СЛУЖБЕНИ ЛИСТ

ОПШТИНЕ БАЧКА ТОПОЛА

TOPOLYA KÖZSÉG

HIVATALOS LAPJA

Број 11 – Година LI
14. август 2019. г. , Бачка Топола

LI. évfolyam–11. Szám
Topolya, 2019. augusztus 14.

109.

Az információbiztonságról szóló törvény 8. szakaszának 1. bekezdése (Az SZK Hivatalos Lapja, 16/6. és 2017/97. szám), a különös jelentőség információs és kommunikációs rendszer biztonságáról szóló aktus részletes tartalmáról, a különös jelentőségű információs és kommunikációs rendszer ellenőrzésének módjáról és a különös jelentőségű információs és kommunikációs rendszer ellenőrzéséről szóló jelentés tartalmáról szóló rendelet 2. szakasza (Az SZK Hivatalos Közlönye, 2016/94. szám) és a Topolya Községi Közigazgatási Hivataláról szóló határozat 45. szakasza (Topolya Község Hivatalos Lapja, 2016/19. szám) alapján, Topolya Községi Közigazgatási Hivatalának vezetője 2019. 07. 26-án meghozza az alábbi

SZABÁLYZATOT
TOPOLYA KÖZSÉG INFORMÁCIÓS ÉS KOMMUNIKÁCIÓS RENDSZERÉNEK BIZTONSÁGÁRÓL

I. Általános rendelkezések

1. szakasz

E szabályzat, az információbiztonságról szóló törvénnyel és a különös jelentőség információs és kommunikációs rendszer biztonságáról szóló aktus részletes tartalmáról, a különös jelentőségű információs és kommunikációs rendszer ellenőrzésének módjáról és a különös jelentőségű információs és kommunikációs rendszer ellenőrzéséről szóló jelentés tartalmáról szóló rendelettel összhangban, megállapítja az információs és kommunikációs rendszer (a továbbiakban: IKT-rendszer) megfelelő biztonsági szintje eléréséhez és fenntartásához szükséges védelmi intézkedéseket, elveket, módot és eljárásokat, valamint a Topolya község (a továbbiakban: Üzemeltető) IKT-rendszerének biztonságával és erőforrásaival kapcsolatok felhatalmazásokat és felelősségeket.

2. szakasz

Az Üzemeltető információs javai közé tartozik minden olyan erőforrás, amely az Üzemeltető üzleti adatait tartalmazza, vagyis az összes olyan erőforrás, amelyen keresztül az adatok létrehozása, feldolgozása, tárolása, továbbítása, törlése és megsemmisítése történik az IKT-rendszerben, beleértve az összes elektronikus feljegyzést, számítógépes berendezést, mobil eszközöket, adatbázisokat, üzleti alkalmazásokat és hasonlókat.

Az információs javakról nyilvántartást vezetnek külön űrlapon, amely jelen aktus szerves része.

A jelen szakasz 2. bekezdésében foglalt nyilvántartást az alkalmazott vezeti, a hatályos munkaköri besorolással összhangban (a továbbiakban: az IKT-rendszer illetékes alanya).

3. szakasz

Az IKT-rendszer biztonságának területéhez tartozó teendők az alábbiak:

- az információs javak, illetve az információbiztonság szempontjából fontos üzleti folyamatok felügyeletére szolgáló eszközök és vagyon védelme,
- kockázatkezelési teendők az információbiztonság terén, valamint az információbiztonsági eljárásokkal előirányzott teendők
- az Üzemeltető IKT-rendszere eszközeinek, illetve információs javainak jogosulatlan vagy nem szándékos módosításának, megkárosításának vagy az azokkal való visszaélésnek, valamint az eszközökhöz való jogosulatlan és nyilvántartás nélküli hozzáférés, azok módosításának vagy használatának az ellehetetlenítésére, vagyis megakadályozására irányuló teendők.
- az információbiztonság kezelése keretében történő tevékenységek, felülvizsgálatok és felügyeletek nyomon követése.
- az illetékes szervek tájékoztatása az IKT-rendszerben történt incidensekről, az előírásokkal összhangban.

II. Az IKT-rendszer használata

4. szakasz

Az IKT-rendszert az IKT-rendszer illetékes alanya kezeli.

Az IKT-rendszer illetékes alanya köteles minden új alkalmazottnak – IKT-erőforrás-felhasználónak elmagyarázni az Üzemeltető IKT-erőforrásának használatára vonatkozó felelősségeket és szabályokat, felkészíteni az IKT-rendszer erőforrásainak használatára, hogy a képzés végén az alkalmazott nyilatkozatot adjon az IKT-erőforrások használatára való felkészítéséről, s minderről nyilvántartást vezet.

5. szakasz

A felhasználó – az IKT-rendszer illetékes alanya munkahelyének, illetve illetékességének megváltozása esetén változtatást eszközölnek az IKT-rendszer használati jogát illetően, amelyet a felhasználó – alkalmazott élvezett a munkaköri leírásával összhangban.

6. szakasz

A felhasználó – alkalmazott foglalkoztatásának megszűnése esetén a felhasználói fiókot törlik.

Az IKT-erőforrások felhasználója, akinek bármilyen alapon megszűnt a foglalkoztatása az Üzemeltetőnél, nem fedheti fel az IKT-rendszer információbiztonsága szempontjából jelentős adatokat.

Rendszergazdai és felhasználói fiók

7. szakasz

Az IKT-rendszerhez csak azok a dolgozók, illetve felhasználók férhetnek hozzá, akiknek rendszergazdai és felhasználói fiókjuk van.

A rendszergazdai fiók egyedüli fiók, amely lehetővé teszi az IKT-rendszer valamennyi erőforrásához való hozzáférést és azon adminisztrálását, csak egy felhasználói fiókkal, valamint új fiókok nyitása és a meglévők módosítása, csak az az alkalmazott használhatja, akit a rendszergazdai teendők és munkakör ellátására osztottak be.

A felhasználói fiók olyan felhasználónevet és jelszót tartalmazó fiók, amelyet be lehet gépelni vagy leolvasni egy olyan adathordozóról, amelyen van elektronikus tanúsítvány, amely alapján az azonosítás – a személyazonosság ellenőrzése és engedélyezés – az alkalmazottnak – felhasználónak az IKT-rendszer erőforrásaihoz való hozzáférési jogának vagy használati jogának ellenőrzése.

A felhasználói fiókot az adminisztrátor jelöli ki az emberi erőforrás menedzsmentért felelős alkalmazott kérése alapján, és csak azután, hogy a munkavállaló adatait bevitte az emberi erőforrás menedzsmentjére szolgáló szoftverbe. Az alkalmazott teendői és munkaköre alapján az adminisztrátor meghatározza a hozzáférési jogokat, az alkalmazott – felhasználó munkavégzési szükségleteivel összhangban.

A rendszergazda nyilvántartást vezet a felhasználói fiókokról, ellenőrzi azok használatát, megváltoztatja a hozzáférési jogokat és megszünteti a felhasználói fiókokat az emberi erőforrás menedzsmenttel foglalkozó alkalmazott, illetve az Üzemeltető szervezeti egységeiben dolgozó illetékes vezető kérelme alapján.

A felhasználó felelőssége saját azonosítási eszközök védelméért

8. szakasz

A felhasználói fiók felhasználónévből és jelszóból áll.

A felhasználónevet mátrix alapján hozzák létre, az utónév első betűje és a vezetéknév, helyköz nélkül, latin betű írásmóddal, a ђ, ж ,љ, њ, ћ, ч, џ, ш cirill betűk használata nélkül. Ezek helyett a betűk helyett az alábbi táblázatban szereplő betűket kell használni:

Cirill betűk	Latin betűk
ђ	dj
ж	z
љ	lj
њ	nj
ћ, ч, ш	c
џ	Dz

A jelszónak legalább nyolc karaktert kell tartalmaznia, keverve kis- és nagybetűket, számokat és speciális jeleket.

A jelszó nem tartalmazhat keresztnevet, vezetéknevet, születési dátumot, telefonszámot és egyéb felismerhető adatokat.

Ha az alkalmazott – felhasználó gyanítja, hogy egy másik személy felfedte a jelszavát, köteles azonnal tájékoztatni az IKT-rendszer adminisztrátorát, aki megteszi a megfelelő intézkedéseket.

Az IKT-rendszer adminisztrátora az alkalmazottal – felhasználóval együttműködve megváltoztatja a jelszavat félévente legalább egyszer.

Ugyanazt a jelszavat nem szabad megismételni egy éven belül.

III. Az IKT-rendszer védelmének tárgya, intézkedései és alanyai

9. szakasz

Az IKT-rendszer védelmének tárgyát az alábbiak képezik:

- az IKT-rendszer hardver és szoftver komponensei
- az IKT-rendszer komponensein feldolgozott és tárolt adatok
- felhasználói fiókok és egyéb adatok az IKT-rendszer informatikai erőforrásának felhasználóiról

10. szakasz

A jelen aktusban előírt intézkedések az Üzemeltető IKT-rendszerének minden szervezeti egységére, minden alkalmazottra – az informatikai erőforrások felhasználóira, valamint harmadik személyekre, akik használják az Üzemeltető informatikai rendszerét.

11. szakasz

Az Üzemeltető IKT-rendszerére vonatkozó védelmi intézkedések biztosítják az incidensek megelőzését, illetve a hatáskör és tevékenységek, különösen a harmadik személyeknek történő szolgáltatásnyújtás keretében történő ellátását veszélyeztető incidensek által okozott károk megelőzését és minimalizálását.

Az adatok titkosságának, valódiságának és integritásának védelme érdekében az Üzemeltető megfontolhatja a megfelelői kriptográfiai védelmi intézkedések használatát.

12. szakasz

Az Üzemeltető IKT-rendszerére vonatkozó biztonsági teendők ellátására a Községi Közigazgatási Hivatal Általános Közigazgatási és Társadalmi Tevékenységügyi Osztályának Informatikai Csoportja illetékes.

Az alkalmazottak kötelezettségei

13. szakasz

Az Üzemeltetőnél alkalmazott személy köteles tiszteletben tartani az IKT-rendszer erőforrásainak biztonságos és megfelelő használatára vonatkozó alábbi szabályokat is:

1) az informatikai erőforrásokat kizárólag a munka céljából használja;
2) elfogadja, hogy az informatikai erőforrások keretében tárolt, átvitt vagy feldolgozott adatok az Üzemeltető tulajdonát képezik, s felügyelet és felülvizsgálat tárgyát képezhetik;
3) az előírásokkal összhangban jár el a bizalmas adatokkal, különösen az adatok másolása és átvitele alkalmával;
4) biztonságosan tárolja jelszavát más személyekkel szemben;
5) a munkaállomástól történő minden eltávolodás előtt kijelentkezik a rendszerből, illetve kikapcsolja a munkaállomást;
6) a munkaállomáson csak az IKT-rendszer illetékes alanyának jóváhagyásával használ DVDRW, CDRW és USB külső memóriákat;
7) a szoftver és hardver telepítésére vonatkozó kérelmet írásban nyújtja be, a közvetlen vezető jóváhagyásával;
8) a hatályos előírásokkal összhangban biztosítja az adatbiztonságot;
9) kifejezetten az illetékes alany által adott felhasználói jogok alapján fér hozzá az informatikai erőforrásokhoz;
10) nem állíthatja le az antivírus program munkáját vagy törölheti azt, nem változtathatja meg beállításait, se nem telepíthet jogosulatlanul másik antivírus programot;
11) a munkaállomáson nem tárolhat olyan tartalmat, amely nem üzleti célokat szolgál;
12) az előírt eljárásokkal összhangban elkészíti az adatok védelmi másolatát (backup);
13) az előírt eljárásokkal összhangban használja az Üzemeltető intranet és internet e-mail szolgáltatását;
14) elfogadja, hogy bizonyos informatikai beavatkozásokat meghatározott időben végez;
15) elfogadja, hogy az informatikai erőforrásokhoz és az információkhoz való minden hozzáférésnek a minimális szükségesség elvén kell alapulnia;
16) elfogadja az IKT-rendszer biztonsága céljából a technikák és programok telepítését;
17) nem szabad védelmi, rendszer vagy applikatív szoftvert telepíteni, változtatni, üzemen kívül helyezni vagy törölni.

Az adatokhoz és az adatfeldolgozó eszközökhöz való hozzáférés korlátozása

14. szakasz

Az IKT-rendszer erőforrásaihoz való hozzáférést az alkalmazott megbízása határozza meg.

A rendszergazdai fiókkal rendelkező alkalmazott az IKT-rendszer minden erőforrásához (szoftver és hardver, hálózat és hálózati erőforrások) hozzáférési joggal rendelkezik az IKT-rendszer erőforrásainak telepítése, karbantartása, beállítása és kezelése céljából.

Az alkalmazott csak a rendszergazdától kapott felhasználói fiókját használhatja, s nem szabad lehetővé tennie másik személy számára a felhasználói fiókjához való hozzáférést, kivéve a rendszergazda számára a felhasználói profil és a munkaállomás beállításához.

Az az alkalmazott, aki bármilyen módon visszaél jogával, illetve az IKT-rendszer erőforrásaival, büntető és fegyelmi felelősségre vonható.

III a Egyéni védelmi intézkedések

Azoknak a létesítményeknek, helyeknek és helyiségeknek, illetve övezeteknek a fizikai védelme, amelyekben az IKT-rendszer eszközei és dokumentumai vannak, és az IKT-rendszer adatait feldolgozzák

15. szakasz

Az a helyiséget, amelyben az adatbázisok vezetésére szolgáló számítógép és a központi számítógép (szerver), az IKT-rendszer hálózati vagy kommunikációs felszerelése található, rendszergazdai övezetként szervezik meg.

A rendszergazdai övezetet az IKT-rendszer erőforrásaihoz való fizikai hozzáférés érdekében hozzák létre egy ellenőrzött, jól láthatóan megjelölt helyiségben, amelyet mechanikus zárral és videó felügyelettel biztosítanak. Az IKT-rendszer illetékes alanya vezeti a nyilvántartást az ezen övezetbe történő belépésekről.

16. szakasz

Csak az IKT-rendszer adminisztrátorának engedélyezett az IKT-felszerelést tároló helyiségbe való belépés.

A rendszergazdán kívül a rendszergazdai övezethez harmadik személy is hozzáférhet az IKT-rendszer meghatározott erőforrásainak telepítése és szervizelése céljából, a Községi Közigazgatási Hivatal vezetőjének előzetes jóváhagyásával.

A jelen szakasz 1. bekezdésében foglalt helyiséget látható jelzéssel kell ellátni, s tűzvédelmi felszerelésnek kell lennie benne, amely csak tűz esetén használható a helyiségben, amelyben az IKT-felszerelés és az adattároló médiumok vannak.

A jelen szakasz 1. bekezdésében foglalt helyiség ablaka és ajtaja mindig zárva kell, hogy legyen.

A szerverek és az aktív hálózati eszközök (switch, modem, router, firewall) állandóan rá kell, hogy legyenek kapcsolva a szünetmentes tápegységre – UPS.

Az UPS kapacitásánál hosszabb idejű áramkimaradás esetén a felhatalmazott személy köteles kikapcsolni a felszerelést a felszerelés gyártójának eljárásával összhangban.

Abban az esetben, ha a felszerelést a jelen szakasz 1. bekezdésében foglalt helyiségből költözés vagy javítás céljából kiviszik, elengedhetetlen a Községi Közigazgatási Hivatal vezetőjének jóváhagyása, aki meghatározza a felszerelés kivitelének feltételeit, módját és helyét.

Ha a felszerelést javítás céljából viszik ki, a Községi Közigazgatási Hivatal vezetőjének jóváhagyása mellett jegyzőkönyvet is készíteni kell, amelyben feltüntetik a felszerelés elnevezését és típusát, sorozatszámát, a szerviz elnevezését, a szerviz felhatalmazott személyének vezeték- és keresztnevét.

A szervizzel kötött szerződésben kötelezően meg kell határozni az Üzemeltető IKT-erőforrásának részét képező médiumokon tárolt adatok védelmére vonatkozó kötelezettséget.

A távmunka biztonsága és a mobil eszközök használata

17. szakasz

A regisztrálatlan felhasználók számára az operátor IKT-rendszerének erőforrásaihoz való hozzáférés mobil eszközökön keresztül csak a weboldalon biztosított.

Az alkalmazottak, az IKT-rendszer erőforrásainak felhasználói az Üzemeltető tulajdonában lévő mobil eszközökön keresztül, amelyeket az IKT-rendszer illetékes alanya állított be, az IKT-rendszernek csak azokhoz a részeihez férhetnek hozzá, amelyek lehetővé teszik számukra a hatáskörükben tartozó munkafeladatok ellátását, ilyen az elektronikus posta, a teendők ellátásával kapcsolatos egyes alkalmazások, mindezt pedig a Községi Közigazgatási Hivatal vezetőjének írásos jóváhagyásával.

A mobil eszközöket úgy kell beállítani, hogy biztos és biztonságos hozzáférést tegyenek lehetővé, az IKT-rendszer VPN-hálózatának és azon eszköz MAC-címlistájának használatával, amelyen keresztül a hozzáférés engedélyezett, a megfelelő aktív vírusvédelmi és egyéb, rosszindulatú szoftverektől védő szoftver használatával.

Az alkalmazottnak tilos önállónak szoftver telepítenie és beállítania a mobil készüléket, valamint átadnia a készüléket jogosulatlan személynek.

Az IKT-rendszer illetékes személye napi szinten ellenőrzi az IKT-rendszer erőforrásaihoz való hozzáférést, s ellenőrzi, hogy ismeretlen készülékről, illetve ismeretlen MAC-címről történik-e hozzáférés.

Ha jogosulatlan hozzáférést állapítanak meg, erről elektronikus posta útján azonnal, de legkésőbb másnap értesítik a Községi Közigazgatási Hivatal vezetőjét, a MAC-címet pedig beviszik a hozzáférés ellenőrző szoftver blokklistájába.

18. szakasz

Az IKT-rendszer erőforrásaihoz nem megengedett a hozzáférés magán mobil eszközről, kivéve, ha az Üzemeltető tulajdonában lévő készülék meghibásodott, s nem biztosított a csere.

A magán készülék használatát a jelen szakasz 1. bekezdésében foglalt esetben a Községi Közigazgatási Hivatal vezetője hagyja jóvá.

Az IKT-rendszer illetékes alanya nyilvántartást vezet azokról a magán készülékekről, amelyekről lehetővé teszik a hozzáférést.

19. szakasz

Az IKT-rendszer illetékes alanyának kell beállítania azokat a magán eszközöket, amelyeket keresztül hozzáférnek az IKT-rendszer erőforrásaihoz.

Az IKT-rendszer erőforrásaihoz hozzáférést biztosító magán eszközök csak a felhasználó – alkalmazott illetékességébe tartozó teendők elvégzésére használhatók, s csak addig, amíg nincs lehetőség az Üzemeltető tulajdonában álló készülék használatára.

Az IKT-rendszer illetékes alanya köteles a készülék felhatalmazott szerviznek történő átadását megelőzően backupot készíteni a mobil eszközökön lévő adatokról, azután pedig letörölni az eszközről, a szervizelés elvégzését követően pedig visszatenni az adatokat a mobil eszközre.

Az adathordozó védelme

20. szakasz

Az IKT-rendszerben lévő adatok titkosak, a közérdekű információkhoz való szabad hozzáférésről szóló törvény, a személyes adatvédelemről szóló törvény, az adatok titkosságáról szóló törvény, valamint az adatok, illetve dokumentumok titkosításának módjáról és eljárásáról szóló rendelet rendelkezéseivel összhangban.

A titkosként megjelölt adatokat védeni kell az információs és telekommunikációs rendszerekben lévő titkos adatok külön védelmi intézkedéseiről szóló rendelet rendelkezéseivel összhangban.

21. szakasz

Az IKT-rendszer illetékes alanya megszervezi az adatokhoz való hozzáférést, különösen azokhoz, amelyeket titkosítanak, az adatok titkosságáról szóló törvénnyel összhangban, mégpedig úgy, hogy a titkosított dokumentumok másolhatók, illetve archiválhatók vagy bevihetők a fájlszerveren abba a folderbe, amelyhez csak az erre jogosult alkalmazottak – felhasználók férhetnek hozzá.

A titkosított dokumentumok csak a Községi Közigazgatási Hivatal vezetője vagy az ő írásos aktusa által felhatalmazott dolgozók – felhasználók által másolhatók egyéb adathordozókra (külső merevlemez, USB, CD, DVD).

Az IKT-rendszer illetékes alanya nyilvántartást vezet azokról az adathordozókról, amelyekre titkos adatokat vettek.

A titkos dokumentumokat tartalmazó adathordozókat az előírás szerint kell megjelölni és tárolni olyan helyen, ahol védettek lesznek a jogosulatlan hozzáféréstől.

A titkos adatokat tartalmazó adathordozó szállítása esetén a Községi Közigazgatási Hivatal vezetője kijelöli az illetékes személyt és a szállítás módját.

A titkos adatok adathordozóról történő letörlése alkalmával az adatokat véglegesen törölni kell, ha viszont ez nem lehetséges, az ilyen adathordozókat meg kell károsítani, vagyis meg kell semmisíteni.

Az adatfeldolgozó eszközök kifogástalan és biztonságos működésének biztosítása

22. szakasz

A szoftvernek az IKT-rendszer munkájába történő bevonását megelőző fejlesztésére és tesztelésére tesztelésre és fejlesztésre szánt szervereket kell használni. Tilos olyan szerver használata, amelyet operatív munkában szoftvertesztelésre használnak.

Mielőbb az új szoftver munkába állítják, elengedhetetlen elkészíteni a meglévő adatok másolatát – archívumát.

Az új szoftver telepítését, valamint a meglévő frissítését, illetve új verzió telepítését a munkaidő letelte után kell végezni, hogy ne álljon le az alkalmazottak – felhasználók operatív munkája.

Az adatok és az adatfeldolgozó eszközök rosszindulatú szoftverekkel szembeni védelme

23. szakasz

A rosszindulatú szoftverekkel szembeni hálózati védelmet a vírusok és egyéb rosszindulatú kódok elleni védelem céljából végzik, amelyek internetkapcsolat, e-mail, fertőzött adathordozók (USB, CD, stb.), engedély nélküli szoftver telepítése által kerülhetnek a számítógépes hálózatba.

A sikeres vírusvédelem érdekében minden számítógépre antivírus programot telepítenek.

Mindennap automatikusan, pontosan meghatározott időben bővülnek az antivírus definíciók.

Minden hét utolsó munkanapján az elzárt számítógépeket is bekapcsolva kell hagyni víruskeresés céljából.

Internethasználat közbeni védelem

24. szakasz

Az Üzemeltető IKT-rendszerébe történő internetes behatolások elleni védelem céljából az IKT-rendszer illetékes alanya köteles karbantartani a rendszert a behatolások megakadályozására. A védelmi mód – Mikrotik Router, amely magában foglalja valamennyi védelmi módot az azonosítatlan és nem megengedett behatolások megakadályozása érdekében.

Az Üzemeltető szervezeti egységeinek vezetői határozzák meg, hogy mely alkalmazottak jogosultak internet-hozzáférésre a hatáskörükbe tartozó teendők ellátásával kapcsolatos adatok és egyéb információk begyűjtése céljából.

Azok a tisztségviselők és alkalmazottak, akiknek engedélyezett az internet- és e-mail-használat, kötelesek annak használata során a nemzetközi konvencióknak és magatartási szabályoknak megfelelően viselkedni.

Az IKT-rendszerre rákapcsolt felhasználóknak tilos önállóan kapcsolódniuk az internethez, illetve tilos saját modemen keresztül kapcsolódni.

Az IKT-rendszer illetékes személye bizonyított visszaélések esetén megszakíthatja az internet-hozzáférést.

Az IKT-rendszer felhasználói, akiknek internet-hozzáférést hagytak jóvá, kötelesek betartani a vírusvédelmi és az IKT-rendszerbe történő internetes behatolások elleni védelmi intézkedéseket, s minden számítógépet, amelyről az alkalmazott – felhasználó kapcsolódik az internethez, megfelelően kell beállítani és védeni, s a beállítást az IKT-rendszer illetékes alanya végzi.

Az internethasználat alkalmával az IKT-rendszer felhasználója, akinek jóváhagyták az internethasználatot, köteles elkerülni a gyanús weboldalakat, mégpedig az IKT-rendszernek kárt okozó programok telepítésének megakadályozása céljából.

Amennyiben a felhasználó a felhasználó számítógépe szokatlanul viselkedik, ezt köteles haladék nélkül jelenteni az IKT-rendszer illetékes alanyának.

25. szakasz

Az IKT-rendszer felhasználójának, akinek megengedett az internethasználat, tilos filmeket néznie és játékokat játszania a számítógépek, valamint tilos pornográf és egyéb illetlen tartalmakat tartalmazó weboldalakat keresnie, valamint önkényesen letölteni ezeket az internetről.

26. szakasz

Az engedély nélküli internethasználat magában foglalja:

- olyan kalóz- van egyéb szoftvertermékek telepítése, terjesztése, hirdetése, átvitele vagy más módon elérhetővé tétele, amelyek nincsenek engedélyezve a megfelelő módon;
- a hálózati biztonság megzavarása, vagy az üzleti internetes kommunikáció más módon való ellehetetlenítése;
- destruktív és obstruktív programok szándékos terjesztése az interneten (internetes vírusok, internetes trójai faló, internetes féreg és egyéb nem megengedett szoftverek);
- a közösségi oldalak és egyéb olyan internetes tartalmak engedély nélküli használata, amelyet az Üzemeltető illetékes szervének határozata korlátoz;
- olyan mennyiségű adat letöltése, amely nagy megterhelést okoz a hálózatnak;
- szerzői jogvédelem alatt álló anyagok letöltése;
- a munkával nem kapcsolatos linkek használata;
- nem engedélyezett tartalom-hozzáférés, tartalommódosítás, törlés vagy tartalomfeldolgozás az interneten keresztül.

Az adatok elvesztése elleni védelem

27. szakasz

Az adatbázist kötelezően archiválják adathordozóra (DVD, szalagos meghajtó, külső hardver), legalább egyszer naponta, hetente, havonta és évente, az adatbázis megújításának szükségleteire.

A többi fájlt – dokumentumot hetente, havonta és évente legalább egyszer archiválják.

Az alkalmazottak – felhasználók adatait legalább havonta egyszer archiválják.

28. szakasz

A napi másolást – archiválást a hét minden munkanapa esetében végzik, 20 órától minden munkanapon.

A heti másolást – archiválást a hét utolsó munkanapján végzik, 20 órától, annyi heti példányban, ahány utolsó munkanap van a hónapban.

A havi másolást – archiválást a hónap utolsó munkanapján végzik, minden hónapra külön, 20 órától.

Az éves másolást – archiválást az év utolsó munkanapján végzik.

29. szakasz

Az éves másolat – archívum minden példányát az államigazgatási szervek irodai ügymenetéről szóló utasításban definiált ideig őrzik.

A másolatot – archívumot tartalmazó adathordozó minden példányán fel kell tüntetni a számot, a fajtát (napi, heti, havi, éves), a másolat – archívum készítésének dátumát, valamint a másolást – archiválását végző alkalmazott – felhasználó nevét.

A napi, heti és havi másolatokat – archívumokat olyan helyiségben őrzik, amely fizikailag és a tűzvédelmi intézkedésekkel összhangban biztosított.

Az éves másolatokból – archívumokból két példány készül, az egyiket abban a helyiségben őrzik, ahol a napi, heti és havi másolatokat – archívumokat is, a másik példányt pedig egy külön objektumban.

Az éves másolat – archívum második példányának őrzésére szolgáló külön objektumról szóló határozatot a Községi Közigazgatási Hivatal vezetője hozza meg külön végzéssel.

30. szakasz

A másolat – archívum kifogástalanságát legalább hathavonta ellenőrizni kell az adathordozón található adatbázisok helyreállításával, amit követően az adatoknak kifogástalanoknak és használatra késznek kell lenniük.

Az IKT-rendszer biztonsága szempontjából jelentősként kezelhető események adatainak megőrzése

31. szakasz

A rendszergazda és az alkalmazottak – felhasználók tevékenységeiről tevékenységnaplót – *transaction log* vezetnek.

Minden hét utolsó munkanapján a tevékenységnaplót tartalmazó fájlt archiválják, az egyéb adatok és az IKT-rendszer másolatának-archívumának készítésére vonatkozó eljárásnak megfelelően, e szabályzat 27. szakaszával összhangban.

Ellenőrző rendszer

32. szakasz

Az IKT-rendszerben a hibák, illetéktelen tevékenységek és egyéb lehetséges problémák ellenőrző és jelentési rendszerét úgy kell beállítani, hogy haladéktalanul értesítse a rendszergazdát, az IKT-ügyekért felelős szervezeti egység vezetőjét és a Községi Közigazgatási Hivatal vezetőjét az alkalmazottak – felhasználók szabálytalan tevékenységeiről, a rendszerbe behatolási kísérletekről és behatolásokról.

A szoftver és az operációs rendszerek integritásának biztosítása

33. szakasz

Csak olyan szoftverek telepíthetők az IKT-rendszerben, amelyek esetében az Üzemeltető érvényes engedéllyel rendelkezik, azaz Freeware és Open source verziók.

A szoftver telepítését és beállítását csak az IKT-rendszer illetékes alanya, azaz a felhatalmazott rendszergazda végezheti.

A szoftver telepítését és beállítását harmadik személy is elvégezheti, ha a szoftvert a közbeszerzési szerződésben meghatározott módon, a közbeszerzési eljárás keretében szerezték be.

Harmadik személy akkor végezheti el a szoftver telepítését és beállítását, ha az Üzemeltetővel megállapodott a szoftver meghatározott időintervallumban történő fenntartásáról.

34. szakasz

A szoftver új verziójának minden egyes telepítése, illetve beállítása előtt el kell készíteni a meglévő másolatát, annak biztosítása érdekében, hogy váratlan helyzetekben visszaállíthassák az előző állapotot.

Védelem az IKT-rendszer biztonsági hiányosságainak visszaéléseivel szemben

35. szakasz

Az IKT-rendszer illetékes alanya legalább havi egyszer, szükség esetén pedig gyakrabban elvégzi a tevékenységnapló – *transaction log* elemzését, az IKT-rendszer potenciális hiányosságainak azonosítása érdekében.

Amennyiben olyan hiányosságokat azonosítanak, amelyek veszélyeztethetik az IKT-rendszer biztonságát, az IKT-rendszer illetékes alanya köteles azonnal elvégezni a beállítást, illetve olyan szoftvert telepíteni, amely elhárítja a tapasztalt hiányosságokat.

Az IKT-rendszer illetékes alanya köteles a felhasználói irányelvek beállításával megakadályozni az olyan szoftverek illetéktelen telepítését, amelyek veszélyeztethetik az IKT-rendszer biztonságát.

Az IKT-rendszer felülvizsgálata

36. szakasz

Az IKT-rendszer felülvizsgálatát úgy kell elvégezni, hogy ne zavarja a felhasználók – alkalmazottak munkafolyamatait.

Az IKT-rendszer illetékes alanya jelöli ki a felülvizsgálat idejét, az Üzemeltető alkalmazottai – felhasználói teendőnek fajtájától és munkafeladataitól függően.

Az IKT-rendszer felszerelésének védelme

37. szakasz

A kommunikációs kábeleket és a tápkábeleket be kell szerelni a falba vagy a csövekbe, hogy megakadályozzák az illetéktelen hozzáférést, illetve szigeteljék.

A hálózati felszerelést (switch, router, firewall) rack szekrényben kell tárolni, bezárva.

Az IKT-rendszer illetékes alanya köteles állandóan ellenőrizni a hálózati felszerelést, s idejében foganatosítani az esetleges szabálytalanságok elhárításához szükséges intézkedéseket.

A vezeték nélküli hálózatnak, amelyet a hivatal illetékességében tartozó létesítmények látogatói használhatnak, el kell különülnie a hivatal alkalmazottai – felhasználói által használt belső hálózattól, amelyen keresztül a hivatalos információcsere történik.

Ezt a hálózatot modell alapján kell megjelölni (SSID).

Az IKT-rendszer biztonsága adatcsere esetén

38. szakasz

A titkosított adatok más szervekkel, szervezetekkel vagy jogi személyekkel történő cseréjét az adatcseréről szóló, aláírt aktussal összhangban kell végrehajtani.

Az jelen szakasz 1. bekezdésében említett aktusnak tartalmaznia kell az adatcserére felhatalmazott személyek adatait, az adatcsere módját, az ilyen típusú adatcsere jogi keretét, valamint a csere tárgyát képező adatok védelmét meghatározó jogi keretet.

Az IKT-rendszer, illetve a rendszer részeinek teszteléséhez használt adatok védelme

39. szakasz

Az IKT-rendszerek tesztelésekor a titkosított, illetve szolgalmi jellel ellátott adatokért az IKT-rendszer illetékes alanya felel, a bizalmas adatok felhasználását és védelmét meghatározó előírásokkal összhangban.

Harmadik személy részvétele az IKT-rendszer teendőiben

40. szakasz

Az Üzemeltetőnél alkalmazásban nem álló harmadik személyek által az IKT-rendszer új erőforrásainak telepítését, a meglévők cseréjét és karbantartását a megkötött szerződés szabályozza.

Az IKT-rendszer illetékes alanya köteles elvégezni a műszaki ellenőrzés a szerződésben foglalt kötelezettségek harmadik személyek általi megvalósítása felett.

41. szakasz

Harmadik személyek – szoftverfejlesztési és karbantartási szolgáltatások nyújtói csak az általuk létrehozott szoftver részét képező adatbázisokban található adatokhoz férhetnek hozzá, azaz azokhoz, amelyekhez szerződésben meghatározott hozzáférés létezik.

Az IKT-rendszer illetékes alanya felelős a hozzáférés ellenőrzéséért és a szerződéses kötelezettségek végrehajtása feletti felügyeletért, valamint az ilyen tevékenységeket meghatározó jelen szabályzat rendelkezéseinek betartásáért.

42. szakasz

Az IKT-rendszer illetékes alanya felelős a szerződésben foglalt kötelezettségek harmadik személyek – szolgáltatásnyújtók általi tiszteletben tartásának felügyeletéért, különösen az IKT-rendszer erőforrásainak biztonságát definiáló rendelkezések tiszteletben tartása terén.

A szerződéses kötelezettségek be nem tartása esetén az IKT-rendszer illetékes alanya köteles haladéktalanul értesíteni a közigazgatás vezetőjét a szabálytalanságok megszüntetésére irányuló intézkedések foganatosítása érdekében.

Megelőző intézkedések és a biztonsági incidensekre való reagálás

43. szakasz

Bármilyen esemény esetén, amely veszélyeztetheti az IKT-rendszer erőforrásainak biztonságát, az alkalmazott – felhasználó köteles haladéktalanul értesíteni az IKT-rendszer illetékes alanyát.

A jelen szakasz 1. bekezdésében foglalt bejelentés vételekor az IKT-rendszer illetékes alanya köteles haladéktalanul értesíteni a közigazgatás vezetőjét és intézkedéseket foganatosítani az IKT-rendszer erőforrásainak védelme érdekében.

44. szakasz

Az adatok megküldéséről, az események listáiról, fajtáiról és jelentőségéről, valamint a különös jelentőségű információs és kommunikációs rendszerekben történő események bejelentésére vonatkozó eljárásról szóló rendelet által meghatározott incidens esetén az illetékes IKT-rendszer illetékes alanya köteles a Községi Közigazgatási Hivatal vezetőjén kívül tájékoztatni a fent említett rendeletben meghatározott illetékes szervet.

Az IKT-rendszer illetékes alanya nyilvántartást vezet minden incidensről, valamint az incidensek bejelentéséről, a rendelettel összhangban, amely alapján a felelős személy ellen fegyelmi, szabálysértési vagy büntetőeljárás folytatható.

IV. A meglévő IKT-rendszer módosítása és új telepítése

45. szakasz

Az új IKT-rendszer létrehozásáról, illetve új részek bevezetéséről és az IKT-rendszer meglévő részeinek módosításáról az IKT-rendszer illetékes alanya vezeti a dokumentációt.

A jelen szakasz 1. bekezdésében foglalt dokumentációnak tartalmaznia kell minden eljárás leírását, különösen az IKT-rendszer biztonságára vonatkozó eljárásokat.

V. Intézkedések a munka folytonosságának rendkívüli körülmények közötti biztosítására

46. szakasz

Olyan rendkívüli körülmények esetén, amelyek az IKT-rendszer áthelyezését eredményezhetik az adminisztrációs épületből, az IKT-rendszer illetékes alanya köteles az IKT-rendszer rendkívüli helyzetekben történő működéshez szükséges részeit a lehető leghamarabb áthelyezni a tartalék helyre, a rendkívüli és válsághelyzeti reagálási tervvel összhangban.

Az IKT-rendszer azon részeinek meghatározását, amelyek szükségesek a rendkívüli helyzetekben történő működéshez, az IKT-rendszer illetékes alanya készíti el, három példányban, amelyek közül egy marad nála, a másik a védelmi és a rendkívüli helyzeti teendőkért felelős alkalmazottnál, a harmadik pedig a Községi Közigazgatási Hivatal vezetőjénél.

Az IKT-rendszer rendkívüli helyzetekben történő működéshez szükséges részeit a tartalék helyszínen tárolják, amelyet a Községi Közigazgatási Hivatal vezetője határoz meg.

Az IKT-rendszer nélkülözhető részeinek tárolását oly módon végzik, hogy a felszerelés biztonságos és megjelölt legyen, a róla vezetett nyilvántartással összhangban.

VI. Az IKT-rendszer ellenőrzése

47. szakasz

Az IKT-rendszer ellenőrzését az IKT-rendszer illetékes alanya végzi.

48. szakasz

Szükség esetén az IKT-rendszer ellenőrzését a közbeszerzési törvény rendelkezéseivel összhangban kiválasztott alany végzi el.

Az ellenőrzést az év utolsó hónapjában végzik.

49. szakasz

Az IKT-rendszer ellenőrzését az alábbi módon végzik:

1) ellenőrzik az IKT-rendszer biztonságáról szóló szabályzatnak az előírt feltételekkel való összehangoltságát, figyelembe véve azt a jogi aktust is, amelyre utalják, azaz ellenőrzi, hogy a szabályzat megfelelően rendelkezik-e az IKT-rendszerben alkalmazott védelmi intézkedésekről, eljárásokról, meghatalmazásokról és felelősségekről;

2) ellenőrizik, hogy az előirányzott védelmi intézkedéseket és eljárásokat megfelelően alkalmazzák-e az operatív munkában, a megállapított hatáskörökkel és felelősségekkel, meghallgatási módszerekkel, szimulációkkal, megfigyelésekkel, az előirányzott nyilvántartásokba és más dokumentumokba való betekintéssel összhangban;

3) ellenőrzik a biztonsági hiányosságokat az IKT-rendszer alkotóelemeinek műszaki jellemzői szintjén, mégpedig a kiválasztott termékekbe, megoldás-architektúrákba, műszaki konfigurációkba, a státusokról szóló műszaki adatokba, eseménynaplókba (naplókba) való betekintés módszerével, valamint az ismert biztonsági hiányosságok meglétének tesztelésével hasonló környezetekben.

Az elvégzett ellenőrzésről jegyzőkönyvet készítenek, amelyek kézbesítenek a Községi Közigazgatási Hivatal vezetőjének.

50. szakasz

A jelen szabályzat 45. szakaszában jelentés az alábbiakat tartalmazza:
1) az Üzemeltető elnevezése;
2) az ellenőrzés ideje;
3) az ellenőrzés végző személyek adatai;
4) jelentés a végrehajtott ellenőrzési tevékenységekről;
5) következtetések az IKT-rendszer biztonságáról szóló aktusnak az előírt feltételekkel való összehangoltságáról;
6) következtetések az előirányzott védelmi intézkedések operatív munkával való megfelelő alkalmazása kérdésében;
7) következtetések az IKT-rendszer alkotóelemei műszaki jellemzőinek szintjén észlelt esetleges biztonsági hiányosságok kérdésében;
8) az információbiztonság teljes szintjének értékelése;
9) az esetleges korrekciós intézkedések javaslata;
10) az IKT-rendszer ellenőrzését végzett felelős személy aláírása.

VII. Fegyelmi felelősség

51. szakasz

A jelen szabályzat rendelkezéseinek be nem tartása a munkaköri kötelezettségek megsértését jelenti, és fegyelmi felelősséget von maga után az Üzemeltető informatikai erőforrásainak alkalmazottja - felhasználója számára.

52. szakasz

Az Üzemeltető IKT-erőforrásainak alkalmazott - felhasználó általi - a ráruházott hatáskörön kívüli - felhasználása esetén az alkalmazott fegyelmi felelőssége, amely meghatározza a vagyon jogosulatlan használatáért való felelősséget.

53. szakasz

A hálózathoz való hozzáférést megtagadhatják azoktól a felhasználóktól, akik az internet nem megfelelő használatával hálózati torlódást okoznak, megszakítják a munkát vagy rontják a hálózat biztonságát.

VIII. A szabályzat módosítása

54. szakasz

Az IKT-rendszer műszaki-technológiai, személyzeti, szervezeti változásai, valamint az információbiztonságot rontható globális és nemzeti szintű események miatt bekövetkező változások esetén az IKT-rendszer illetékes szerve köteles tájékoztatni a Községi Közigazgatási Hivatal vezetőjét, hogy megkezdhesse a jelen szabályzat módosítását, az IKT-rendszer megfelelő biztonsági szintjének elérése és fenntartása érdekében tett biztonsági intézkedések, módszerek és eljárások javítása céljából, valamint az IKT-rendszer biztonságával és erőforrásaival kapcsolatos meghatalmazások és felelősségek felülvizsgálata céljából.

IX. Átmeneti és záró rendelkezések

55. szakasz

E szabályzat a Községi Közigazgatási Hivatal hirdetőtábláján való közzététele napján lép hatályba, s megjelenik Topolya Község Hivatalos Lapjában.

Szerb Köztársaság
Vajdaság Autonóm Tartomány
Topolya Községi Közigazgatási Hivatala
Szám: 09-5/2019-V
Kelt: 2019. 07. 26-án

Szedlár Péter okl. jogász, s.k.
a Községi Közigazgatási Hivatal vezetője

110.
SZERB KÖZTÁRSASÁG
VAJDASÁG AUTONÓM TARTOMÁNY
TOPOLYA KÖZSÉG
KÖZSÉGI KÖZIGAZGATÁSI HIVATAL
Szám: 02-53/2019
Kelt: 2019. 08. 09-én
Topolya

Az oktatási és nevelési rendszer alapjairól szóló törvény 77. szakaszának 3. bekezdése (A Szerb Köztársaság Hivatalos Közlönye, 2017/88., 2018/27. – másik törvény és 2019/10. szám), a gyerekek, diákok és felnőttek kiegészítő oktatási, egészségügyi és szociális támogatásáról szóló szabályzat 5. szakaszának 1. bekezdése (A Szerb Köztársaság Hivatalos Közlönye, 2018/80. szám) és Topolya Községi Közigazgatási Hivataláról szóló határozat 45. szakasza (Topolya Község Hivatalos Lapja, 2016/19. szám) alapján Topolya Községi Közigazgatási Hivatala meghozza az alábbi

VÉGZÉST

A TÁRCAKÖZI BIZOTTSÁG MEGALAKÍTÁSÁRÓL

I.

Ezennel megalakítjuk a Tárcaközi Bizottságot a gyermekek, diákok és felnőttek kiegészítő oktatási, egészségügyi és szociális támogatás iránti szükségletének felbecslésére, Topolya község területére vonatkozóan (a továbbiakban: bizottság), négyéves megbízatási időszakra.

A bizottságnak négy állandó és egy alkalmi tagja van. A bizottság elnökét a bizottság állandó tagjai választják meg maguk közül.

A bizottság alkalmi tagját a bizottság elnöke jelöli ki.

A bizottság állandó tagjai:

1. Herbut Elvira, **gyermekorvos**, az egészségvédelmi rendszer képviselőjeként – tag
2. Kovács Szilvia, **iskolapszichológus**, az oktatási-nevelési rendszer képviselőjeként – tag
3. Mgr. Jasmina Zimonjić, **a szociális központ képviselőjeként** – tag
4. Pintér Melinda, **gyógypedagógus** – tag

II.

A bizottság koordinátori teendőit Mák Árpád okl. jogász látja el, aki Topolya Községi Közigazgatási Hivatalának dolgozója.

III.

A bizottság az oktatási és nevelési rendszer alapjairól szóló törvény, valamint a gyerekek, diákok és felnőttek kiegészítő oktatási, egészségügyi és szociális támogatásáról szóló szabályzat alapján dolgozik.

A bizottság véleménye az alábbiakat tartalmazza: a gyermek, diák, felnőtt személyes adatait; a bizottsági tagok adatait; a felmérés helyszínét; a felmérés módszereit – a felmérés során használt eszközöket és technikákat; a gyermek, diák és felnőtt funkcionális státusának leírását, valamint a gyermek, a diák, a felnőtt és a család életfeltételeinek leírását; az azonosított akadályok leírását, melyekkel a gyermek, diák és felnőtt szembesül (fizikai, kommunikációs és szociális akadályok); a gyermek, diák és felnőtt kiegészítő támogatás iránti szükségletének felbecslését, valamint a szükséges kiegészítő támogatás fajtáját; a gyermeknek, diáknak és felnőttnek nyújtott egyéni támogatási terv, amely az egészségügyi és szociális védelem, valamint az oktatás rendszerén belül nyújtott jogokon és szolgáltatásokon alapul, melyeket már igénybe vesz, vagy erre jogot formálhat; a kiegészítő támogatás biztosításában illetékes szerv vagy szolgálat; a kiegészítő támogatási intézkedések időtartamát.

A bizottság véleménye ellen a gyermek szülője, illetve egyéb törvényes képviselője és a felnőttek folyamodványt nyújthatnak be, a vélemény kézbesítésétől számított 15 napon belül.

A bizottság a folyamodvány alapján felülvizsgálja véleményét, s végleges véleményt mond, a folyamodvány átvételének napjától számított 30 napos határidőn belül.

A Bizottság véleményét eljuttatják a gyermek szülőjéhez, illetve egyéb törvényes képviselőjéhez, a felnőtt személyekhez és a kiegészítő támogatást biztosító illetékes szervhez, illetve szolgálathoz, a törvénnyel összhangban.

A bizottság köteles megőrizni a gyermek és családtagjai adatainak titkosságát, a személyi adatvédelemről szóló törvénnyel összhangban.

IV.

E végzés meghozatalával hatályát veszti a gyermekek és tanulók pótlólagos tanügyi, egészségügyi és szociális támogatását felmérő bizottság megalakításáról szóló végzés (Topolya Község Hivatalos Lapja, 2011/2. szám), minden módosításával és kiegészítésével együtt.

V.

E végzés megjelenik Topolya Község Hivatalos Lapjában.

Szedlár Péter, s.k.
a Községi Közigazgatási Hivatal
vezetője

Sor-Szám — TARTALOM — Oldal

Kiadó: Topolya Községi Közigazgatási Hivatalának a Községi Szervek Teendőivel és a Közös Teendőkkel Foglalkozó Osztálya. Telefonszám: 715-310. Felelős szerkesztő: a Községi Képviselő-testület titkára. A 2019. évi előfizetés 15.000,00 dinárt tesz ki, az alábbi befizetőszámlára: 840-70640-56 Topolya községi költségvetésének végrehajtása, Topolya Község Hivatalos Lapjára.