebb jogosultság elve

A felhasználók csak a számukra kijelölt feladatok végrehajtásához szükséges jogosultságokat kaphatják meg az információkhoz és a rendszer erőforrásaihoz való logikai hozzáférés során.

4.3.2. Jogosultságok felülvizsgálata

A nem indokolt, felesleges jogosultságok megszüntetésének érdekében a hozzáférési jogosultságokat éves rendszerességgel felül kell vizsgálni, és az indokolatlan – a legkisebb jogosultság elvével nem megegyező – hozzáféréseket vissza kell vonni.

4.4. Felügyelet

4.4.1. Sikertelen hitelesítési kísérletek

Öt sikertelen bejelentkezési kísérletet követően az elektronikus információs rendszernek automatikusan zárolnia kell a fiókot – legyen az felhasználói vagy privilegizált, hagyományos vagy technikai – legalább egy óra időtartamra. A feloldást az Informatikai vagy VMA üzem arra jogosult munkatársai oldhatják fel, miután meggyőződtek arról, hogy nem valós fenyegetés miatt történt a zárolás.

Valós fenyegetés vagy egymás utáni többszöri zárolás esetén haladéktalanul értesíteni kell az Informatikai vagy VMA üzem vezetőjét és az Információbiztonsági Felelőst!

4.4.2. Inaktív fiókok nyomon követése

A meghatározott ideje inaktív – használaton kívüli – fiókokat felül kell vizsgálni és szükség szerint gondoskodni azok letiltásáról vagy eltávolításáról. A tolerálható inaktivitás ideje – mely egyben a felülvizsgálat gyakoriságát is meghatározza – fióktípusonként az alábbi:

- nem technikai fiókok esetében: 30 nap;
- technikai fiókok esetében: egy naptári év.

4.4.2.1. Kivételek

Kivételt képeznek a munkaállomások operációs rendszerének beépített technikai fiókjai – built-in administrator –, melyek jellegüknél fogva inaktív – használaton kívüli – állapotban vannak.

5. Incidensek kezelése

Feladat	Felhasználó (személyzet)	Diszpécser	Informatikai osztályvezető	VMA üzem-vezető	Információ-biztonsági Felelős
Üzemen belüli incidensek	V	T, V	T, V, Sz	T, V, Sz	K
Üzemen kívüli incidensek	V	T, V	T, V, Sz	T, V, Sz	K
Információbiztonsági incidensek	-	-	V	V	T, V, Sz
V=Végrehajtó; Sz=Számonkérhető; K=Konzulens; T=Tájékoztatandó					

5.1. Üzemen belüli incidensek

Az üzem területén – vagy az üzemhez tartozó rendszerek esetében – bekövetkező incidensek esetén a felhasználó (személyzet) köteles azt haladéktalanul jelenteni a diszpécser felé, aki jogosult a hibát az Informatikai osztály vagy a VMA üzem illetékes – munkaidőn kívül az ügyeletet ellátó – munkatársa felé jelezni.

5.2. Üzemen kívüli incidensek

Az üzem területén kívül – irodai vagy külső helyszínen – bekövetkező incidensek esetén a felhasználók kötelesek azt haladéktalanul jelenteni az Informatikai osztály illetékes munkatársa felé.

5.3. Információbiztonsági incidensek

Az Informatikai osztály vagy VMA üzem illetékes – vagy ügyeletet adó –munkatársának minden információbiztonságot érintő – személyes vagy üzleti adatok bizalmasságát, sértetlenségét vagy rendelkezésre állását veszélyeztető – incidensről haladéktalanul – telefonon – tájékoztatnia kell az Információbiztonsági Felelőst!

Az információbiztonsági incidensekről az Információbiztonsági Felelős köteles nyilvántartást vezetni, valamint szükség esetén kezdeményezi a megfelelő kárenyhítő intézkedéseket vagy a jogszabály által előírt lépéseket.

6. Meghatározások

- **adat:** az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;
- **adatbiztonság:** az adatok jogosulatlan megszerzése, módosítása vagy tönkretétele elleni műszaki és szervezeti intézkedések és eljárások együttes rendszere;
- **adatgazda:** annak a szervezeti egységnek a vezetője, ahová jogszabály vagy közjogi szervezetszabályozó eszköz az adat kezelését rendeli, illetve ahol az adat keletkezik;
- **azonosítás:** azonosításról beszélünk, amikor egy személy – vagy program – valakinek – vagy valaminek – állítja vagy vallja magát. Ez történhet felhasználónévvel, folyamatazonosítóval, intelligens kártyával vagy bármi mással, amely egyedileg azonosítja az alanyt;
- **bizalmasság:** az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;
- **biztonsági osztály:** az elektronikus információs rendszer védelmének elvárt erőssége;

- **biztonsági osztályba sorolás:** a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása;
- **biztonsági szint:** a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
- **biztonsági szintbe sorolás:** a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére;
- **elektronikus információs rendszer:** az adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;
- **elektronikus információs rendszer biztonsága:** az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;
- **életciklus:** az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;
- **engedélyezés:** a felhasználók – vagy programok – csak sikeres azonosítás és hitelesítés után kaphatnak engedélyt a rendszer erőforrásaihoz való hozzáféréshez, az azonosságuknak és a jóváhagyott jogosultságaiknak megfelelően;
- **felhasználó:** egy adott elektronikus információs rendszert igénybe vevők köre;
- **fenyegetés:** olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;
- **fizikai védelem:** a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem;
- **hitelesítés:** a személyazonosság igazolásának folyamata, amikor az alanyok megfelelő hitelesítő adatokat (pl. jelszó, kulcs, újlenyomat) nyújtanak személyazonosságuk igazolásához;
- **incidens:** nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat;
- **információbiztonsági incidens:** olyan incidens, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és

amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;

- **internet:** az egész világot körülölelő nyilvános információs hálózat;
- **intranet:** vállalati belső információs hálózat;
- **külső felhasználó:** A Nitrogénművek Zrt.-vel szerződéses – vagy egyéb, nem munkavállalói – kapcsolatban álló személy, aki a szervezet informatikai rendszerével kapcsolatba kerülhet;
- **rendelkezésre állás:** annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;
- **sértetlenség:** az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;
- **sérülékenység:** az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetés megvalósulhat;
- **üzleti titok:** A működéshez, az üzletmenethez és a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik;
- **védelmi intézkedés:** a fenyegetettség bekövetkezési valószínűségének csökkentésére, illetve a bekövetkezéskor jelentkező kár mérséklésére szervezési vagy technikai eszközökkel tett intézkedés;

7. Mellékletek

1. SZÁMÚ MELLÉKLET: BIZTONSÁGI SZINTBE ÉS OSZTÁLYBA SOROLÁS

A szervezeti egységek elvárt biztonsági szintbe sorolása:

Szervezeti egység neve	Biztonsági szint
Informatikai osztály	**2**
Villamos és Műszer-Automatika üzem	**2**

Az elektronikus információs rendszerek elvárt biztonsági osztályba sorolása:

Elektronikus információs rendszer	Biztonsági osztály	Bizalmasság	Sértetlenség	Rendelkezésre állás
IT technikai rendszerek	**2**	2	2	2
Vagyonvédelmi rendszer	**2**	2	2	2
Termelési adatokat archiváló rendszerek	**2**	2	2	2
Üzleti rendszer	**2**	2	2	2
Bérszámfejtő rendszer	**2**	2	2	2
Termelésirányítási rendszerek	**2**	2	1	1
SAP Integrált ügyviteli rendszer	**2**	2	2	2

Az egyes elektronikus információs rendszerek részét képező alkalmazások:

Alkalmazás \ Rendszer	IT technikai rendszerek	Vagyonvédelmi rendszer	Termelési adatokat archiváló rendszerek	Üzleti rendszer	Bérszámfejtő rendszer	Termelésirányítási rendszerek	SAP Integrált ügyviteli rendszer
Fájlszerver - hálózat	x						
Levelező rendszer	x						
Sales Force				x			
SAP							x
PHD			x				
OPUS					x		
Munkruha nyilvántartó					x		
Webshop				x			
Vision			x				
Emerson - Delta V						x	
Man - Turbo						x	
Honeywell - Experion PKS						x	
InTouch						x	
ABB Scada						x	
ExpertAlert						x	
Siemens WinCC						x	
Seawing		x					
Video rendszer		x					
Proplanta				x			
Coface				x			
Banki alkalmazások							x

2. SZÁMÚ MELLÉKLET: DOLGOZÓI FELELŐSSÉGVÁLLALÁSI NYILATKOZAT

A nyilatkozat célja

A nyilatkozat célja a felhasználókban tudatosítani, hogy munkájuk során a lehető legnagyobb gondossággal járjanak el az elektronikus információs rendszerekben tárolt adatok használatakor annak érdekében, hogy az adatok bizalmassága, sértetlensége, és rendelkezésre állása a felhasználó szándékos, vagy gondatlan magatartásából ne sérüljön, illetve a felelősségük számon kérhető legyen. Az informatikai infrastruktúrában tárolt adatok a munkáltató tulajdonát, üzleti titkát, illetve a munkavállalóinak és partnereinek személyes adatát képezik.

Dolgozói felelősségvállalási nyilatkozat

Alulírott …….…… (azonosító vagy cégnév: ……..), mint a Nitrogénművek Zrt. munkavállalója/szerződéses partnere kijelentem, hogy az Informatikai Biztonsági Szabályzatban foglaltakat megismertem, a rám vonatkozó szabályokat megértettem és azokat magamra nézve kötelező érvényűnek elismerem.

Pétfürdő, 201… ……

…….

Nyilatkozattevő

3. SZÁMÚ MELLÉKLET: JOGOSULTSÁG IGÉNYLÉS, MÓDOSÍTÁS, VISSZAVONÁS

JOGOSULTSÁG IGÉNYLÉS:

ÚJ: **MÓDOSÍTÁS:** **VISSZAVONÁS:**

Szervezeti egység / üzem neve:.....

Felhasználó neve: .....

azonosítója (ha van már): .....

Beállítandó jogosultság: .....

.....

Törlendő jogosultság:.....

Módosítás oka: .....

Érvényesség, módosítás kezdete:.....

Érvényesség, visszavonás vége:.....

Dátum: ....

Területi vezető aláírása

JOGOSULTSÁG BEÁLLÍTÁS:

Rendszer / Szoftver	Módosítás	Csoporttagság	Jogosultság
	Ú / M / V		
	Ú / M / V		
	Ú / M / V		
	Ú / M / V		

Dátum: ....

Rendszerüzemeltetést végző munkatárs aláírása