Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium

Adatvédelmi szabályzat

2023

Tartalomjegyzék

Preambulum ... 3

I. Fejezet ... 4

AZ ADATOK KEZELÉSÉVEL ÖSSZEFÜGGŐ SZABÁLYOK ... 4

1. A Szabályzat hatálya, érvényesítése: ... 4
2. A védelmi szabályozás célja: ... 5
3. Értelmező rendelkezések: ... 5
4. Az adatkezelői és adatfeldolgozói tevékenységre vonatkozó szabályok: ... 6
5. Hatásvizsgálat, Mérlegelési teszt, kockázat elemzése: ... 8
6. Az adatkezelési nyilvántartásba vétel: ... 9
7. Az érintett jogai ... 9
8. Az adatvédelmi felelős, adatvédelmi tisztviselő: ... 10
9. Az adatvédelmi tisztviselő jogállása: ... 10
10. A kezelt adatok célja és fajtái: ... 10
11. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium tulajdonát képező és a munkavállalók által használt eszközök ellenőrzése ... 14
12. Adatvédelmi szabályok megsértésének estei: ... 16
13. Adatvédelmi incidens jelentése: ... 16

II. Fejezet ... 19

AZ ADATBIZTONSÁGGAL KAPCSOLATOS ÁLTALÁNOS SZABÁLYOK ... 19

14. A Szabályzatban foglaltak érvényesüléséhez szükséges feltételrendszer: ... 19
15. Megismerési kötelezettség: ... 19
16. Az infrastruktúrához kapcsolódó biztonsági intézkedések ... 19
17. informatikai, számítástechnikai adatvédelem: ... 20
18. Iratkezeléssel kapcsolatos Alapelvek és biztonsági intézkedések ... 23
19. Az informatikai rendszer átadása – átvétele ... 23
20. Az informatikai Rendszer üzemeltetése ... 23
21. Az informatikai rendszer leállítása ... 24
22. Az informatikai rendszer fejlesztésének biztonsági szempontból lényeges dokumentumai: ... 24

III. Fejezet ... 25

AZ INFORMATIKAI HÁLÓZAT ÉS A HOZZÁFÉRÉSI JOGOSULTSÁGOK ... 25

23. A Déli Agrárszakképzési Centrum fizikailag elkülönülő informatikai területek ... 25

IV. Fejezet 25
ADATVÉDELMI INCIDENS 25
24. Fogalma 25
25. Incidensek besorolása 25
26. Incidens-kezelő csoport 26
27. Adatvédelmi incidens azonosítása, minősítése, típusa 26
28. Adatvédelmi incidens jelentése 27
29. Az érintett tájékoztatása az adatvédelmi incidensről 28
30. Az adatvédelmi incidensek nyilvántartása 28
31. Kockázatértékelés szempontjai 29
V. Fejezet 29
FOGALMAK 29
BELSŐ ADATKEZELÉSI NYILVÁNTARTÁS, MINT ÖNÁLLÓ DOKUMENTUM 32

Preambulum

A munkáltatói, munkavállalói, tanuló jogviszonnyal és a vizsgákra jelentkezőkkel, valamint a vagyonvédelemmel kapcsolatos és szükséges iratok, adatok kezelése megköveteli az adatvédelemmel, a személyes adatok védelmével kapcsolatos feladatok egységes rendszerbe foglalását.

A szabályozás célja, hogy biztosítsa az adatok védelmét, garanciákat teremt, amelyek alapján az adatvédelem a lehetőségekhez képest a legmagasabb szinten valósítható meg. Az adatkezelővel szemben támasztott követelményeknek való megfelelés érdekében a megfogalmazott adatvédelmi intézkedések az adatok bizalmasságát, hitelességét és sértetlenségét kívánják biztosítani.

A megbízható működés érdekében az informatikai rendszer hardware és szoftver eszközeinek rendelkezésre állását és funkcionalitását biztosító intézkedéseket fogalmaz meg.

A szabályzat jogszabályi alapjai a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról szóló (továbbiakban: adatvédelmi) törvény, a társadalmi indokoltság, a személyes részvétel, az érintettek és az adatfajták korlátozása, a célhoz kötöttség, a továbbadás korlátozása, az adathelyesség, az időbeli korlátozás, a nyíltság, a biztonsági intézkedések és a felelősség elveiről és szabályozásáról szóló európai Adatvédelmi törvény rendelkezései, az Európai Parlament által elfogadott „A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről” (továbbiakban rendelet).
A munka törvénykönyvéről szóló 2012. évi I. törvény (továbbiakban Mt.) a személyhez fűződő jogokra (9.§, 10.§ és a 11.§) vonatkozó előírásai, a szakképzésről szóló 2019. évi LXXX. törvény XX. fejezete (szakképzési adatkezelés), valamint a személy és vagyonvédelemről szóló 2005. évi CXXIII. törvény.

A személyes adatok védelme érdekében feladatok kerülnek megfogalmazásra, azért, hogy érvényesüljenek az adatok kezelésével, feldolgozásával kapcsolatos különböző jogszabályok előírásai.

Adatvédelmi szempontból az EU Parlament 2016. május 16-án hatályba lépett adatvédelmi rendelet 2. szakasz 32. cikk adatbiztonsági követelményeinek való megfelelés érdekében a nagy tömegű személyes adatok, az adatkezelésre használt rendszer bizalmas jellegét, integritását, elérhetőségét és rugalmasságát, a fizikai vagy műszaki probléma esetén a visszaállíthatóság, rendelkezésre állás és hozzáférés biztosítani kell.

I. Fejezet

AZ ADATOK KEZELÉSÉVEL ÖSSZEFÜGGŐ SZABÁLYOK

Jelen Adatvédelmi Szabályzat (továbbiakban: Szabályzat) az adatvédelmi törvényre figyelemmel, és a Déli Agrárszakképzési Centrum biztonságpolitikai elveire épülve készült.

A szabályozás az adatkezelő által kezelt személyes adatok biztonságának kialakítása érdekében meghatározza, és egységes keretbe foglalja azokat az eljárási követelményeket, amelyeket az adatkezelő valamennyi alkalmazottjának - a rávonatkozó mértékben - ismernie és a biztonsági követelmények érvényesítése érdekében alkalmaznia kell.

Biztosítja a rendkívüli eseményekre, katasztrófa elhárítására, valamint a rendkívüli időszaki kötelezettségekre történő adatvédelmi felkészülést, illetve bekövetkezésük esetén az adatkezelő adatvédelmi szempontoknak való megfelelést és működőképességet.

1. A SZABÁLYZAT HATÁLYA, ÉRVÉNYESÍTÉSE:

1.1. A Szabályzat területi hatálya:

Kiterjed az adatkezelő teljes működési területére, valamennyi alkalmazott informatikai eszközre és szoftverre, az iratkezelésre és az irattári tervre.

1.2. A Szabályzat személyi hatálya:
Kiterjed az adatkezelővel munkaviszonyban vagy munkavégzésre irányuló jogviszonyban álló valamennyi természetes és jogi személyre, vizsgára jelentkezettekre, vizsgázókra, a vizsgáztatásban résztvevő valamennyi érintettre.

1.3. A Szabályzat időbeli hatálya:

A kiadás napjától visszavonásig érvényes.

1.4. A Szabályzat érvényesítése és a megismerési kötelezettség:
A Szabályzat kidolgozása, elkészítése és szükség szerinti módosítása és a szabályzat betartásának ellenőrzése az igazgató feladata. A Szabályzatban előírtak betartatásáért hatás- és jogosultsági körére vonatkozóan minden érintett alkalmazott felelős.

A Szabályzat előírásait az adatkezelőnél dolgozó minden személy a szakmai feladatköréhez szükséges mértékben köteles megismerni, a vonatkozó előírásokat betartani és betartatni.

A Szabályzat egyes előírásait, a munkavégzéséhez szükséges mértékben, minden, az adatkezelővel munkaviszonyban, illetve egyéb szerződéses jogviszonyban álló foglalkoztatottal ismertetni kell.

A Szabályzat előírásait megszegőkkel, illetve a jelentési kötelezettséget elmulasztókkal szemben, a hatályos törvényeknek, rendeleteknek és belső szabályzóknak megfelelő, jogszerű felelősségre vonást kell alkalmazni.

2. A VÉDELMI SZABÁLYOZÁS CÉLJA:

2.1. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium biztonságos ügymenetének érdekében meg kell határozni, és egységes keretbe foglalni azokat a biztonsági hardware és software feltételeket, valamint informatikai rendszeralkalmazási- és eljárási követelményeket, amelyeket a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium valamennyi alkalmazottjának - a rávonatkozó mértékben - ismernie és a biztonsági követelmények érvényesítése érdekében alkalmaznia kell.

2.2. Biztosítani a rendkívüli eseményekre, katasztrófa elhárításra, valamint a rendkívüli időszaki kötelezettségekre történő informatikai felkészülést, illetve bekövetkezésük esetén a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium informatikai működőképességét.

3. ÉRTELMEZŐ RENDELKEZÉSEK:

Személyes adat:
A személyes adatok körébe minden olyan adat beletartozik, ami tetszőleges élő személlyel, az érintettel kapcsolatos bármilyen információt hordoz, függetlenül attól, hogy az érintett ezeket mennyire kívánja védeni. Személyes adat az érintettre vonatkozó vélemény, minősítés, továbbá az adatból levonható következtetés is, sőt azok az adatok is személyes adatnak minősülnek, amelyek önmagukban nem, de más személyes adatokkal összekapcsolva az érintettel kapcsolatba hozhatók.
Az adatvédelmi törvény abból indul ki, hogy a személyes adataival mindenki maga rendelkezik, vagyis információs önrendelkezési jogot deklarál, de nem hagyja figyelmen kívül azt sem, hogy e jog nem korlátlan, így lehetővé kell tenni és teszi is a törvény, hogy a személyes adatok kezelését jogszabály elrendelhesse, vagy személyes adatok átadását – bizonyos keretek között –megengedje. A személyes adatok az érintett hozzájárulása nélküli kezelésének, és ehhez átadásának, átvételének igénye elsősorban az államigazgatás, a bűnüldözés területein merül fel, azonban nem hagyható figyelmen kívül az, hogy ez az igény mások jogainak biztosítása érdekében vagy például a gazdasági élet egyes területein is indokolt lehet.

Adatkezelés:
Személyes adat akkor kezelhető, ha ahhoz az érintett hozzájárult, vagy azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben - illetékes önkormányzat rendelete elrendeli. Az adat kezelésének jogalapja igazolt, célhoz kötöttsége fennáll.

Adatfeldolgozó:

Az adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az adatkezelő határozza meg. Az adatkezelési műveletekre vonatkozó utasítások jogszerűségéért az adatkezelő felel.
Az adatfeldolgozó tevékenységi körén belül, illetőleg az adatkezelő által meghatározott keretek között felelős a személyes adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért.

Adatvédelmi incidens:
A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan nyilvánosságra hozatalát vagy az azokhoz való jogosulatlan hozzáférést eredményezi.
Adatvédelmi kockázatok:

- adatok feletti rendelkezés elvesztése,
- adatlopás.

4. AZ ADATKEZELŐI ÉS ADATFELDOLGOZÓI TEVÉKENYSÉGRE VONATKOZÓ SZABÁLYOK:

4.1. Adatfelvétel, adatátvétel, adatigénylés

- Közvetlenül az érintettől felvett adatok.

4.2. Adatok tárolása

A személyes adatokat a célhoz-kötöttség fennállásáig lehet csak tárolni.

Adatfeldolgozással, adatkezeléssel és az adattovábbítással kapcsolatos technikai adatok tárolása
Az alábbi un. technikai adatokat kell - a tárolt személyes adatok célhoz-kötöttségének megszűnését és törlését követően is - számítógépes nyilvántartásba vett adathordozón 5 évig tárolni:

- Adatigénylés érkezésének dátuma,
- Személyes adatok felhasználásának módja,
- Személyes adatok továbbításának dátuma,
- Személyes adatok törlésének dátuma

4.3. Az adatkezeléssel szemben támasztott követelmények:

- felvételük és kezelésük tisztességes és törvényes;
- pontosak, teljesek és időszerűek;

- tárolásuk módja alkalmas arra, hogy az érintettet csak a tárolás céljához szükséges ideig lehessen azonosítani.

4.4. Az adatok felhasználása

Személyes adatokat csak a vonatkozó jogszabályokban és engedélyekben megfogalmazott célra lehet felhasználni. Harmadik személynek csak az érintett írásos beleegyezése esetén lehet továbbítani, illetéktelennek átadni tilos.

Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig.

4.5. Tájékoztatás hírközlő eszközön

Hírközlő eszközökön csak olyan tájékoztatás adható, amely a személyes adatok védelméhez fűződő, és az Adatkezelő üzleti és működési érdekeit, valamint az adatvédelmet és adatbiztonságot nem sérti. Felvilágosítás adható általában az Adatkezelő adatkezelői, és az adatfeldolgozó szolgáltatói tevékenységéről, partnereiről, engedélyező és felügyeletet ellátó szervezetekről.

4.6. Adatok törlése, helyesbítése

A személyes adatot törölni kell, ha

a) kezelése jogellenes;
b) az érintett kéri;
   kivéve, ha a törvényi felhatalmazás alapján kezelt adatok, ill. jogérvényesítéshez szükséges adatok;
c) az adatkezelés célja megszűnt.

A törlési kötelezettség –a jogellenes adatkezelés kivételével - nem vonatkozik azon személyes adatra, amelynek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni.

A törlés tényéről a számítógépes adatbázisban technikai adatként öt évig tárolásra kerül a csoportazonosító és a dátum.

A valóságnak meg nem felelő adatot az adatkezelő helyesbíteni köteles.

A helyesbítésről és a törlésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban az adatot adatkezelés céljára továbbították. Az értesítés mellőzhető, ha ez az adatkezelés céljára való tekintettel az érintett jogos érdekét nem sérti.

4.7. Adattovábbítás

Az adatok akkor továbbíthatók, valamint a különböző adatkezelések akkor kapcsolhatók össze, ha az érintett ahhoz hozzájárult, vagy törvény azt megengedi, és ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.

Személyes adat az országból - az adathordozótól vagy az adatátvitel módjától függetlenül - külföldi adatkezelő részére csak akkor továbbítható, ha az érintett ahhoz hozzájárult, vagy törvény azt lehetővé teszi, feltéve, hogy az adatkezelés feltételei a külföldi adatkezelőnél minden egyes adatra nézve teljesülnek.

4.8. Adattovábbítás nyilvántartása

Az adatok átadását, minden esetben, jegyzőkönyvben kell rögzíteni, a jegyzőkönyveket nyilvántartásba vett iktatókönyvbe be kell iktatni. A jegyzőkönyvek elektronikus napló fájljait is öt évig meg kell őrizni.

Adatátadás céljára csak nyilvántartásba vett elektronikus adathordozó használható. E-mail mellékletként személyes adatokat csak tömörítve és titkosítva lehet továbbítani.

5. HATÁSVIZSGÁLAT, MÉRLEGELÉSI TESZT, KOCKÁZAT ELEMZÉSE:

5.1. A Rendelet meghatároz néhány körülményt (rendelet 35. cikk (7) bekezdés), amikor adatvédelmi hatásvizsgálatot kell elvégezni. Ezek a következők:

- természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen jelentős mértékben érintő döntések épülnek;
- a személyes adatok különleges kategóriái (Rendelet 9. cikk), vagy a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok (Rendelet 10. cikk) nagy számban történő kezelése; vagy
- nyilvános helyek nagymértékű, módszeres megfigyelése.

5.2. A hatásvizsgálatnak ki kell terjednie:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére (beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket);
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
- a kockázatok kezelését célzó intézkedések bemutatására.

6. AZ ADATKEZELÉSI NYILVÁNTARTÁSBA VÉTEL:

Az adatkezelő köteles az általa kezelt személyes adatokat nyilvántartásba venni és abban rögzíteni:

a) az adatkezelés célját;
b) az adatok fajtáját és kezelésük jogalapját;
c) az érintettek körét;
d) az adatok forrását;
e) a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját;
f) az egyes adatfajták törlési határidejét;
g) az adatkezelő, valamint az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét;
h) a belső adatvédelmi felelős nevét és elérhetőségi adatait.

.

7. AZ ÉRINTETT JOGAI

7.1. Hozzáférési jog, az adatkezelés céljának, a személyes adatok kategóriáinak, tárolásának időtartamának megismerése. Tájékoztatást és másolatot kérhet.

7.2. Helyesbítéshez való jog, kérheti a hiányos adatok kiegészítését, helyesbítését.

7.3. Törléshez való jog („az elfeledtetéshez való jog”), megszűnik a jogalapja az adatkezelésnek.

7.4. Adatkezelés korlátozásához való jog, ha vitatja az adatok pontosságát, ha az adatkezelés jogellenes és ellenzi a törlését, egyben kéri a felhasználás korlátozását.

7.5. Az adatkezelés korlátozásához való jog

7.6. Az adathordozhatóságához való jog, ha az adatkezelés hozzájáruláson vagy szerződésen alapul, a rá vonatkozó adatokat megkapja, kérheti adatkezelők közötti közvetlen továbbítását.

7.7. A tiltakozáshoz való jog, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak a kezelése ellen.

7.8. A jog gyakorlásának biztosítása

7.9. Az érintett kérelmére az Adatkezelő tájékoztatást ad az általa kezelt, illetőleg az általa feldolgozott adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről (székhelyéről) és az adatkezeléssel összefüggő tevékenységéről, továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az adatokat.

7.10. Az Adatkezelő köteles az írásos kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül írásban, közérthető formában megadni a tájékoztatást.

7.11. Megtagadás esetén az Adatkezelő köteles az érintettel a felvilágosítás megtagadásának indokát közölni.

7.12. Az elutasított kérelmeket az adatkezelő nyilvántartja.

8. AZ ADATVÉDELMI FELELŐS, ADATVÉDELMI TISZTVISELŐ:

8.1. Az adatvédelmi felelős/tisztviselő Erdélyi Tamás. elérhetőségei

elektronikus mail címen erdelyit@deliaszc.hu
telefon: +36300196079

8.2. Az adatvédelmi felelős

8.3. közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

8.4. ellenőrzi e törvény és az adatkezelésre vonatkozó más jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzatok rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;

8.5. kivizsgálja a hozzá érkezett bejelentéseket, és a jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;

8.6. elkészíti a belső adatvédelmi és adatbiztonsági szabályzatot;

8.7. vezeti a belső adatvédelmi nyilvántartást;

8.8. gondoskodik az adatvédelmi ismeretek oktatásáról.

9. AZ ADATVÉDELMI TISZTVISELŐ JOGÁLLÁSA:

- Az adatvédelmi tisztviselő tevékenységének aktív támogatása a kancellár, főigazgató, vizsgaközpont vezető és az intézményvezetők feladata.
- Az adatvédelmi tisztviselő részére elegendő idő biztosítása a feladatai ellátására.
- Az adatvédelmi tisztviselő kulcsszerepet játszik a szervezeten belül az adatvédelmi kultúra előmozdításában, és elősegíti a rendelet alapvető, például az adatok kezelésére vonatkozó elvekre, az érintett jogaira, a beépített és alapértelmezett adatvédelemre, az adatkezelési tevékenységek nyilvántartására, az adatkezelés biztonságára, valamint az adatvédelmi incidens bejelentésére és arról való tájékoztatásra vonatkozó rendelkezéseinek végrehajtásában.

10. A KEZELT ADATOK CÉLJA ÉS FAJTÁI:

10.1. Személyügyi adatkezelések a munkaviszony létesítése, teljesítése vagy megszüntetése céljából a munkavállaló

- neve,
- születési neve,
- születési helye,
- születési ideje,
- anyja születési neve,
- állandó bejelentett lakcíme,
- tartózkodási hely (amennyiben eltérő a lakóhelytől),
- adóazonosító jele,
- társadalombiztosítási azonosító jele (TAJ-szám),
- nyugdíjas törzsszám (nyugdíjas munkavállaló esetén),
- banki folyószámla száma.

10.2. Vagyonvédelmi kamera rendszer alkalmazása:

A 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól (továbbiakban Vvtv.) 26. § (1) pontja alapján az Adatkezelő jogosult a területén elektronikus megfigyelőrendszert kiépíteni.

A Vvtv. 28. (2) pontja alapján a közönség számára nyilvános jól látható helyen, jól olvashatóan, a területen megjelenni kívánó harmadik személyek tájékozódását elősegítő módon köteles figyelemfelhívó jelzést, ismertetést elhelyezni.

A Vvtv. 31. és 31/A § alapján a rögzített kép-, hang-, valamint kép- és hangfelvételt felhasználás hiányában legfeljebb a rögzítéstől számított harminc nap elteltével meg kell semmisíteni, illetve törölni kell.

A felvételek megtekintésére a intézményvezető és az Adatvédelmi felelős jogosult.

10.2.1. Vagyonvédelemmel és kamerás megfigyelő rendszer működtetésével kapcsolatos adatkezelés a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium területén.

A kamerarendszer a következő feltételek együttes fennállása esetén üzemeltethető:

- a kamerarendszer kizárólag az emberi élet, a testi épség, a személyi szabadság védelmét, a jogsértő cselekmények megelőzését és bizonyítását, valamint a közös tulajdonban álló vagyon védelmét szolgálja,
- a fennálló körülmények valószínűsítik, hogy a jogvédelem más módszerrel, mint a felvételek felhasználása, nem érhető el,
- alkalmazása a meghatározott célok eléréséhez elengedhetetlenül szükséges mértékig terjed, és nem jár az információs önrendelkezési jog aránytalan korlátozásával.

10.2.1. A kezelő személyek a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium alkalmazottjai, vagy megbízottjai tevékenységüket az adatfeldolgozói szerződésben foglaltak szerint végzik.

10.2.2. A képek, videó-felvételek tárolására digitális, beépített merevlemez áll rendelkezésre, amely 30 nap anyagát tudja tárolni.

10.2.3. A kamera-rendszer 0-24 óra működési vagy üzemelési idő/időszakot biztosít.

10.2.4. A kamerarendszer által rögzített felvételekhez kizárólag a rendszergazda és az intézmény igazgatója férhet hozzá, a felvételeket csak a bíróság, a szabálysértési vagy más hatóság részére továbbíthatják.

10.2.5. Az, akinek jogát vagy jogos érdekét a kamerarendszer által rögzített felvétel érinti, a felvétel rögzítésétől számított tizenöt napon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot annak üzemeltetője ne semmisítse meg, illetve ne törölje.

10.2.6. A kamerarendszerrel felszerelt épületbe, épületrészbe és a kamerák által megfigyelt területre belépni, ott tartózkodni szándékozó személyek figyelmét jól látható helyen, jól olvashatóan, a megfelelő tájékoztatásra alkalmas módon fel kell hívni az elektronikus megfigyelőrendszer alkalmazásának tényére, a tájékoztatásban meg kell jelölni az üzemeltető személyét és elérhetőségét is.

10.2.7. Az üzemeltető az érintett személyt - kérésére - köteles tájékoztatni a felvételek készítésével kapcsolatos minden tényről, így különösen annak céljáról és jogalapjáról, az üzemeltetésre jogosult személyéről, a felvételek készítésének időpontjáról és tárolásának időtartamáról, továbbá arról, hogy kik ismerhetik meg a felvételeket, a tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira, valamint jogorvoslati lehetőségeire.

10.2.8. Az adatkezelés jogalapja a Vvtv. 31. § (1) (2) bekezdése, a 30 § (2) bekezdése, valamint a 31 § (6) bekezdése.

10.2.9. Az adattárolás határideje: 30 nap, melyet az élelmiszeripari technológiai szabályok betartásának ellenőrzése és visszakereshetősége, valamint a nagy értékű áruszállítással kapcsolatos vagyonvédelmi érdekek indokolnak.

10.2.10. A kamera és megfigyelő rendszer működtetésére, karbantartására szolgáltatói szerződéses megállapodás és adatfeldolgozói megbízási szerződés alapján az illetékes kötelezett és jogosult. A személyes adatok körébe tartozó képfelvételekkel kapcsolatosan semmilyen adatkezelői jog nem illeti meg, ezért nem készíthet másolatokat, mentéseket sem.

10.2.11. A működtetési, karbantartási feladatainak ellátását és az adatvédelmi szempontok betartását a megbízó, mint adatkezelő a kancellár, a rendszergazdai feladatokat ellátó személy/vállalkozás és az adatvédelmi felelős köteles ellenőrizni.

10.3. Tárgyaláson készült hangfelvétel

Tárgyalásokkor a későbbi írásos jegyzőkönyv készítése érdekében hangfelvétel készülhet. A rögzítés lehetősége hozzájáruláson alapul, így az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény

20. § (2) pontja alapján a felvétel megkezdése előtt az érintetteket egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a 6. § (5) bekezdése alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

A hangfelvétel csak saját felhasználásra készíthető, azt másik fél számára nem adható ki. A hangfelvételt az írásos jegyzőkönyv elkészítése után 1 munkanappal, de legkésőbb a hangfelvétel készítése után 10 munkanappal később meg kell semmisíteni.

10.4. Pandémiás intézkedések esetén különleges adatok ideiglenes kezelése

10.4.1. Az adatkezelés jogalapja a rendelet 6. cikk (1) bek f) pontja szerinti jogos érdek, ill. közfeladatot ellátó adatkezelései esetében a 6. cikk (1) bek. e) pontja, az alapfeladatok zavartalan ellátásának szükségessége.

10.4.2. Az egészségügyi adatok kezelésének ezen esetében a rendelet 9. cikk (2) bek. b) pontja szerinti feltétel fennáll, mert a munkáltatónak munkajogi előírásokból fakadóan kötelezettsége a munkavállalók számára egészséges és biztonságos munkavégzési körülmények biztosítása.

10.4.3. Érintettek (munkavállalók) kötelezettsége:

A munkavégzésre irányuló jogviszonyban foglalkoztatott személyre vonatkozó magatartási követelményekből, az együttműködési kötelezettségből, valamint a jóhiszeműség és tisztesség elvéből levezethetően a foglalkoztatottaknak tájékoztatniuk kell a munkáltatót arról, ha bármilyen, a munkahelyet, a többi munkavállalót vagy a velük kapcsolatba kerülő harmadik személyeket érintő egészségügyi vagy egyéb kockázatról tudomásuk, ideértve saját potenciálisan fertőző megbetegedésük fennállásának veszélyét, így az esetlegesen fertőzött személlyel való feltételezett érintkezés tényét is.

10.4.4. a munkavállalók kötelezettsége, hogy a koronavírussal való feltételezett érintkezésük esetén ezt a tényt saját maguk és munkatársaik egészségének védelme érdekében haladéktalanul jelentsék az arra kijelölt személy részére, valamint haladéktalanul forduljanak a háziorvoshoz/foglalkoztatás egészségügyi szakellátó helyhez vagy más kezelőorvoshoz.

10.4.5. Az ideiglenesen kezelt adatok:

Amennyiben a munkavállaló bejelentést tesz vagy a kitettség gyanúja a munkavállaló által megadott adatokból megállapítható, akkor rögzíthetők az alábbi adatok:

- bejelenés időpontja,
- érintett személyazonossága megállapításához szükséges személyes adatok,
- külföldi utazás (magáncélú is) helyszíne és időpontja,
- külföldről érkező személlyel történő érintkezés tényére vonatkozó adatok.

10.4.6. Az adatok felvételének módja:

Kérdőív kitöltése alkalmazható, viszont a kérdőív nem tartalmaz egészségügyi kórtörténetre vonatkozó adatokat, nem kérjük dokumentum becsatolását sem.

10.4.7. Az adatok kezelésének időtartama:

A Járványügyi készültséget kezelő intézményi intézkedési terv szükségességének, a célhoz kötöttség fennállásáig.

10.5. Portaszolgálat:

10.5.1. Személyautóval érkező személyek beléptetése

A parkolóba történő behajtáskor a portaszolgálatot ellátó portás engedi be a gépjárműveket.

11. A DÉLI ASZC SZÉCHENYI ZSIGMOND MEZŐGAZDASÁGI TECHNIKUM, SZAKKÉPZŐ ISKOLA ÉS KOLLÉGIUM TULAJDONÁT KÉPEZŐ ÉS A MUNKAVÁLLALÓK ÁLTAL HASZNÁLT ESZKÖZÖK ELLENŐRZÉSE

11.1. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium igazgatója a munkavállalóknak indokolt esetben a munkavégzés céljára biztosítanak mobiltelefont, számítógépet, e-mail címet és internet-hozzáférést. A használat szabályairól és az ellenőrzés lehetőségéről a jelen szabályzat rendelkezik.

11.2. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium tulajdonát képező személyi számítógépeket és laptopokat, céges e-mail címeket a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium a munkavégzés céljából biztosítja, azokon magán célból személyes adatot tárolni tilos. Amennyiben a munkavállaló a tiltás ellenére ezen eszközökön magáncélú személyes adatait, (pl.: családi fotók, telefonkönyvek, saját adatbázisok stb.) tárolja, úgy Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium számítógép ellenőrzése során ezeket az adatokat is megismerheti. Ezen adat kezelése ellen kifogással nem élhet a munkavállaló, mert a nem munkavégzés céljából történő, de a Déli Agrárszakképzési Centrum eszközein való személyes adatok tárolása az adatkezeléshez történő Infotv. 5. § (1) a) szerinti érintetti hozzájárulásnak minősül.

11.3. A munkaadói e-mail címek, elektronikus levelezés ellenőrzése:

A Déli Agrárszakképzési Centrum munkavállalói tudomásul veszik, hogy mindazon e-mail címek, amelyekben a Déli Agrárszakképzési Centrum kiterjesztésként szerepel (...@deliaszc.hu; …@agrarvk.hu), a Déli Agrárszakképzési Centrum tulajdonát képezik és az ezen a címeken folytatott levelezés munkacélú levelezésnek minősül. A fogadott és küldött e-mailek tartalma a Déli Agrárszakképzési Centrum tulajdonát képezik.

Az ilyen címeken folytatott levelezésbe a Déli Agrárszakképzési Centrum megfelelő jogalap esetén jogosult betekinteni. A Déli Agrárszakképzési Centrum jogosult a fenti címeken folytatott levelezések meghatározott időnkénti biztonsági mentésére, az elektronikus levelező rendszer folyamatosságának és stabilitásának érdekében.

A céges e-mail címeken nem munkavégzési célú (magán vagy bármilyen egyéb) levelezést tilos folytatni. Amennyiben a munkavállaló „(...@deliaszc.hu;)" céges e-mail címén található leveleiben magán- vagy bármilyen egyéb célú levelezést folytat, ezzel egy időben a postafiókban magáncélú személyes adatait tárolja, úgy a Déli Agrárszakképzési Centrum az e-mail cím ellenőrzése során ezeket az adatokat is megismerheti. Ezen adat kezelés ellen kifogással nem élhet a munkavállaló, mert a nem munkavégzés céljából történő, de a Déli Agrárszakképzési Centrum e-mail címein való személyes adatok tárolása az adatkezeléshez történő Infotv. 5. § (1) szerint az érintett hozzájárulásának minősül. A Centrum intézményei által biztosított e-mail címekre is a fent megjelöltek az irányadók.

11.4. Az internet, külső kapcsolódások ellenőrzése

A fenti szabályok érvényesek az internethasználatra is: az internet használata munkaidőben csak Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium céljaira engedélyezett. Emiatt az internetezési adatok céges adatoknak minősülnek, - amennyiben egy ellenőrzés során a Déli Agrárszakképzési Centrum ezeket megismeri, ezek elveszítik személyes adat-jellegüket, illetve ezek megismerésére és tárolására az Infotv. 5. § (1) szerinti érintetti hozzájárulás ad jogalapot.

11.5. Az ellenőrzés folyamata

A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium a tulajdonában álló eszközöket, indokolt esetben korlátozás nélkül ellenőrizheti. Az ellenőrzés tényéről az ellenőrzés céljával összefüggően tájékoztatja az ellenőrzéssel érintett munkavállalót. A technikai ellenőrzést az igazgató által megbízott személy végezheti alkalmi vizsgálatok lefolytatásával. Amennyiben az intézmény gazdasági érdekeit veszélyeztető tevékenység valószínűsíthető, azt a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium bármely munkavállalója jelezheti az intézmény igazgatójának.

12. ADATVÉDELMI SZABÁLYOK MEGSÉRTÉSÉNEK ESTEI:

12.1. A szabályozás megsértéséből származó jogosulatlan és/vagy célhoz kötöttség nélküli adatkezelés, adattovábbítás vagy adatátadás.

12.2. Hanyag vagy gondatlan magatartással ok-okozati összefüggésbe hozható illetéktelen hozzáférés személyes adatokhoz.

12.3. Az adat- és informatikabiztonsági szabályzatban foglaltak (rezsimszabályok) be nem tartása miatt bekövetkezett adatvesztés, adatsérülés.

12.4. Jogosulatlan vagy a céltól eltérő adatkezelés

Adatkezelésnek tekintendő a személyes adatok felvétele, tárolása, feldolgozása, hasznosítása, megváltoztatása és a további felhasználásának a megakadályozása. Az adatkezelés akkor jogszerű, ha ahhoz az érintett hozzájárul, illetve ennek hiányában is, ha az adatkezelést törvény vagy törvényi felhatalmazás alapján helyi önkormányzati rendelet írja elő. Személyes adatot csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet kezelni. Ez esetben is csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas és csak a cél megvalósulásához szükséges mértékben és ideig. Ami e körbe nem illeszthető, az már az adatkezelés célhoz kötöttsége szabálya megsértésének minősül.

12.5. Tájékoztatási kötelezettség megszegése

Az érintett kérelmére az adatkezelő köteles tájékoztatás adni az általa kezelt adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, továbbá arról, hogy kik és milyen célból kapják vagy kapták meg az adatokat. Az adattovábbításra vonatkozó nyilvántartás és ennek alapján a tájékoztatási kötelezettség időtartamát az adatkezelést szabályozó jogszabály korlátozhatja. A korlátozás időtartama személyes adatok esetében öt évnél, különleges adatok esetében pedig húsz évnél rövidebb nem lehet. Az érintett tájékoztatása csak honvédelemi, nemzetbiztonsági, bűnmegelőzési és bűnüldözési érdekből tagadható meg. Az érintett polgári per útján (keresettel) érvényesítheti a tájékoztatáshoz fűződő jogát, míg a tájékoztatási kötelezettségét nem teljesítő, az adatot eltitkoló adatkezelő magatartása bűncselekménynek minősül.

13. ADATVÉDELMI INCIDENS JELENTÉSE:

13.1. Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az rendelet 55. cikk alapján illetékes felügyeleti hatóságnak, Nemzeti Adatvédelmi és Információszabadság Hatóságnak (NAIH) kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes

személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

Ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

Közölni kell a további tájékoztatást nyújtó adatvédelmi kapcsolattartó nevét és elérhetőségeit.

Ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

Ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

13.2. Az adatvédelmi incidensek nyilvántartása:

- az adatvédelmi incidenshez kapcsolódó tények,
- annak hatásai,
- tett intézkedéseket.

13.3. Az érintett tájékoztatása az adatvédelmi incidensről:

- Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.
- Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell az intézkedéseket is.
- Az érintettet nem kell tájékoztatni, ha az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat.
- Az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg.
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy

olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

- Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását.

13.4. Adatbiztonsági intézkedés elmulasztása

Az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

13.5. Szankciók (a magatartás által bekövetkezett sérelem, érdeksérelem súlyától függően):

Vezetői figyelmeztetés, fegyelmi eljárás, büntető feljelentés.

II. Fejezet

AZ ADATBIZTONSÁGGAL KAPCSOLATOS ÁLTALÁNOS SZABÁLYOK

A Számítástechnikai Védelmi Szabályzat is az adatvédelmi törvényre és a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium biztonságpolitikai elvei figyelembevételével készült.

14. A SZABÁLYZATBAN FOGLALTAK ÉRVÉNYESÜLÉSÉHEZ SZÜKSÉGES FELTÉTELRENDSZER:

14.1. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium informatikai és informatikavédelmi eszközei működtetéséhez szükséges pénzügyi fedezetet folyamatosan biztosítani kell.

14.2. Az informatikai védelmi tevékenység ellátásához kapcsolódó személyi és tárgyi feltételeket, a prioritásoknak és a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium esetleges szervezeti változásainak megfelelőn kell érvényesíteni.

15. MEGISMERÉSI KÖTELEZETTSÉG:

- A szabályzat előírásait a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégiumban dolgozó minden személy a szakmai feladatköréhez szükséges mértékben köteles megismerni, a vonatkozó előírásokat betartani és betartatni.
- A szabályzat egyes előírásait, a munkavégzéséhez szükséges mértékben, minden, a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégiummal munkaviszonyban, illetve egyéb szerződéses jogviszonyban álló foglalkoztatottal ismertetni kell.
- A szabályzat előírásait megszegőkkel, illetve a jelentési kötelezettséget elmulasztókkal szemben, a hatályos törvényeknek, rendeleteknek és belső szabályzóknak megfelelő, jogszerű felelősségre vonást kell alkalmazni.

16. AZ INFRASTRUKTÚRÁHOZ KAPCSOLÓDÓ BIZTONSÁGI INTÉZKEDÉSEK

16.1. ÁLTALÁNOS INTÉZKEDÉSEK

16.1.1. Az adatállományok kezelését, tárolását ellátó helyiségekbe, illetőleg munkaterületre kizárólag az adott adatállomány kezelését végző ügyintéző, illetőleg az illetékes vezető jelenlétében léphetnek be, illetőleg tartózkodhatnak más személyek.

16.1.2. Az ügyintézés csak az ügyfélfogadásra kijelölt részen lehetséges ügyintézői jelenlét mellett. Ezeket a helyiségeket az arra jogosult távolléte idején zárva kell tartani.

16.1.3. A számítógépeket az irodahelységekben úgy kell elhelyezni, illetve használni, hogy a képernyőn megjelenő információk ne legyenek láthatóak illetéktelen személyek (pl. ügyfél stb.) részére. A munkavégzés szüneteiben a számítógépet alaphelyzetbe kell állítani úgy, hogy azon információk, dokumentumok ne legyenek láthatóak.

16.1.4. Az adatkezelő a saját jelszavát köteles titokban tartani, azt harmadik fél számára semmilyen körülmény között át nem adhatja. Az adatkezelő jelszavával elkövetett cselekmény az adatkezelőt terheli. Amennyiben az adatkezelő azt észleli, hogy a jelszava illetéktelen személy tudomására jutott, köteles jelszavát azonnal megváltoztatni és ennek tényét az adatvédelmi felelősnek és rendszergazdának jelenteni.

16.1.5. Az igazgató, valamint az adatvédelmi felelős feladatkörében eljárva az intézmény valamennyi helyiségébe jogosult belépni, az ügyintézés bármely folyamatát jogosult megtekinteni, bármely iratanyagba jogosult betekinteni.

16.1.6. Az adatállományok kezelését, tárolását ellátó helyiségek és eszközök kulcsait a jogosult még ideiglenes jelleggel sem adhatja át más személy részére.

16.1.7. A helyiségek és az adattároló eszközök kulcsairól másolat csak indokolt esetben, az igazgató írásbeli engedélyével készíttethető.

16.1.8. A riasztóval ellátott helyiségek riasztóját az ügyintéző a napi munkavégzés befejezésekor üzembe helyezi. A riasztóberendezések üzemképességét havonta ellenőrizni kell. Az ellenőrzés tényét, valamint eredményét dokumentálni szükséges.

16.1.9. A - különös tekintettel a számítógépes helyiségekre - a tűzvédelmi előírásoknak megfelelő készültségi állapotú és számú tűzoltó-berendezést kell elhelyezni. A szerverszobát külön is el kell látni tűzvédelmi berendezéssel. A tűzvédelmi berendezések biztosításáért és annak üzemképességéért a tűzvédelmi felelős gondoskodik.

16.1.10. Minden számítástechnikai és informatikához kapcsolódó berendezést a napi munka befejezésével ki kell kapcsolni, a tápegységet áramtalanítani kell. A szervergépek kizárólag szükség esetén kapcsolhatók ki, erről a felhasználókat előzetesen értesíteni kell.

16.1.11. Az infrastruktúrához kapcsolódó biztonsági intézkedéseket a személyi változások során naprakészen aktualizálni kell.

17. INFORMATIKAI, SZÁMÍTÁSTECHNIKAI ADATVÉDELEM:

17.1. Az adatkezelés és az adatok feldolgozásának általános szabályai

17.1.1. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium számítástechnikai biztonságának - adatbiztonságnak - koncentrálódnia kell minden olyan, az intézményre vonatkozó tény, információ,

megoldás vagy adat komplex védelmére, amelynek „házon belül” maradásához a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium biztonsági érdeke fűződik, szerződéses kötelezettséget vállalt, ill. jogszabály arra kötelezi.

17.1.2. Számítástechnikai (logikai)- adatbiztonság körébe tartozik a számítástechnikai rendszer felépítése és működése; a külső- és belső rendszerfejlesztési tervek; az adatvédelmi előírások; a hozzáférési szintek, adat- és rendszertulajdonosi kijelölések; a számítógépes programok és nyilvántartások; az archiválási rendszer; a titokvédelem; a rendkívüli helyzetek kezelése, más országos informatikai rendszerhez csatlakozás; a híradástechnikai eszközök vonal- és titkosítási védelme; a szünetmentes tápellátás;

17.1.3. Egyéb irányú adatbiztonság körébe tartozik a nem elektronikus adathordozók (iratok) tárolása;

17.1.4. Az információk adatok “kiszivárgásának” vagy „kiszivárogtatásának” megelőzése, illetéktelen hozzáférés megakadályozása, adatvesztés kizárása.

17.1.5. Az adatállományok kezelését, tárolását ellátó helyiségekbe, illetőleg munkaterületre kizárólag az adott adatállomány kezelését végző ügyintéző, illetőleg az illetékes vezető jelenlétében léphetnek be, illetőleg tartózkodhatnak más személyek.

17.1.6. A szervergépek tárolására szolgáló helyiségbe kizárólag az informatikus jelenlétében lehet belépni, illetőleg benntartózkodni. Az informatikus távollétében a szerverszobában senki sem tartózkodhat.

17.1.7. Az adatállomány kezelését végző ügyintéző távolléte alatt az általa használt programokból köteles kijelentkezni, ezzel is megakadályozva az illetéktelen adathozzáférést.

17.1.8. A számítógépeket az irodahelységekben úgy kell elhelyezni, illetve használni, hogy a képernyőn megjelenő információk ne legyenek láthatóak illetéktelen személyek (pl. ügyfél stb.) részére. A munkavégzés szüneteiben a számítógépet alaphelyzetbe kell állítani úgy, hogy azon információk, dokumentumok ne legyenek láthatóak.

17.2. A hardverállományhoz kapcsolódó biztonsági intézkedések

17.2.1. A számítástechnikai berendezések használatára elsősorban annak kezelője, távolléte esetén a szervezeti egység munkatársai, illetve az informatikus jogosult. A szerverek kezelésére kizárólag az informatikus jogosult, annak üzemeltetéséért, illetőleg üzembiztonságáért felelős.

17.2.2. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium állományában lévő valamennyi számítástechnikai berendezésről technikai háttérnyilvántartást (gép-, szerver- és szoftvernyilvántartás) kell vezetni. Valamennyi hardver berendezés műszaki állapotáról, annak változásáról, átkonfigurálásáról nyilvántartást kell vezetni. A technikai háttérnyilvántartást naprakészen az informatikus, a leltárnyilvántartást a gazdasági csoport vezeti.

17.2.3. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium belső hálózatán kizárólag az intézmény állományába tartozó számítástechnikai eszköz hardver, szoftver — használható.

17.2.4. Az állományába tartozó számítástechnikai eszköz a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégiumon kívül nem használható, azt az intézményből kivinni tilos. E rendelkezés nem vonatkozik a hordozható számítástechnikai eszközökre (pl. notebook, mobiltelefon) illetve az előadások megtartásához igényelt informatikai eszközökre.

17.2.5. A hardver és a szoftver elemek rendszerbe állítását - amennyiben nem a forgalmazó cég végzi el - kizárólag az informatikus jogosult elvégezni.

17.2.6. A munkaidő alatt az informatikus köteles folyamatosan rendelkezésre állni annak érdekében, hogy a számítástechnikai rendszerben fellépő meghibásodás elhárítható legyen. Jelentősebb szolgáltatás kiesés esetén köteles értesíteni a jegyzőt.

17.2.7. A számítástechnikai rendszerben keletkező üzemzavar esetén az adatkezelő a hiba, illetve a tünetek megjelölésével értesíti az informatikust. Az informatikus haladéktalanul megkezdi a hibaelhárítást, az üzemzavar megszüntetését.

17.2.8. A hardver eszközök karbantartásáról, javításáról az informatikus rendszergazda gondoskodik.

17.3. A szoftverekhez kapcsolódó biztonsági intézkedések

17.3.1. Szoftver installációt kizárólag az informatikus végezhet a teljes informatikai rendszerben.

17.3.2. Fájlcserélésre alkalmas szoftver (torrent) használata a rendszerben tilos.

17.3.3. Az installált valamennyi szoftvert nyilván kell tartani. A nyilvántartás naprakész vezetéséért az informatikus a felelős.

17.3.4. A meglévő szervereken tárolt adatállományokról rendszeresen biztonsági mentéseket kell készíteni. A biztonsági mentéseket és azok tárolását az informatikus látja el.

17.3.5. A beszerzett szoftver termékek- kizárólag a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégiumi leltárban nyilvántartott eszközökre telepíthetők, azokat harmadik személy részére átadni tilos.

17.3.6. Az adatkarbantartást az adatállomány kezelője folyamatosan látja el. Az érintett adatállomány kezelője felelős az általa kezelt adatállomány naprakészségéért.

17.3.7. Az igazgató az oktatással kapcsolatos kérdésekben az informatikus javaslatára szükség esetén külső céget vagy személyt is megbízhat egyes adatállományok karbantartásával.

17.3.8. A számítógépes programok, szoftverek kezelésében, használatában az informatikus igény esetén segítséget nyújt az adatkezelők részére.

17.4. Programhoz való hozzáférés, programvédelem

17.4.1. A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni.

17.4.2. Minden felhasználónak jelszóval kell védenie a programhoz tartozó profilját. Ezeket a jelszavakat illetéktelen személyektől gondosan védeni kell.

18. IRATKEZELÉSSEL KAPCSOLATOS ALAPELVEK ÉS BIZTONSÁGI INTÉZKEDÉSEK

18.1. A papír alapú adathordozókra vonatkozóan az érvényes irattári terv és iratkezelési szabályzat szerint kell iktatni, tárolni és megsemmisíteni az iratanyagokat.

18.2. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium csak a rendszergazdánál nyilvántartásba vett, és archivált szoftvereket (rendszereket) szabad alkalmazni.

18.3. Az informatikai beszerzések és fejlesztések során a biztonságot és titokvédelmet érintő szoftverek, nyilvántartások, adatbázisok és adatátviteli rendszerek kialakításánál törekedni kell a belső erőforrások felhasználására.

18.4. Vizsgálni kell a programhelyességet, valamint a dokumentációkat, a szakmai követelményeknek-, valamint ügyviteli szakmai-, továbbá a rendszerbiztonsági megfelelést;

18.5. Az elfogadott rendszert archiválni kell, és el kell készíteni a biztonsági- és tartalék példányokat, azokat a megfelelő biztonsági fokozattal kell tárolni;

18.6. A rendszert, vagy annak módosítását a rendszergazda telepíti;

18.7. Ugyancsak a rendszergazda felelőssége a számítógépes katasztrófa után a rendszer helyreállítása, ismételt installálása.

19. AZ INFORMATIKAI RENDSZER ÁTADÁSA – ÁTVÉTELE

A rendszer átadás - átvétele csak az üzemszerű körülmények között hibátlanul működő teszt eredmények után engedélyezhető;

A vonatkozó dokumentációkat a rendszer átadásával egyidejűleg át kell adni a felhasználónak.

A rendszer átvétele során a felhasználó az igénye szerinti működőképes állapotot-, a rendszer minősítésének megfelelő biztonsági védettségét a biztonságért felelős informatikai szolgáltatást nyújtó az aláírásával igazolja.

Olyan rendszert a felhasználónak kiadni tilos, amelynek logikai- és számítógépes rendszerterve, illetve maga a rendszer és annak felhasználói dokumentáció minden eleme nincs összhangban.

20. AZ INFORMATIKAI RENDSZER ÜZEMELTETÉSE

A rendszereket a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium, mint a rendszer felhasználója üzemelteti. Felhasználók azok a személyek, akik a napi és időszaki tevékenységeket elvégzik.

A rendszer üzemeltetésével kapcsolatos észrevételeiket Üzemeltetési Naplóban kötelesek vezetni.

A rendszergazda köteles az észrevételekre a szükséges intézkedéseket megtenni;

A rendszer hibáit a rendszergazda köteles összegyűjteni. A vonatkozó fejlesztési javaslatokat és a fejlesztéssel kapcsolatos feladatokat a rendszergazda közreműködésével igazgató készíti el.

Az üzemelés során felmerült hiányosságok pótlását, a hibák kijavítását, illetve a szükséges módosítások és a vonatkozó dokumentációk elkészítését a rendszergazdának kell megtennie;

Az ügyvitelkövetésből adódó változtatások miatt minden esetben új rendszer-verziószámot kell adni.

21. AZ INFORMATIKAI RENDSZER LEÁLLÍTÁSA

A rendszer leállítását, a rendszert alkalmazó felhasználói környezet megszűnése, vagy olyan mértékű átalakítási igény okozhatja, amely teljesen új rendszer kialakítását igényli.

A rendszert, az üzemeltetési feltételek megszűnésével le kell állítani. A menteni szükséges adatokat az igazgató igénye alapján kell menteni, illetve azokat és a záró adatállományokat az érvényességi idő lejártáig (utódrendszer alkalmazása esetén is) archiválni kell.

A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium számára a továbbra is szükséges adatok mentéséről, az új rendszerbe történő átemeléséről, illetve a szabályzókban előírt archiválási kötelezettségek betartásáról, a rendszergazdának kell gondoskodnia.

22. AZ INFORMATIKAI RENDSZER FEJLESZTÉSÉNEK BIZTONSÁGI SZEMPONTBÓL LÉNYEGES DOKUMENTUMAI:

- Projektindítási jegyzőkönyv;
- Megvalósíthatósági tanulmány
- Számítógépes rendszerterv
- Felhasználói dokumentáció

III. Fejezet

AZ INFORMATIKAI HÁLÓZAT ÉS A HOZZÁFÉRÉSI JOGOSULTSÁGOK

23. A DÉLI AGRÁRSZAKKÉPZÉSI CENTRUM FIZIKAILAG ELKÜLÖNÜLŐ INFORMATIKAI TERÜLETEK

23.1. Adatbázisok, nyilvántartások
  23.1.1. munkavállalók adatainak nyilvántartása
  23.1.2. diákok, vizsgázók adatainak nyilvántartása
  23.1.3. könyvelő program és adatbázis
  23.1.4. bérszámfejtési bérkönyvelési program és adatbázis
23.2. Fénykép-felvételek tárolása.
23.3. Internetes és más külső kapcsolatot biztosító szerver/számítógépek;
23.4. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium kommunikációs eszközei;
23.5. A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium egyéb tevékenysége keretében működő számítógépek.

IV. Fejezet

ADATVÉDELMI INCIDENS

24. FOGALMA

A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan kezelését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

25. INCIDENSEK BESOROLÁSA

25.1. Bizalmassági incidens, amikor a személyes adatok véletlen vagy felhatalmazás nélküli közlése vagy ezekhez való hozzáférés történik,
25.2. sértetlenséggel kapcsolatos incidens, amikor az adatok véletlen vagy jogtalan megváltoztatása történik,
25.3. hozzáférhetőséggel kapcsolatos incidens, amikor személyes adatok véletlen vagy jogtalan megsemmisítése vagy ezek elvesztése következik be.
25.4. Az adatvédelmi incidens következményei a megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek:
  - a személyes adatok feletti rendelkezés elveszítése,
  - jogaik korlátozása,

- személyazonosság lopását vagy a személyazonossággal való visszaélés,
- pénzügyi veszteség,
- jó hírnév sérelmét,
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése.

26. INCIDENS-KEZELŐ CSOPORT

Az adatvédelmi incidenst vizsgáló csoport tagjai:

az intézmény igazgatója
rendszergazdai feladatokat ellátó személy
az érintett terület vezetője, ahol az incidens bekövetkezett.

A döntést hozó vezető az oktatást érintő ügyekben az igazgató.

Az incidens kezelésével összefüggő feladatok

- incidens azonosítása,
- incidens minősítését bizonyító adatok, dokumentumok vizsgálata,
- incidens által bekövetkezett kockázat, kár, veszélyhelyzet meghatározása,
- elhárítás érdekében teendő intézkedések meghatározása,
- incidens bejelentésére vonatkozó döntés meghozatala,
- incidens okainak feltárása,
- érintettek tájékoztatása,
- teljes vizsgálat megindítása igény szerint,
- kapcsolattartás a NAIH-val.

27. ADATVÉDELMI INCIDENS AZONOSÍTÁSA, MINŐSÍTÉSE, TÍPUSA

A biztonságnak olyan sérülése, amely által a tárolt, továbbított vagy más módon kezelt adatok véletlen vagy jogellenes módon megsemmisül, elvész, megváltozik, jogosulatlanul közlésre kerül, vagy jogosulatlan hozzáférést eredményez.

- Személyes adatok feletti rendelkezés elvesztése,
- jogok korlátozása,
- hátrányos megkülönböztetés,
- személyazonosság-lopás vagy azzal való visszaélés,
- pénzügyi veszteség,
- az álnevesítés engedély nélküli feloldása,
- jóhírnév sérelme,
- titoktartási kötelezettség megszegése által bizalmas jelleg sérülése,
- gazdasági vagy szociális hátrány.

Az azonosítást követően a minősítés érdekében tisztázni kell az alábbiakat:

- Milyen kockázatot jelent az érintett természetes személy(ek) jogaira és szabadságaira tekintettel.
- Kiváltó okok, körülmények, amelyek az incidens bekövetkezéséhez vezettek. Az incidens bekövetkezésének körülményei.
- A személyes adatok érzékenységének meghatározása,
- Az incidensben érintett személyes adatok száma.
- Az érintett adatok fajtái, ill. az érintetti kör speciális tulajdonságai.

28. ADATVÉDELMI INCIDENS JELENTÉSE

28.1. Az adatvédelmi incidenst az érintett részleg, ill. az adatfeldolgozó a tudomására jutást követően indokolatlan késedelem nélkül azonnal jelenti az adatvédelmi incidenst kezelő csoport valamely állandó tagjának;

28.2. Ismertetnie kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

28.3. Közölni kell az a további tájékoztatást nyújtó adatkezelésért felelős kapcsolattartó nevét és elérhetőségeit;

28.4. Ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

28.5. Ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket is;

28.6. A csoport döntése alapján bejelenti az adatvédelmi incidenst (legfeljebb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott), a rendelet 55. cikk alapján illetékes felügyeleti hatóságnak, NAIH-nak.

28.7. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

28.8. Ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve, akkor nem kell bejelentenie a hatóságnak, de az incidenst nyilvántartásba kell venni.

28.9. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

29. AZ ÉRINTETT TÁJÉKOZTATÁSA AZ ADATVÉDELMI INCIDENSRŐL

- Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.
- Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell az intézkedéseket is.
- Az érintettet nem kell tájékoztatni, ha az adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
- az adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az (1) bekezdésben említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.
- Ha az adatkezelő még nem értesítette az érintettet az adatvédelmi incidensről, a felügyeleti hatóság, miután mérlegelte, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár-e, elrendelheti az érintett tájékoztatását.

30. AZ ADATVÉDELMI INCIDENSEK NYILVÁNTARTÁSA

Az adatvédelmi nyilvántartás a NAIH által ajánlott és kitöltött bejelentő lapok (Melléklet) alapján, azok iktatásával és elektronikus másolatának tárolásával valósul meg, mely a teljes felsorolás nélkül az alábbiakat tartalmazza:

- az incidens jellege, az adatvédelmi incidenshez kapcsolódó tények, annak hatásai,
- érintettek kategóriái és száma,
- adatok kategóriái és száma,
- valószínűsíthető következmények,
- az incidens következményei elhárítására, következmények enyhítésére tett és tervezett intézkedések,

Az adatvédelmi incidensek nyilvántartását az adatvédelmi felelős vezeti elektronikus dokumentumban, Excel táblázatban.

A nyilvántartás része az incidenssel kapcsolatos vizsgálódás dokumentumának elektronikus másolata.
Az incidens vizsgálatát és kezelését - a NAIH honlapjáról letölthető - papíralapú incidens-bejelentő lap (Melléklet) kitöltésével kell dokumentálni.

31. KOCKÁZATÉRTÉKELÉS SZEMPONTJAI

- az incidens típusa,
- a személyes adatok típusa és mennyisége,
- az érintettek azonosíthatóságának lehetősége,
- a következmények súlya az érintettekre nézve – kategóriái, száma,
- a következmények súlya az adatkezelőre nézve (speciális kategória).

V. Fejezet

FOGALMAK

Az üzleti titok fogalma:

A tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvény 4. §-a (3) bekezdésének a) pontja határozza meg az üzleti titkot, amely „a gazdasági tevékenységhez kapcsolódó minden olyan tény, információ, megoldás vagy adat, amelynek titokban maradásához a jogosultnak méltányolható érdeke fűződik, és amelynek titokban tartása érdekében a jogosult a szükséges intézkedéseket megtette”.

Ezt erősíti meg a Btk. 300. §-a, amely az üzleti titok védelméről rendelkezik. A Btk. „a büntetőjogi védelmet kizárólag azokra az üzleti titkokra terjesztette ki, amelyeknek titokban maradásához a jogosultnak nemcsak, hogy méltányolható érdeke fűződik, hanem a szükséges intézkedéseket meg is tette az üzleti titok titokban tartása érdekében. Az intézkedések körében a legkézenfekvőbb az üzleti titokká minősítés, de e körbe tartozik minden olyan ésszerű és szükséges intézkedés, amely az üzleti titok megőrzése érdekében indokolt”.

Tehát a menedzsment csak akkor bízhat joggal abban, hogy az üzleti tikok megsértőivel szemben (jogi) védelemben részesül, ha bizonyítani tudja, hogy minden ésszerű intézkedést megtett az üzleti titkok megőrzéséhez.

Adatvédelem

Az információs önrendelkezési jogról és az információszabadságról1 (röviden adatvédelmi törvény) szóló 2011. évi CXII. törvény szerint az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához

szükségesek. Az adatokat – kiemelten az államtitokká és a szolgálati titokká minősített személyes adatot – védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

Adat- informatika-biztonság:

Az adatok bizalmasságának, hitelességének és sértetlenségének biztosítása. A megbízható működés érdekében az informatikai rendszer hardware és szoftver eszközeinek folyamatos rendelkezésre állása és funkcionalitása.

Bizalmasság:

A titokvédelmi szempontból lényeges értékek, adatok védelme a jogosulatlan felfedés ellen.

Információ:

Az adat, az adatállomány szerkezete, a kezelésére vonatkozó szabályok, eljárások és az adathordozó együttesen.

Logikai védelem:

Az értékekhez és információkhoz való szándékos vagy véletlen illetéktelen hozzáférés, megváltoztatás és megsemmisítés ellen alkalmazott eszközök, eljárások és módszerek alkalmazása.

Kockázat:

A veszélyforrások által okozható károk bekövetkezésének lehetősége, amely az intézménynél veszteséget vagy szolgáltatási, működési zavarokat okozhat.

Felhasználói kézikönyv:

A rendszerindítás és a rendszerzárás közötti műveletek, menük, a rendszer által támogatott, vagy megvalósított folyamatok (tranzakciókat) szabatos leírását tartalmazza.

Tartalmazza továbbá a felhasználó számára kezelhető módon, a felhasználói hibákból való kivezetések lehetőségeit és az informatikai biztonsági - védelmi előírásokat.

Üzemeltetési kézikönyv:

A rendszer szabályszerű indításához és lezárásához, valamint a meghatározott időszakonként végzett tevékenységek (mentések, archiválások) végrehajtásához szükséges műveleteket írja le.

Rendszergazda kézikönyv:

A rendszergazda részére készül. Az adatbázisok szerkezetét, a programok összefüggéseit és logikai sémáját, valamint a lehetséges hibák okait és következményeinek leírását tartalmazza.

Ügyviteli leírás:

Azon szakmai terület szaknyelvű leírása, amelynek részleges vagy teljes támogatására az adott informatikai rendszer készült.

Help Desk szolgálat:

A számítástechnikai központ munkatársai által ellátott, szolgáltatás-jellegű tevékenység (felhasználói problémák kezelése).

Help Desk napló:

A HelpDeskhez érkező felhasználó bejelentések, információk, továbbá az azokkal kapcsolatos események rögzítésére szolgáló napló. A naplózást az Számítógépközpont vezetője végzi.

Függő ügy:

Minden önálló tárgyú bejelentés és információ, amely további intézkedéseket igénylő ügy, a befejezéséig.

Rendelkezésre állás:

Annak biztosítása, hogy az erőforrás az eredeti szolgáltatásokat folyamatosan és rendeltetés-szerűen nyújtsa ott és akkor, amikor és ahol szükség van rá.

a Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium

ADATKEZELÉSI BELSŐ NYILVÁNTARTÁSA

Székhely: 8734 Somogyzsitfa, Ady E. u. 8.

Készült: 2023. január 2.

Jóváhagyta:

Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum Szakképző Iskola és Kollégium 2. Somogyzsitfa-Szőcsénypuszta

Tóth Krisztina
igazgató

1. Munkaviszonnyal kapcsolatos adatkezelés

Adatkezelési nyilvántartási azonosító	adatkezelésről szóló 2011. évi CXII. tv. 65. § (3) a) alapján a NAIH nem vezet nyilvántartást az adatkezelővel munkaviszonyban álló személyek adatinak kezeléséről
adatkezelés célja	munkavállalók jogosultságok elismerése, kötelezettségek tanúsítása,
adatkezelés jogalapja	MT 10.§ (1) és (3) szakasz, a szakképzésről szóló 2019. évi LXXX. törvény XX. fejezet 114.§. (2) A szakképző intézmény az alkalmazottja foglalkoztatása, számára a juttatások, kedvezmények, kötelezettségek megállapítása és teljesítése, továbbá az e törvényben meghatározott nyilvántartások vezetése céljából kezeli valamint érintett hozzájárulása
érintettek köre	munkavállalók
érintettekre vonatkozó adatok	a) az alkalmazott aa) családi és utónevét és születési családi és utónevét, ab) nemét, ac) születési helyét és idejét, ad) anyja születési családi és utónevét, állampolgárságát, nem magyar állampolgár esetén a Magyarország területén való tartózkodás jogcímét és a tartózkodásra jogosító okirat megnevezését és számát, ae) lakcímét, levelezési címét, elektronikus levelezési címét és telefonszámát, af) végzettségével, szakképesítésével, szakképzettségével és idegennyelv-ismeretével kapcsolatos adatokat, ag) oktatási azonosító számát, ah) pedagógusigazolványának számát, ai) társadalombiztosítási azonosító jelét, aj) adóazonosító jelét, ak) fizetésiszámla-számát, b) az alkalmazott valamennyi korábbi foglalkoztatásával kapcsolatosan ba) a munkahely megnevezését, bb) a jogviszony típusát, kezdő és záró dátumát, valamint megszűnésének módját, bc) a beosztását és a munkakörének megnevezését,

	bd) bér- és bérjellegű juttatásai mértékét, valamint az azok kiszámításának alapjául szolgáló időtartamot, c) az alkalmazott szakképző intézménnyel fennálló jogviszonyával kapcsolatosan ca) a b) pontban meghatározott adatokat, cb) a bűnügyi nyilvántartó szerv által kiállított hatósági bizonyítvány számát és keltét, cc) a munkaköri alkalmassági vizsgálat eredményének adatait, cd) munkaidejének mértékét, munkából való távollétének jogcímét és időtartamát, ce) kirendelésének adatait, cf) értékelésének eredményét, cg) továbbképzési kötelezettsége teljesítésével kapcsolatos adatokat, ch) vétkes kötelezettségszegésével, illetve kártérítési felelősségével összefüggő adatokat.
adatok forrása	munkavállalók
adatkezelés időtartama	a foglalkoztatásra irányuló jogviszony megszűnésétől számított ötödik év utolsó napjáig kezeli, az adatkezelés céljának megvalósulásáig, a munkaviszony megszűnéséig, a nyugdíjfolyósításról szóló jogszabályban meghatározott határideig
adatkezelés módja	elektronikus és papírhordozó

2. Tanulói jogviszonnyal és a képzésekben résztvevőkel, valamint a vizsgázókkal kapcsolatos adatkezelés

Adatkezelési nyilvántartási azonosító	adatkezelésről szóló 2011. évi CXII. tv. 65. § (3) a) alapján a NAIH nem vezet nyilvántartást az adatkezelővel munkaviszonyban álló személyek adatinak kezeléséről
adatkezelés célja	tanulói jogviszony, jogosultságok elismerése, kötelezettségek tanúsítása,
adatkezelés jogalapja	a szakképzésről szóló 2019. évi LXXX. törvény XX. fejezet 114.§. (1) A szakképző intézmény a szakmai oktatással összefüggésben a tanulói jogviszony, illetve a felnőttképzési jogviszony létesítése és fenntartása céljából kezeli, valamint a szakmai és szakképesítő vizsgákkal kapcsolatos adatokat az érintett szakképző intézmények és az Agrár Vizsgaközpont kezeli. a) a tanuló, illetve a képzésben részt vevő személy, valamint érintett hozzájárulása
érintettek köre	képzésekbe felvett tanulók, vizsgázók
érintettekre vonatkozó adatok	a) a tanuló, illetve a képzésben részt vevő személy aa) természetes személyazonosító adatait, ab) nemét, ac) állampolgárságát, nem magyar állampolgár esetén a Magyarország területén való tartózkodás jogcímét és a tartózkodásra jogosító okirat megnevezését és számát, ad) lakcímét, levelezési címét, elektronikus levelezési címét és telefonszámát, ae) társadalombiztosítási azonosító jelét, af) adóazonosító jelét, b) a kiskorú tanuló törvényes képviselője ba) természetes személyazonosító adatait, bb) lakcímét, levelezési címét, elektronikus levelezési címét és telefonszámát, c) a tanulói jogviszonnyal kapcsolatos adatok keretében ca) a felvételi eljárással kapcsolatos adatokat, cb) a tanulói jogviszony szünetelésével, megszűnésével kapcsolatos adatokat, ideértve annak időpontját és okát, cc) a tanuló mulasztásával kapcsolatos adatokat, cd) a tanulóbalesetre vonatkozó adatokat,

	ce) a tanuló oktatási azonosító számát, cf) az egyéni tanulmányi renddel kapcsolatos adatokat, cg) a tanuló tudásának értékelésével és minősítésével, valamint a tanuló által tett vizsgákkal kapcsolatos adatokat, ch) az oktatás munkarendjével kapcsolatos adatokat, ci) a tanulói fegyelmi és kártérítési ügyekkel kapcsolatos adatokat, cj) a tanuló diákigazolványának sorszámát, ck) a tankönyvellátással kapcsolatos adatokat, cl) az évfolyamismétlésre vonatkozó adatokat, d) a felnőttképzési jogviszonnyal kapcsolatos adatok keretében a c) pont cb)–cf) és ci)–ck) alpontjában meghatározott adatokat, e) jogszabályban biztosított kedvezményekre való igényjogosultság elbírálásához és igazolásához szükséges olyan adatokat, amelyekből megállapítható a jogosult személye és a kedvezményre való jogosultsága. f) szakmai vizsgához kapcsolódó adatok
adatok forrása	tanulók, kiskorú törvényes képviselője, vizsgázók
adatkezelés időtartama	A szakképző intézmény a tanulói jogviszony megszűnésétől számított tizedik év utolsó napjáig, az adatkezelés céljának megvalósulásáig, a tanulói jogviszony megszűnéséig, a nyugdíjfolyósításról szóló jogszabályban meghatározott határideig A vizsgázók adatait az Agrár Vizsgaközpont dokumentum és iratkezelési szabályzatában leírtak szerint kezeljük.
adatok továbbítása	115. § [A kezelt adatok továbbítása] (1) A szakképző intézmény köteles a jogszabályban előírt nyilvántartásokat vezetni, a szakképzés információs rendszerébe bejelentkezni, a regisztrációs és tanulmányi alaprendszert használni, valamint az országos statisztikai adatfelvételi program keretében előírt és a korai iskolaelhagyással veszélyeztetett tanulókról összesített adatot szolgáltatni.
adatkezelés módja	elektronikus és papírhordozó

3. Elektronikus megfigyeléssel, vagyonvédelemmel kapcsolatos adatkezelés

Adatkezelési nyilvántartási azonosító	adatkezelésről szóló 2011. évi CXII. tv. 65. § (3) a) alapján a NAIH nem vezet nyilvántartást az adatkezelővel munkaviszonyban álló személyek adatinak kezeléséről
adatkezelés célja	elektronikus megfigyelés - vagyonvédelmi célú kamerafigyelés
adatkezelés jogalapja	2005. évi CXXIII. törvény 31. § (1)(2) bekezdése, az Szvtv 30 § (2) bekezdése, valamint az Szvtv 31 § (6) bekezdése felhatalmazása alapján
érintettek köre	A megfigyelt területen tartózkodó munkavállalók, vendégek
érintettekre vonatkozó adatok	érintett képmása
adatok forrása	közvetlenül az érintettől felvett
adatkezelés időtartama	Törvényben meghatározott határidő – főszabályként: a felvétel felhasználás hiányában a rögzítéstől számított 3, azaz három munkanap elteltével törlésre kerül
adatkezelés módja	kézi, elektronikus

5. A Járványügyi készültséget kezelő intézményi intézkedési terv alapján végzett ideiglenes adatkezelés

Adatkezelési nyilvántartási azonosító	
adatkezelés célja	a munkavállalók és munkatársaik egészségének védelme érdekében a szervezési feladatokhoz szükséges adatok nyilvántartása
adatkezelés jogalapja	a GDPR 6. cikk (1) bek f) pontja szerinti jogos érdek, ill. közfeladatot ellátó adatkezelései esetében a 6. cikk (1) bek. e) pontja, az alapfeladatok zavartalan ellátásának szükségessége. Az egészségügyi adatok kezelésének ezen esetében a GDPR 9. cikk (2) bek. b) pontja szerinti feltétel fennáll, mert a munkáltatónak munkajogi előírásokból fakadóan kötelezettsége a munkavállalók számára egészséges és biztonságos munkavégzési körülmények biztosítása.
érintettek köre	a fertőzés tüneteivel orvoshoz fordult munkavállalók
érintettekre vonatkozó adatok	bejelenés időpontja, érintett személyazonossága megállapításához szükséges személyes adatok, külföldi utazás (magáncélú is) helyszíne és időpontja, külföldről érkező személlyel történő érintkezés tényére vonatkozó adatok
adatok forrása	Kérdőív kitöltése alkalmazható, viszont a kérdőív nem tartalmaz egészségügyi kórtörténetre vonatkozó adatokat, nem kérjük dokumentum becsatolását sem
adatkezelés időtartama	A Járványügyi készültséget kezelő intézményi intézkedési terv szükségességének, a célhoz kötöttség fennállásáig.
adatkezelés módja	kézi, elektronikus

6. Eszközök használatának ellenőrzése során kezelt adatok:

Adatkezelési nyilvántartási azonosító	
adatkezelés célja	A Déli ASzC Széchenyi Zsigmond Mezőgazdasági Technikum, Szakképző Iskola és Kollégium tulajdonát képező elektronikus eszközök magán célú használatának kiszűrése, jogos érdek érvényesítéséhez szükséges adatok tárolása
adatkezelés jogalapja	Infotv. 5. § (1) a) szerinti érintetti hozzájárulásnak minősülnek.
érintettek köre	munkavállalók
érintettekre vonatkozó adatok	név, beosztás,
adatok forrása	technikai és szoftveres protokoll alkalmazása
adatkezelés időtartama	célhoz kötöttség fennállásáig, a jogosulatlan használat megszüntetéséig
adatkezelés módja	kézi, elektronikus