Jelen dokumentumot elfogadom és végrehajtását elrendelem: ……

Karsai József

Igazgató

VIDÉKFEJLESZTÉSI MINISZTÉRIUM

INTÉZMÉNYI INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Pálóczi Horváth István Mezőgazdasági Szakképző Iskola és Kollégium

Verzió: v1.00

Ügyiratszám:

Kiadványozó:

Dátum: 2014.04.03.

Dokumentum leíró adatok			
Szervezet neve:	**Pálóczi Horváth István Szakképző Iskola és Kollégium**		
Dokumentum címe:	**INFORMATIKAI BIZTONSÁGI SZABÁLYZAT**		
Ügyiratszám:			
Kiadványozó:			
Készítette:	**Pálóczi Szakképző Iskola ;** **Hegyi László**	**Dátum:**	**2014.04.03.**
Szakmailag jóváhagyta:	**Karsai József igazgató**	**Dátum:**	**2014.04.03.**
Adatvédelmi minősítés:	**3-as szintű biztonsági osztály**	**Verzió:**	**v1.00.**
A dokumentum leírása:	**A Pálóczi Szakképző Iskola minden szervezeti egységére érvényes informatikai biztonsági szabályok, ill.módszertani útmutatók**		
A dokumentum felülvizsgálatának szükségessége:	**1. Jogszabály változás, szervezeti változás**		
	2. Évente		
	3. Lényeges informatikai fejlesztés megvalósulás		
A dokumentum karbantartásáért felelős:	**Karsai József igazgató**		

A dokumentum változásai

Verzió:	Dátum:	Készítette:	Jóváhagyta:	A változások leírása:
v1.00	2014.04.03	Pálóczi Szakképző Iskola ; Hegyi László	Karsai József igazgató	Első, jóváhagyott változat

Tartalomjegyzék

2.A dokumentum célja, hatálya.....7
3.Az informatikai biztonsági szabályozáshoz kapcsolódó dokumentumok.....8
4.Kockázatkezelés.....10
5.IT biztonsági politika.....11
6.Az IT biztonság szervezete.....12
6.1.Feladatok, felelősségek, hatáskörök.....12
6.2.Belső szervezethez kapcsolódó további intézkedések.....12
6.3.Együttműködés külső szervezetekkel.....12
7.Vagyontárgyak kezelése.....14
7.1.Informatikai eszközök.....14
7.1.1.Adatvagyon.....14
7.1.2.Osztályba sorolás(3-as szintű biztonsági osztály).....14
8.Emberi erőforrások biztonsága.....16
9.Fizikai védelem.....17
10.A működés és kommunikáció védelme.....18
11.Hozzáférés kontroll.....19
11.1.Felhasználó hozzáférés kezelés és felügyelet.....19
11.2.Felhasználói felelősségek.....19
12.Információs rendszerek fejlesztése, karbantartása.....20
13.Incidensek kezelése.....21
14.Működésfolytonosság.....22
15.Megfelelőség.....23
15.1.Megfelelés a jogi követelményeknek.....23
15.2.Megfelelés a politikának, szabványoknak és műszaki megfelelés.....23
16.Melléklet.....24
16.1.Informatikai rendszerek védelmi igényei.....24
16.2.Releváns IT biztonsági szerepkörök – szervezeten belüli munkakörök összerendelése.....24
16.3.Fogalomtár.....24

Jelen dokumentum a Pálóczi Horváth István Szakképző Iskola és Kollégium(továbbiakban: Pálóczi Szakképző Iskola) magas szintű Informatikai Biztonsági Szabályzata (IBSZ), amely támaszkodik az ISO/IEC 27001:2005 nemzetközi szabvány követelményeire, felépítése a szabvány felépítését követi.

A szabályzat tartalmazza a Pálóczi Szakképző Iskola minden szervezetére érvényes informatikai biztonsági szabályokat és egyúttal módszertani útmutatót is jelent.

A Pálóczi Szakképző Iskola a Vidékfejlesztési Minisztériumi anyag figyelembe vételével, annak szerkezetét követve kellett elkészítenie saját szabályzatát. Ezek kialakításakor jelen anyagban szereplő tartalmi és formai elemeket kötelezően szerepeltetnie kellett, melyeket ki kellett egészíteni szervezetei sajátosságaiknak megfelelő szabályozási rendszerükkel. Kötelező formai elem az IBSZ kialakítása során a szerkezet, ez biztosítja, hogy az Ágazat valamennyi szervezetének IT biztonsági működését azonos felépítésű, a szabványnak megfelelő dokumentum szabályozza.

Amennyiben valamely szervezet esetén valamely fejezet nem releváns, saját szabályzatának kialakítása során az illető fejezet címét akkor is szerepeltetnie kell, a fejezetnek azonban ebben az esetben a „Nem releváns” kifejezést kell tartalmaznia.

2. A dokumentum célja, hatálya

Jelen szabályozás célja, hogy az ágazaton belül a szervezeti sajátosságok meghatározta korlátok között egységes megközelítéssel legyenek rögzítve az informatikai biztonsághoz kapcsolódó szabályozások.

AzIntézményi Informatikai Biztonsági Szabályzat vonatkozik a Pálóczi Szakképző Iskola valamennyi szervezeti egységére és rögzíti azokat az összetevőket, amelyeket részletesen ki kellett dolgozni.

Az Intézményi Informatikai Biztonsági Szabályzat az igazgató jóváhagyásával és aláírásával lép életbe és visszavonásig érvényben marad.

A dokumentum aktualitását, alkalmasságát, hatékonyságát minden nagyobb változáskor, de legalább évente a Pálóczi Szakképző Iskola igazgatója felülvizsgálja.

3. Az informatikai biztonsági szabályozáshoz kapcsolódó dokumentumok

Az ágazat egyes szervezeteinek Intézményi Informatikai Biztonsági Szabályzattal, és ehhez szorosan kapcsolódó szabályozási dokumentum rendszerrel kell rendelkezniük. Ennek megfelelően az Informatikai Biztonsági Szabályzat a következő dokumentumokra hivatkozik:

- Ágazati Szintű Informatikai Biztonsági Szabályzat
- Intézményi Informatikai Biztonsági Szabályzat
- Informatikai szabályozási térkép
- Kockázat kezelési útmutató
- Kockázatkezelési szabályzat
- Szervezeti és Működési Szabályzat
- Munkaköri leírások
- IT eszközgazdálkodási adatlap
- IT adatkörök adatlap
- IT üzemeltetési szabályzat
- IT változáskezelési szabályzat
- Felhasználói informatikai biztonsági útmutató
- Szerverszoba üzemeltetési szabályzat
- Tűzvédelmi szabályzat
- Mentési szabályzat
- Incidenskezelési szabályzat
- Hozzáférés-kezelési szabályzat
- Működésfolytonossági terv
- Beszerzési szabályzat
- Selejtezési szabályzat
- Iratkezelési szabályzat

Minisztériumi ajánlás:

Amennyiben valamely szervezet úgy ítéli meg, hogy esetében célszerűbb a fenti dokumentumok kialakítása helyett valamely kérdéskört közvetlenül az IBSZ-ben szerepeltetni, úgy ezt megteheti.

4. Kockázatkezelés

Az informatikai biztonsági kockázatok csökkentése érdekében az ágazat egyes szervezeteinek kockázatkezelési eljárásokat kell végrehajtania, amelynek ki kell terjednie a kockázatok felmérésére, értékelésére, valamint a kockázatokat csökkentő intézkedések meghatározására.

A kockázatkezelés módszertanára vonatkozóan az Ágazat részéről kötelező előírás nincs, azt az egyes szervezetek saját maguk választhatják meg.

5. IT biztonsági politika

A Pálóczi Szakképző Iskola működésnek szükséges feltétele, hogy a munkatársak számára folyamatosan és megbízhatóan, elfogadható szinten álljon rendelkezésre a munkájuk végzéséhez szükséges elegendő számú és megfelelő minőségű erőforrás mind hardver, mind jogtiszta szoftver, mind pedig kommunikációs lehetőség vonatkozásban. Szükséges feltétel továbbá, hogy ezen erőforrások feleljenek meg az adott időponthoz illeszkedő hardver és szoftver technológiai fejlettségi szintnek.

Annak érdekében, hogy a Pálóczi Szakképző Iskola közalkalmazottai zavartalanul és hatékonyan végezhessék tevékenységüket, a rendelkezésre álló informatikai erőforrások biztonságos működtetése, az erőforrások optimális kihasználhatóságának biztosítása elengedhetetlen. Szükséges, hogy az intézmény és az intézménnyel kapcsolatba kerülők érdekei maximálisan figyelembe legyenek véve és a releváns jogszabályok be legyenek tartva.

A Pálóczi Szakképző Iskola közalkalmazottai tevékenységük során hozzáférnek, létrehoznak, felhasználnak, kezelnek bizalmas adatokat, adatbázisokat. A Pálóczi Szakképző Iskola tevékenységét információs eszközök, adatbázisok, tudásbázisok támogatják, ill. teszik lehetővé. Ennélfogva a Pálóczi Szakképző Iskola közalkalmazottai számára kiemelt követelmény az információk és a kezelésükhöz szükséges eszközök biztonságának (bizalmasság, sértetlenség, rendelkezésre állás) folyamatos fenntartása, a szolgáltatások megbízható, működő infrastruktúrával támogatása.

A fentiek betartásához a Pálóczi Szakképző Iskola közalkalmazottainak következőket kell szem előtt tartaniuk:

- Azonosítják és betartják a kezelt információkra, információs eszközökre vonatkozó szervezeti, jogszabályi és az ügyfelek által megkövetelt előírásokat, a szükséges intézkedéseket beépítik dokumentációs rendszereikbe.
- Gondoskodnak a szolgáltatási tevékenységek támogatására, követésére, felügyeletéhez használt megbízható informatikai rendszerekről, szolgáltatásokról, folyamatos rendelkezésre állásukról, megfelelő működésükről, az igényekkel, változásokkal és a rendelkező erőforrásokkal összhangban fejlesztésükről.
- Biztosítják a biztonságos kommunikációs eszközöket a partnerekkel történő együttműködéshez.
- Időszakonként azonosítják, értékelik az információbiztonságot veszélyeztető kockázatokat, döntést hoznak az elfogadható és a kezelendő kockázatokról és a kezelendő kockázatok esetén a kockázatokkal arányban meghatározzák a kockázatok kezeléséhez szükséges kockázatjavítási intézkedéseket, kontrollokat. Csak olyan kockázatok tekinthetők elfogadhatónak, amelyek az információk és a kezelésükhöz szükséges eszközök biztonságának (bizalmasság, sértetlenség, rendelkezésre állás) folyamatos fenntartását nem veszélyeztetik.

- Biztosítják, hogy a munkatársak és minden érintett szerződéses partner megismerje a rá vonatkozó biztonsági előírásokat, ezek megtartásának fontosságát.
- Gondoskodnak az informatikai rendszer biztonságának fenntartásáról, az esetleges incidensek kezeléséről, a folyamatos működés megszakadása esetén ennek helyreállításáról.
- Követik a biztonság növelése érdekében tett intézkedések megvalósulását, eredményességét, a kockázatok változásait, szükség esetén további intézkedéseket tesznek a kockázatok csökkentésére.

Az Intézményi Informatikai Biztonsági Politika aktualitását, alkalmasságát, hatékonyságát minden nagyobb változáskor, de legalább kétévente a Pálóczi Szakképző Iskola informatikai biztonsági felelőse felülvizsgálja és az értékelést az igazgató elé terjeszti.

6. Az IT biztonság szervezete

Az informatikai biztonság megfelelő szintű biztosítása érdekében a szabályozásnak ki kell terjednie szervezeti kérdésekre, mind a szervezeten belüli, mind a külső ügyfelekkel fenntartott kapcsolatok kezelésére vonatkozóan.

6.1. Feladatok, felelősségek, hatáskörök

Annak érdekében, hogy a Pálóczi Szakképző Iskola közalkalmazottai és a munkavégzésre irányuló egyéb jogviszony alapján ott munkát végző munkatársak (például külső fejlesztők, támogatók) tisztában legyenek felelősségükkel, alkalmasak legyenek feladatkörük betöltésére, valamint a vétlen, vagy a rosszhiszemű tevékenységből, illetve az informatikai eszközökkel való bármilyen visszaélésből származó kockázatok csökkenjenek, a biztonsággal összefüggő feladat- és felelősségi köröket az IBSZ-szel összhangban kell meghatározni és dokumentálni.

A szervezeti munkaköröket, feladatokat, felelősségeket és hatásköröket alapvetően a Pálóczi Szakképző Iskola Szervezeti és Működési Szabályzata valamint az egyes munkatársak munkaköri leírásai határozzák meg. A Pálóczi Szakképző Iskola IT biztonsági rendszereinek kialakítása során részletesen szabályozni kell az IT biztonság tekintetében kitüntetett szerepkörökhöz tartozó feladatokat, felelősségeket és hatásköröket a Pálóczi Szakképző Iskola sajátosságainak megfelelően.

Az informatikai eszközök előírásszerű és biztonságos üzemeltetésének biztosítására, a Pálóczi Szakképző Iskola vagyontárgyainak jogosulatlan illetve nem szándékolt módosítása, valamint a visszaélés lehetőségének csökkentése érdekében a feladat- és a felelősségi köröket megfelelően szét kell választani.

Tipikusan a következő szerepköröket kell meghatározni:

- IT biztonságért felelős vezető
- Adatgazdák/vagyongazdák
- IT rendszer üzemeltetéséért felelős vezető
- Személyzeti vezető
- IT üzemeltető (rendszergazda)
- Munkatársak

A releváns IT biztonsági munkakörök és a szervezeten belüli munkakörök összerendelése a 16.2. c. pontban van megadva.

6.2. Belső szervezethez kapcsolódó további intézkedések

Titoktartási kötelezettség terhel minden, a Pálóczi Szakképző Iskola informatikai rendszereivel kapcsolatba kerülő természetes és jogi személyt, tekintet nélkül arra, hogy a kapcsolat milyen jogviszonyból ered. A titoktartási kötelezettség a szerződéses partnerek alvállalkozóira teljes körűen vonatkozik.

A titoktartási kötelezettség kiterjed a rendszerben kezelt adatokra, valamint a rendszer felépítésére, működési rendjére vonatkozó adatokra, a biztonsági rendszabályokra egyaránt. A titoktartási kötelezettség a időkorlát nélkül áll fenn és az érintett személy a mindenkor érvényes jogszabályok alapján tartozik ezen kötelezettségéért felelősséggel.

Minden munkatárs (beleértve az ideiglenes, ill. megbízási szerződés alapján munkát végző munkatársakat is) csak Titoktartási nyilatkozat aláírása után kezdheti meg az érdemi munkát, kaphat hozzáférést információkhoz, erőforrásokhoz.

A munkatársak informatikai biztonsághoz kapcsolódó felelősségi és hatásköreit a „Munkaköri leírások” tartalmazzák. Ezek kitérnek a hatóságokkal, felügyeleti és kormányzati szervekkel történő kapcsolattartásra, illetve a szakmai szervezetekkel, fórumokkal, szervezetekkel, személyekkel való kapcsolattartásra is.

6.3. Együttműködés külső szervezetekkel

Bármely informatikához kapcsolódó szolgáltatást nyújtó szolgáltató, ill. alvállalkozó valamint más együttműködő partnerrel való együttműködés megkezdése előtt a szerződést előkészítő munkatárs az informatikai biztonságért felelős vezető bevonásával megvizsgálja a felmerülő informatikai biztonsági kockázatokat, hozzáférési igényeket, és a szükséges kontrollokat beépíti a partnerrel kötött szerződésbe, kapcsolódó megállapodásba, Projekt Alapító Dokumentumba (PAD-ba). Szolgáltató, ill. alvállalkozó bevonása miatt fellépő új kockázat felmerülésekor a kockázatot az informatikai biztonságért felelős vezető a kockázat-felmérési eljárások során kezeli.

A külső partnerek képviselőivel az IBSZ-t a feladatnak megfelelő mértékben ismertetni kell. A betekintés mélységének meghatározása az IT üzemeltetésért felelős munkatárs felelőssége. A szerződéskötés és az együttműködés során biztosítani kell, hogy a külső partner (fejlesztő cég) az általa telepített, fejlesztett informatikai rendszert úgy konfigurálja, hogy annak minden eleme és egésze eleget tegyen az IBSZ-ben előírtaknak.

7. Vagyontárgyak kezelése

Az IT vagyontárgyak védelmének megfelelő szintű védelme érdekében nyilvántartásba kell venni és vagyongazdákhoz kell rendelni, továbbá osztályozni szükséges az összes materiális és immateriális vagyontárgyat. A Pálóczi Szakképző Iskola informatikai vagyonát folyamatosan frissülő listák tartalmazzák. Ezek kiindulásként szolgálnak a kockázatelemzéshez és a védelmi intézkedések meghatározásához.

A Pálóczi Szakképző Iskola adatvagyona informatikai rendszerekben van tárolva. Annak érdekében, hogy a különböző informatikai rendszerek sajátosságaiból adódó eltérő védelmi igények érvényre juthassanak, ugyanakkor a rendszerek nagy számából adódó összetett követelményrendszer egységesen kezelhető legyen, szükség van arra, hogy az informatikai rendszerek biztonsági osztályokba kerüljenek besorolásra.

Az egyes biztonsági osztályokba az egymással közel azonos védelmi igényű rendszerek kerülnek. A követelmények az egyes kategóriák eltérő védelmi igényei alapján, differenciáltan kerültek meghatározásra. Az egyes informatikai rendszereket annak alapján kell biztonsági osztályokba sorolni, hogy a hozzájuk kapcsolódó adatvagyon elemek milyen biztonsági osztályba tartoznak. Több biztonsági osztály esetén a legszigorúbbat kell alapul venni. Az IT üzemeltetést leíró dokumentációnak tartalmaznia kell, hogy az egyes rendszerek milyen biztonsági osztályba tartoznak és ennek megfelelően milyen követelményeket szükséges érvényesíteni rájuk. Az egyes biztonsági osztályokra vonatkozó követelményeket a melléklet tartalmazza.Ez a minimálisan szükséges követelményeket tartalmazza, ennek megfelelően az egyes konkrét rendszerek esetén további követelmények is felmerülhetnek

A már meglévő rendszerek cseréje, megújítása esetén meg kell vizsgálni, és szükség esetén az aktuális kockázatoknak megfelelően módosítani kell a besorolást. Új rendszerek bevezetésénél el kell végezni a rendszerek osztályokba való besorolását. Amennyiben a módosítások vagy az újonnan történő besorolások esetén megállapítást nyer, hogy a meglévő kategóriák már nem megfelelőek, új osztályozási rendszert kell felállítani, és végre kell hajtani valamennyi rendszer újbóli besorolását. Új kategória rendszert csak működési folyamatok új, aktuális kockázatelemzése alapján lehet felállítani.

A kategóriákba való besorolás, illetőleg maguknak a kategóriáknak a szükség esetén való módosítása tekintetében a szakmai felelősöknek és az információbiztonságért felelős vezetőnek együttesen kell javaslatot tenniük, amit az igazgató fogad el, ill. hagy jóvá.

7.1. Informatikai eszközök

A Pálóczi Szakképző Iskola informatikai eszközei a következő kategóriákba vannak besorolva.

- Alkalmazások.

- Szoftverek.
- Szerverek.
- Hálózati aktív elemek.
- Hálózatok.
- Felhasználói munkaállomások.
- Nyomtatók, szkennerek.
- Egyéb berendezések.

7.1.1. Adatvagyon

Az egyes adatkörök leginkább releváns jellemzőiként a következő biztonsági osztályok vannak rögzítve:

7.1.2. Osztályba sorolás (3-as szintű biztonsági osztály)

- Nyilvános adatok

  Azok az adatok, amelyek minél szélesebb körű megismerése az Ágazat érdeke (pl. a web oldalakra kikerülő tájékoztató anyagok). Ezekre az adatokra vonatkozóan nincsenek előírva bizalmassági követelmények és ennek megfelelően a bizalmasság tekintetében biztonsági osztályokba sincsenek besorolva.

- Biztonsági osztály

  Az elektronikus információs rendszer védelmének elvárt erőssége.

- Biztonsági osztályba sorolás

  A kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása.

- A rendszer teljes életciklusában biztosítani kell:

  Az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét. A szervezetünknek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják a megelőzést és a korai figyelmeztetést, az észlelést, a reagálást és a biztonsági események kezelését.

- Biztonsági szint

  A szervezet felkészültsége a törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

- Biztonsági szintbe sorolás

  A szervezet felkészültségének meghatározása a törvényben és végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére.

- 3-as szintű biztonság

  A központi államigazgatási szervekre vonatkozik (a Kormány és a kormánybizottságok kivételével). A Pálóczi Szakképző Iskola, mint a Vidékfejlesztési Minisztérium alá tartozó háttérintézmény ebbe a 3-as szintű biztonsági osztályba tartozik.

8. Emberi erőforrások biztonsága

Az emberi erőforrás rosszhiszemű és nem rosszhiszemű tevékenysége miatti károk megelőzése, ill. a károk hatásának minimalizálása érdekében védelmi intézkedéseket kell bevezetni a munkavégzés minden fázisában. Az emberi erőforrások védelme során figyelembe kell venni a hatályos jogszabályokat, szabályzatokat, eljárásrendeket.

Az alkalmazás informatikai biztonsági feltételeit a munkaszerződéseknek (vállalkozói együttműködés esetén az vállalkozói szerződés), és a munkaköri leírásoknak is tartalmazniuk kell. A munkatársak kiválasztási folyamatában az alkalmazási feltételek között szerepeltetni kell az informatikai biztonsági követelményeket is.

A Személyzeti vezető meghatározza, hogy mely munkakörök betöltéséhez szükséges nemzetbiztonsági átvilágítás. E munkakörökben a munkavégzés csak akkor kezdhető meg, ha a vizsgálat alapján a munkatárs az adott munkakör betöltésére alkalmasnak bizonyul.

A munkavégzés csak akkor kezdhető meg, ha a munkatárs megismerte a vonatkozó informatikai biztonsági szabályzatokat és erről írásban nyilatkozott. Törekedni kell arra, hogy a munkatársak informatikai biztonsági képzettsége és tudatossága folyamatosan fejlődjön. Az e területen megtett intézkedéseket dokumentálni kell.

A vezetőknek minden szinten feladata az informatikai biztonsági követelmények, eljárások működésének elvárása, betartatása és ellenőrzése. Az informatikai biztonsági követelmények megszegése esetén az alkalmazott fegyelmi eljárást és az alkalmazott szankciók részleteit rögzíteni kell.

Munkatársak munkaviszonyának megszűnése, változása esetén a munkatárssal a közvetlen vezető átadás-átvételi megállapodást köt, mely tartalmazza a felelősségek, feladatok, a munkatárs által kezelt információk átadását. A megállapodás rögzíti az átadás ütemtervét, a hozzáférések megszüntetését, az eszközök visszaadását, visszavételét, az esetleges átmeneti intézkedéseket. A hozzáférések megszüntetéséért a közvetlen vezető felelős.

9. Fizikai védelem

Az illetéktelen fizikai behatolás, károkozás, rongálás, a vagyontárgyak fizikai károsítása, eltulajdonítása és egyéb fizikai jellegű negatív események megelőzése, ill. hatásuk mértékének csökkentése érdekében védelmi intézkedéseket szükséges bevezetni. Ennek megfelelően rögzíteni kell a következő szabályokat:

- A telephelyek, épületek és helyiségek védelmére vonatkozó szabályok
- A berendezések védelmére vonatkozó szabályok

10. A működés és kommunikáció védelme

A biztonságos és megbízható üzemeltetés érdekében védelmi intézkedéseket szükséges bevezetni. Ennek megfelelően rögzíteni kell a következő szabályokat:

- A rendszerek üzemeltetésére vonatkozó szabályok
- Külső szolgáltatók nyújtotta szolgáltatások igénybe vételére vonatkozó szabályok
- Rendszerek tervezésre és bevezetésre vonatkozó szabályok
- A rosszindulatú szoftverek negatív hatásainak megelőzésére, ill. kezelésre vonatkozó szabályok
- A biztonsági mentésre vonatkozó szabályok
- A hálózati működésre vonatkozó szabályok
- Az adathordozók kezelésre vonatkozó szabályok
- Az biztonságos adattovábbításra vonatkozó szabályok
- Az e-kereskedelemre vonatkozó szabályok
- A naplózásokra vonatkozó szabályok

11. Hozzáférés kontroll

A Pálóczi Szakképző Iskola minden munkatársa számára biztosított az IT hálózathoz, az intranethez, az email rendszerhez, a felhasználói munkaállomásokra telepített standard konfiguráció szoftvereihez egyedi azonosítóval, jelszóval történő hozzáférés, ill. saját használatú munkaállomásán az adatok kezelése a munkavégzéshez szükséges mértékben. Olyan levelező rendszerek használata, amelyek kívül esnek a Pálóczi Szakképző Iskola üzemeltetésén, nem vagy korlátozottan megengedett.

A fentiektől különböző alkalmazásokhoz való hozzáférés a szervezetben elfoglalt munkakörnek megfelelően lehetséges.

Az internet használatot és az email rendszer használatát saját döntése alapján az IT bármikor korlátozhatja, megtilthatja, a forgalmat ellenőrizheti, fekete és fehér listákat alkalmazhat, tartalomszűrést végezhet.

A Pálóczi Szakképző Iskola informatikai rendszeréhez külső szervezetek, munkatársak VPN kapcsolaton keresztül történő hozzáférése alapvetően tiltott. Ugyancsak alapvetően tiltottak a WIFI rendszerek felhasználására épülő kapcsolatok. A tiltás alól különösen indokolt esetben eseti felmentést adhat az informatikai biztonságért felelős vezető. Az indoklást minden esetben írásban kell rögzíteni és engedélyezés esetén pontosan meg kell határozni a betartandó feltételeket (pl. elkülönült hálózat, VPA2 titkosítás stb.). Minősített adatok VPN-en keresztüli eléréséhez nem adható engedély.

Az IT üzemeltetés operatív feladatainak elvégzése, az alapbeállítások megtétele, telepítések elvégzése az IT üzemeltetők feladatai. Amennyiben lehetséges, a hozzáférés felügyeletet a központi címtárra épülően kell megvalósítani, funkcióhoz kapcsolódó csoportokra megadott hozzáférés beállítások segítségével.

11.1. Felhasználó hozzáférés kezelés és felügyelet

Minden munkatársnak egyedi azonosítóval és ehhez kapcsolódóan egyedi jelszóval kell rendelkeznie abban az esetben ha a munkavégzése jól behatárolható munkaállomásokon történik. A felhasználói azonosítókat, ill. jelszavakat munkába álláskor az adott szervezeti egység vezető dokumentált kérésére az IT üzemeltetés biztosítja. A szervezeti egység vezető kérésében megadja, hogy a munkába álló munkatárs mely csoportoknak lesz tagja. A munkatárs az IT üzemeltetéstől kapott azonosítókat kizárólag személyesen veheti át és a jelszavakat a munkatársnak az első belépés során meg kell változtatnia.

Csoportosan használt accountok tantermekben és az oktatással kacsolatos munkaállomásokon alkalmazhatók. Ezek év közben a tantermi és/vagy tantervi követelményeknek megfelelően szigoríthatóak.

Jelszónak kell tekinteni a biometriai azonosítást is, azonban ez esetben törekedni kell a biometriai azonosítás és a hagyományos jelszó együttes alkalmazására. A Szentannai Középiskolában jelenleg nem alkalmazunk biometriai azonosítást.

A felhasználói accountok alkalmazásával korlátozásra kerülnek az információk és erőforrások használata a felhasználó számára, úgy, hogy az munkaköri feladatainak ellátásához szükséges, de elégséges mértékű legyen, azaz minden egyes felhasználó hozzáférjen a munkavégzéshez szükséges minden adat- és programfájlhoz, de semmi olyan állományt ne érhessen el, amelyek nem szükségesek a feladatai maradéktalan ellátásához.

Az egyes adatkörökhöz hozzáférést csak az adatgazda dokumentált engedélyével lehet kiadni, a kiadott, érvényes hozzáféréseket az IT biztonságért felelős munkatárs kezdeményezésre évente ellenőrizni kell.

11.2. Felhasználói felelősségek

A felhasználó felelős a szervezet által kezelt (birtokolt) adatok és erőforrások védelméért, etikus módon történő használatáért, a biztonsági és egyéb belső szabályozások, utasítások betartásáért.A munkatársaknak az IT biztonság megvalósítása során a tipikusan a következő kötelezettségeik vannak:

- Az informatikai erőforrások rendeltetésszerű használata, megóvása.
- A jogszabályokban, és a belső szabályozásokban megjelenő informatikai biztonsági követelmények, előírások betartása.
- Az informatikai biztonsági eseményt azonnali jelentése közvetlen felettesének, annak eredménytelensége esetén közvetlenül az IT biztonságért felelős vezetőnek.

12. Információs rendszerek fejlesztése, karbantartása

A fejlesztésekre vonatkozó szerződéseknek, ill. a szerződésekhez tarozó műszaki specifikációknak, ill. a fejlesztési projektekhez tartozó PAD-oknak ki kell térniük az IT biztonsági követelményekre és azokra az átadás-átvételi feltételekre, amelyek alapján ezek ellenőrzésre kerülnek.

A fejlesztés tervezése során az IT biztonsági követelményeket a fejlesztésért felelős az IT biztonságért felelős vezetővel együttműködve azonosítja, és illeszti a specifikációba. meghatározzák, hogy a rendszer működése során milyen bemenő adat ellenőrzési, feldolgozás ellenőrzési, titkosítási, üzenet sértetlenség ellenőrzési, kimenő adat ellenőrzési követelmények fogalmazódnak meg, és a kapcsolódó követelményeket szintén beépítik a specifikációba. A specifikációt elfogadás előtt írásban véleményezi az IT biztonságért felelős vezető.

Minden fejlesztés esetén át kell venni és el kell tárolni a forráskódot és a fejlesztői környezetet.

A bevezetésre kerülő rendszereket bevezetés előtti tesztelni szükséges. A tesztelésnek ki kell térnie a bevezetés által érintett kapcsolódó rendszerek tesztelésére is. A tesztelések és a bevezetés során az IT üzemeltetésnek kell gondoskodnia arról, hogy éles rendszeren csak engedélyezett és felügyelt módosítás történhessen. Ugyancsak az IT üzemeltetésnek kell gondoskodnia arról, hogy a megfelelőség ellenőrzéséhez használt teszt adatokhoz, illetve a forráskódokhoz illetéktelen ne férjen hozzá.

Amennyiben külső fejlesztők működnek közre a fejlesztésben, a fejlesztéshez kijelölt projektvezető feladata az információ kiszivárgás kockázatának csökkentése és a fejlesztőkkel együttműködés során a biztonsági követelmények betartása, betartatása. E célból együtt kell működnie az IT biztonságért felelős vezetővel.

Annak érdekében, hogy az informatikai rendszereknek a biztonság szerves részét képezze, a biztonsági követelményeket már az életciklus tervezési, fejlesztési, beszerzési szakaszában figyelembe kell venni. Az üzemeltetés és karbantartás során az információbiztonsági követelményeket folyamatosan fenn kell tartani.

13. Incidensek kezelése

Minden munkatárs feladata, hogy az információbiztonsági incidenseket, észlelt gyengeségeket jelentse közvetlen felettesének, eredménytelenség esetén az igazgatási osztály vezetőjének.

Az értesített feladata a szükséges intézkedések meghozatala, a teljes elhárítási folyamat dokumentálása. Amennyiben az incidens gyengíti az informatikai biztonsági rendszert, értesítik az IT biztonságért felelős vezetőt.

Az incidensekről készült feljegyzéseket az IT biztonságért felelős vezető rendszeresen áttekinti, szükség esetén további helyesbítő, megelőző intézkedésekre tesz javaslatot.

Az informatikai biztonsági események és gyengeségek követése szabályozott kezelése érdekében a következő szabályokat kell rögzíteni:

- Az informatikai biztonsági eseménynek és gyengeségek bejelentésének és eszkalációjának szabályai
- Az informatikai biztonsági eseménynek és gyengeségek kezelésére vonatkozó szabályok

14. Működésfolytonosság

A Működésfolytonossági tervben rögzíteni szükséges azokat a kontrollokat, amelyek a működési folyamatok kiesésmentes menetét biztosítják. A követelményeknek tartalmaznia kell az informatikai rendszerek, eszközök rendelkezésre állási követelményeit. Azonosítani kell azokat az intézkedéseket, amelyek elősegítik a kiesésmentes működést, továbbá azokat, amelyek az esetleges kiesések esetén alkalmazhatók.

Kockázatelemzésre épülően működésfolytonossági tervet kell készíteni a működésfolytonosság megszakadásának megelőzésére, elkerülésére, illetve az informatikai katasztrófa helyzetek kezelésre, a folytonosság helyreállítására.

A terveket rendszeresen karban kell tartani, ill. tesztelni szükséges. A felülvizsgálatoknak az IT biztonsági felelős kezdeményezésre legalább évente (ill. nagyobb változások esetén a változást követően) meg kell történnie.

A kritikus működési folyamatok megszakadásának megelőzése, továbbá az esetleges kiesések kezelése érdekében a következőket kell rögzíteni:

- A kritikus működési folyamatok és maximális megengedett kieséseik
- A megszakadások megelőzésre vonatkozó preventív jellegű szabályok
- Reaktív jellegű informatikai katasztrófa tervek

15. Megfelelőség

15.1. Megfelelés a jogi követelményeknek

Folyamatosan követni kell az IT biztonság tekintetében releváns jogszabályokat és a szervezet által kötött szerződések IT biztonságot érintő összetevőit. Az informatikai biztonságot meghatározó belső szabályozást a releváns jogszabályok változása esetén aktualizálni szükséges.

Az informatikai biztonságot érintő jogszabályok változásának követése az IT biztonságért felelős vezető feladata. A jogszabályok megváltozása esetén az IT biztonságért felelős vezető feladata, hogy szükség esetén javaslatot tegyen intézkedésekre, folyamatok, eljárások módosítására. Amennyiben szerződés keretében keletkezik új, informatikai biztonságra vonatkozó követelmény, a projektvezető feladata a követelmény jelzése az IT biztonságért felelős vezetőnek.

A szoftverek jogtisztaságának betartása érdekében a szoftverek használatához szükséges licence-ekről nyilvántartást kell vezetni. A licence nyilvántartás kérdése hozzákapcsolódik más IT eszközök nyilvántartásához. A licence-ek nyilvántartása az IT üzemeltetés, a nyilvántartás értékelése az IT biztonságért felelős vezető feladata. Amennyiben licence-igény következik be, az IT biztonságért felelős vezető tesz javaslatot a probléma feloldására.

Az Információs önrendelkezési jogról és az információszabadságról szóló törvénynek való megfelelés érdekében el kell készíteni és folyamatosan naprakészen kell tartani a törvény által előírt adatvédelmi nyilvántartásokat. A nyilvántartások elkészítése és karbantartása az adatvédelmi felelős felelőssége. A nyilvántartás elkészítéséhez az Adatgazdáknak információt kell nyújtaniuk.

15.2. Megfelelés a politikának, szabványoknak és műszaki megfelelés

A folyamatos vezetői, IT biztonsági felelősi ellenőrzések mellett a megfelelőségeket belső felülvizsgálatok, ill. külső, független felülvizsgálatok lefolytatásával időszakonként vizsgálni szükséges. A felülvizsgálatoknak az IT biztonságért felelős vezető kezdeményezésre legalább évente (ill. nagyobb változások esetén a változást követően) meg kell történnie.

A vizsgálatok során feltárt eltérésekre a kockázatokkal arányos helyesbítő és megelőző intézkedéseket kell végrehajtani. Az intézkedések kezdeményezése az IT biztonságért felelős vezető tesz javaslatot.

Amennyiben a vizsgálatokhoz szoftvereket, teszt adatbázisokat kell használni, úgy ezeket hozzáférési szempontból elkülönítetten kell kezelni. Az éles rendszereket, meg kell védeni az illegális betekintés, módosítás ellen. A vizsgálatokat úgy kell tervezni, hogy biztosított legyen a kellő mélység, de a vizsgálat a bizalmassági, sértetlenségi, rendelkezésre állási követelményeket ne sértse.

A jogi, törvényi vagy szerződéses kötelezettségek betartása érdekében a következőket kell rögzíteni:

- A releváns jogszabályok követésének szabályai
- A rendelkezésre álló licence-ek
- Adatvédelmi nyilvántartások
- Auditálási szabályok

16. Melléklet

16.1. Informatikai rendszerek védelmi igényei

Biztonsági osztály	A biztonsági osztályra vonatkozó minimális védelmi igények
3-as szintű biztonsági osztály	• A 3-as szintű biztonsági osztályba tartozó anyagok logikai hozzáférését jelszavakon és hozzáférési jogosultságokon alapuló védelmi rendszerrel kell biztosítani. • A jelszavak használatára vonatkozó fő szabályok a következők: o Legalább 8 karakterből kell állnia. o Legalább 1 számot, 1 nagybetűt és nem értelmes karakter sorozatot kell tartalmaznia. o Jelszavak helyett biometriai azonosítás használható. • Naplózni kell a következőket: o Sikeres bejelentkezések. o Sikeres alkalmazás és rendszerindítások ill. leállítások. • A 3-as szintű biztonsági osztályba tartozó adatok képernyőkön történő megjelenítése csak felügyelet esetén lehetséges (üres képernyő policy). • A 3-as szintűbiztonsági osztályba tartozó papíralapú anyagok nyomtatott példányai csak munkaidőben, felügyelet mellett lehetnek elzáratlanok (üres íróasztal policy), munkaidőn kívül elzárva kell őket tartani. Amennyiben nem feltétlenül szükséges, kerüljük az anyagok kinyomtatását. • A 3-as szintűbiztonsági osztályba tartozó adatokat tartalmazó adathordozókat, ill. ezek papír alapú változatait selejtezni kizárólag fizikai megsemmisítés útján lehetséges. • A 3-as szintű biztonsági osztályba tartozó adatokat tartalmazó meghibásodott számítógép szervízbe történő szállítása előtt belőle az adathordozót el kell távolítani. • Adatátvitelre valamint mentésre, archiválásra használt adathordozók tárolása csak megbízhatóan zárt helyen történhet. • Biztosítani kell az adathordozók és dokumentációk tűz- és vagyonvédett tárolását. • Figyelembe kell venni a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információ-szabadságról törvény előírásait • A rendszer megbízhatóságát jó minőségű és megfelelő számú referenciával rendelkező hardver és szoftver termékek beszerzésével kell biztosítani. • A szerverek és a hálózati aktív elemek számára olyan szünetmentes villamos energia ellátást kell biztosítani, amely képes legalább 30 percnyi villamos energia kiesés áthidalására.

Biztonsági osztály	A biztonsági osztályra vonatkozó minimális védelmi igények
	• A szervereket és a hálózati aktív elemeket, valamint a kábelrendezőket, továbbá a dokumentációt zárható helyiségekben kell elhelyezni. • A szervereket és a hálózati aktív elemeket hideg tartalékolással kell ellátni. • Hibatűrő diszk alrendszereket és tápegységeket kell alkalmazni. • Adatbázisokról (beleértve a biztonsági napló állományokat is) heti teljes és napi inkrementális mentést kell végezni külön adattárolóra. Biztosítani kell, hogy a külső adattárolók ciklikus csere esetén legalább 1 hétig ne kerüljenek felülírásra. • A rendszerek üzemeltetésének támogatására 24 órán belüli hibaelhárításra vonatkozó support szükséges.

16.2. Releváns IT biztonsági szerepkörök – szervezeten belüli munkakörök összerendelése

IT biztonsági szerepkör	Szervezeten belüli munkakör
IT biztonságért felelős vezető	Pálóczi Szakképző Iskola
Adatgazdák/vagyongazdák	igazgató
IT rendszer üzemeltetéséért felelős vezető	igazgató

16.3. Fogalomtár

Adat

Az információ absztrakt, egyezményes jelrendszerben rögzített reprezentációja. Tények, elképzelések, utasítások emberi vagy technikai eszközökkel történő formalizált ábrázolása ismertetés, feldolgozás, ill. távközlés céljára.

Adatállomány

Valamely informatikai rendszerben lévő adatok logikai összefogása, amelyet egy névvel jelölnek.

Adatátvitel

Adatok szállítása összeköttetéseken, összekötő utakon (például számítógépek között).

Adatbázis

Informatikai szemléletű megközelítés esetén használatos: strukturált adatok összessége, amelyet egy tárolására, lekérdezésére és szerkesztésére alkalmas szoftvereszköz kezel.

Adatbiztonság

Az adatok jogosulatlan megszerzése, módosítása és tönkretétele elleni műszaki és szervezési intézkedések és eljárások együttes rendszere.

Adatfeldolgozás

Az adatok gyűjtése, rendszerezése, törlése, archiválása.

Adatkör

A szervezeti működést szem előtt tartó megközelítés fogalma: az azonos működési területekhez tartozó adatok összességét jelenti.

Adatgazda

Az a szervezeti pozíció, aki rendelkezik az adott adatkörhöz történő hozzáférésekről.

Adathordozó

Adatok tárolására alkalmas eszköz (diszk, pen drive, memóriát tartalmazó kisméretű eszköz, mikrofilm, papír stb.)

Adatvagyon

A külső szervezetek számára szolgáltatott, ill. a szervezet saját belső működéshez szükséges releváns adatok összessége, függetlenül attól, hogy az milyen adathordozón, ill. milyen jelleggel (adatbázis, fájl, papír) áll rendelkezésre.

Adatvédelem

Az adatok kezelésével kapcsolatos törvényi szintű jogi szabályozás formája, amely az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó adatkezelés során érintett személyek jogi védelmére és a kezelés során felmerülő eljárások jogszerűségeire vonatkozik.

Biztonság

Kedvező állapot, amelynek a megváltozása nem kizárt, de kis valószínűségű.

Bizalmasság

Az a tulajdonság, amely arra vonatkozik, hogy az adatot csak az arra jogosultak ismerhessék meg, illetve rendelkezhessenek a felhasználásáról.

Fenyegetettség

Olyan állapot, amelyben az erőforrások bizalmassága, sértetlensége, rendelkezésre állása sérülhet.

Háttérintézmény:

A vidékfejlesztési miniszter irányítása alá tartozó központi költségvetési szervek, továbbá a vagyonkezelésébe, vagy tulajdonosi joggyakorlása alá tartozó gazdasági társaságok.

Hoax

Leggyakrabban emailben terjedő álhírek, megtévesztő lánclevelek elnevezése.

Információ

Az információ a világ egy megragadott aspektusának visszatükröződése, mentális reprezentációja az emberi tudatban.

Informatika

A tudomány és technika azon területe, amely az információk keletkezésének, kezelésének és felhasználásának elméletével, gyakorlati megvalósításával és eszközrendszerével foglalkozik.

Informatikai biztonság

Olyan állapot, amikor a cég vagy intézmény informatikai erőforrásai bizalmassága, sértetlensége, hitelessége és rendelkezésre állásának a fenyegetettsége minimális, azaz igen kicsi a kedvező állapot megváltozásának valószínűsége.

Informatikai szolgáltatás

Információtechnológián alapuló rendszerek által működtetett kapcsolódó funkciók rendszere, amely egy vagy több szervezeti tevékenységet támogat. Bár számos hardver, szoftver, telekommunikációs elem alkotja, a felhasználó számára koherens és önálló entitásként érzékelhető.

Informatikai (IT) infrastruktúra

A szervezet, a számítógépek, a hálózat, a hardver elemek, a szoftver elemek, illetve a szoftverrel kapcsolatos telekommunikáció, melyeken az alkalmazói rendszerek és az egyes informatikai szolgáltatások ráépülnek és futnak.

ISO27001

Az információbiztonságra vonatkozó nemzetközi szabvány.

IP cím

Az internetre csatlakoztatott gépek egyedi azonosításra szolgáló logikai szintű cím.

ITIL

IT InfrastructureLibrary – Az IT rendszerek tágabb értelemben vett üzemeltetésére vonatkozó nemzetközi ajánlásgyűjtemény.

Kockázat

Annak esélye, hogy egy esemény vagy intézkedés előre nem látható módon befolyásolja egy szervezet lehetőségeit céljainak és stratégiáinak megvalósítása során.

Közérdekből nyilvános adat

"a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli" (2011. évi CXII. törvény)

Közérdekű adat

„az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat" (2011. évi CXII. törvény)

Megengedő lista

Klasszikus spamszűrési módszer (whitelist), amellyel biztosítható, hogy a legitim levelek véletlenül se kerüljenek a spamek közé.

Nemzeti adatvagyon

"a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége" (2010. évi CLVII. törvény)

Okostelefon

Operációs rendszert tartalmazó, összetett funkciókat biztosító mobil telefonkészülék.

PIN kód

Personal Identification Number, személyes azonosító kód.

Rendelkezésre állás

Olyan állapot, amelyben a rendszer az eredeti rendeltetésének megfelelő szolgáltatásokat nyújtani tudja elvárt performanciával, meghatározott helyen és időben.

ServiceDesk

Az a szervezeti egység, amely felé a felhasználók jelezhetik az informatikai rendszer használata során fellépő problémáikat és amely ezek elhárításában támogatást, segítséget nyújt.

Sértetlenség

Az a tulajdonság, amely arra vonatkozik, hogy az adat az eredeti állapotnak megfelel, fizikailag és logikailag teljes és bizonyítottan vagy bizonyíthatóan az elvárt forrásból származik.

SPAM

Kéretlen reklámlevelek, melyek küldése a legtöbb esetben törvénybe ütköző tevékenység.

Szakrendszer

Jogszabály által szabályozott, a VM, illetve egy vagy több háttérintézmény szakmai munkáját támogató egyedi fejlesztésű alkalmazás, adatbázis, illetve egyéb szoftver.

Személyes adat

"az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés" (2011. évi CXII. törvény)

Torrent

Tartalmak felhasználók egymás közötti cseréjére létrehozott elosztott rendszer. Sok esetben jogvédett tartalmak illegális megosztására alkalmazott szolgáltatás.

Tűzfal

A szervezet hálózatának határfelületén elhelyezett berendezések és szabályok összessége, amelyek segítségével a külső és belső hálózat közötti forgalom naplózásra és korlátozásra kerül.

Veszélyforrás

Olyan tényező, amelynek hatására, ill. bekövetkezésekor az IT rendszerben nem kívánt állapot jön létre, az IT rendszer biztonsága sérül.

Vírus

Szándékosan károkozás céljából készített kód, amely a felhasználó szándéka ellenére települ fel a számítógépre és annak hibás működését okozza

VPN

Virtual Private Network. Olyan magánhálózat, amely az internet felhasználásával, de azon keresztül titkosított csatornán valósul meg.

Warez oldal

A szerzői jogvédett tartalmak jogsértő kereskedelme céljából létrehozott tartalomszolgáltatás.

Védelmi intézkedés

Olyan tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, folyamatosan szinten tartsa és fejlessze azt informatikai biztonságot.

WiFi

Wireless Fidelity. Vezeték nélküli lokális hálózat.