Iktatószám: NSZFH/630/001735-1/2025 Sorszám: V_2

A Nógrád Vármegyei Szakképzési Centrum (NVSZC) Informatikai Szabályzata

Jóváhagyta: .....(Gembiczki Ferenc) kancellár
Készítette: .....(Fekete Balázs) gazdasági vezető
Hatályos: 2025.03.31-től
Érvényes visszavonásig

Általános rendelkezések

1.§

A Nógrád Vármegyei Szakképzési Centrum (a továbbiakban: Centrum) informatikai szabályzata (a továbbiakban: szabályzat) a Centrum szervezetében üzemeltetett, működtetett informatikai rendszer, hardver, szoftver, e-mail, internet és intranet szolgáltatására vonatkozó intézkedéseket szabályozza az IT infrastruktúra szabályszerű használatának biztosítása céljából.

(1) A szabályzat tárgyi hatálya a Centrum tulajdonában lévő, az általa bérelt vagy üzemeltetett informatikai infrastruktúra elemekre és az azokon tárolt, illetve szolgáltatott adatokra, adatbázisokra (pl. hardver elemek, nyomtatók, fénymásolók, az informatikai hálózat, hálózati erőforrások, hálózati szolgáltatások, rendszerszoftverek, alkalmazások) terjed ki.

(2) A szabályzat személyi hatálya kiterjed:

a) A Centrum valamennyi szervezeti egységére, valamennyi munkavállalójára, a Centrummal szerződéses vagy egyéb munkavégzésre irányuló jogviszonyban álló személyekre (a továbbiakban együttesen: foglalkoztatottak).

b) A Centrum részeként működő szakképző intézmények a tanulókra, oktatásban résztvevőkre vonatkozó további részletszabályzatokat külön belső szabályzatukban határozzák meg. A szakképző intézmények speciális helyzetekre tekintettel belső szabályzatukban jelen szabályzat előírásaitól a kancellár engedélyével eltérhetnek. A szakképző intézmények informatikai belső szabályzatainak kancellár által történő jóváhagyása szükséges.

c) a Centrummal egyéb szerződéses jogviszonyban álló természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (a továbbiakban: külső személy) a velük kötött szerződésben rögzített mértékben, az általuk tett titoktartási nyilatkozat alapján.

Fogalmak

E szabályzat alkalmazásában:

1. Felhasználó: az a természetes személy, aki az informatikai rendszer erőforrásait és szolgáltatásait a napi munkájának elvégzéséhez igénybe veszi. Nem tekintendő felhasználónak az, aki az interneten keresztül veszi igénybe a Centrum által nyilvánossá tett informatikai szolgáltatásokat, és így kerül kapcsolatba az informatikai infrastruktúrával.

2. WLAN: vezeték nélküli hálózati kapcsolat.

3. Adat: meghatározható, leírható elemi tulajdonság, adottság, személytelen tényt közlő ismeret, illetve tények, fogalmak, összefüggések formalizált reprezentációja, amely alkalmas személyek, és az informatikai eszközök által történő kezelésre, feldolgozásra. Olyan jelsorozat (pl. bit, byte, egyéb karakter stb.), amely lehetőséget teremt információ előállítására.

4. Adatállomány: egy nyilvántartó rendszerben kezelt adatok összessége. Adathordozón tárolt adatok halmaza, amelyet azonosító névvel látnak el.

5. Adatátvitel: adatok továbbítása összeköttetéseken, összekötő utakon (pl. számítógépek között) információtechnológiai eszközök segítségével.

6. Adatbázis: adatok egymással kapcsolatban álló, rendezett állománya. Egy vagy több adatállomány összessége, amelyet erre alkalmas kezelőszoftverrel humán szereplő számára értelmezhető formában elérhetővé, megjeleníthetővé lehet tenni.

7. Adatbiztonság: az adatok rendelkezésre állásának kérdése. Célja, hogy a jogosult felhasználó és csakis az bármikor hozzáférhessen a számára szükséges adatállományhoz. Tágabb értelemben azon fizikai elemek, műszaki és szervezési megoldások, intézkedések összessége, melyek az előbbiekben meghatározott cél elérését biztosítják.

8. Adatfeldolgozás: az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

9. Adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő megbízásából beleértve a jogszabály rendelkezése alapján történő megbízást is — a személyes adatok feldolgozását végzi.

10. Adatgazda: adott — jogszabályban meghatározott — célra szolgáló és meghatározott összetételű adatok kezelését, felügyeletét végző személy.

11. Adatkezelés: az adatokon végzett bármely művelet vagy műveletek összessége az alkalmazott eljárástól függetlenül, így az adatok gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása. Adatkezelésnek számít a fénykép, hang- vagy képfelvétel készítése, valamint személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS minta, íriszkép) rögzítése is.

16. Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

17. Adattovábbítás: az adat meghatározott harmadik személy számára hozzáférhetővé tétele.

18. Adatvédelem: a személyes adatok kezelésének korlátozását, az érintett személyek jogi védelmét, illetőleg információs önrendelkezésük gyakorlását biztosító szabályok, eljárások, eszközök és módszerek összessége.

19. Alkalmazás, alkalmazói program: valamely meghatározott cél érdekében működtetett (futtatott) algoritmus sorozat, amely a hardver és üzemi rendszer funkcióit használja, és amely a kimenetén a célinformációkat (outputot) szolgáltatja.

20. Archiválás: az adatok állományának kiírása egy közvetetten hozzáférhető elkülönített tárolóba.

21. Bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

22. Elektronikus adathordozó: az adatok elektronikus, mágneses vagy optikai rögzítésére, tartós tárolására szolgáló eszköz.

23. Futtatás, futtatási folyamat: valamely program, algoritmus operátorok útján történő elindítása, működése, célfeladatának végzése a számítógépen.

24. Hardver: az informatikai rendszer fizikai elemei, műszaki berendezések.

26. Hálózat: két vagy több számítógép, vagy általánosabban informatikai rendszerek összekapcsolása információtechnológiai eszközökkel, amely a komponensei közti adatcserét teszi lehetővé.

27. Hírlevél: levelező listán szereplő személyek, vagy szervezeti egységek felé rendszeresen továbbított, esetlegesen tematikus tartalmú elektronikus levél.

28. Hozzáférés: olyan eljárás, amely a felhasználó számára, jogosultsága függvényében elérhetővé teszi az informatikai rendszer erőforrásait.

29. Hozzájárulás: az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok teljes körű vagy egyes műveletekre kiterjedő kezeléséhez.

30. Információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti.

31. Információs rendszer: azon eljárások, tevékenységek összessége, amelyek a szervezet működéséhez és irányításához szükséges információkat tárolják, előállítják, szétosztják.

32. Informatika: az információ rendszeres és automatikus — elsősorban számítógéppel történő rögzítésével, tárolásával, feldolgozásával és továbbításával foglalkozó tudomány.

36. Informatikai eszköz: az informatikai- és információszolgáltatás valamennyi tárgyi, illetve tárgyiasult szellemi komponense, így a számítógépek, számítógépes hálózatok és kapcsolódó eszközök, szoftverek, konfigurációk, rendszer-beállítási paraméterek, dokumentációk stb.

37. Informatikai biztonság: az informatikai rendszer olyan állapota, amelyben az adatokhoz minden felhasználó kizárólag jogosultsága mértékében tud hozzáférni. Az adatok egyéb módon nem változnak, hitelességük megállapítható.

38. Informatikai rendszer: a hardverek és szoftverek olyan kombinációjából álló rendszer, amit az adat-, illetve információfeldolgozás különböző feladatainak teljesítésére alkalmaznak.

39. LAN: helyi hálózat.

40. Log fájlok: a rendszernapló bejegyzései.

41. Letöltés: adattartalom (szöveges, kép, hang, program stb.) importálása saját gépre.

42. Meghajtó: fájlrendszerrel formázott, betűjellel jelölt adattároló terület. A tár lehet hajlékonylemez, CD, merevlemez vagy más típusú lemez. A meghajtó tartalmának

megtekintéséhez a meghajtó ikonjára kell kattintani (pl. a Windows Intézőben vagy a Sajátgép ablakban).

43. Mentés: az adatok reprodukálása (átmásolása, duplikálása) egy elkülönített tároló helyre (meghajtóra). A művelet után az adat továbbra is közvetlenül elérhető marad a helyén (ld. archiválás).

44. Működőképesség: a rendszernek és elemeinek az elvárt és igényelt üzemelési állapotban való fennmaradása. A működőképesség fogalom sok esetben azonos az üzembiztonság fogalommal.

45. Olvasás, olvasási folyamat: az előzőleg már rögzített adat dekódolása és megjelenítése.

46. Operációs rendszer: az az algoritmusokkal meghatározható speciális program, amely lehetővé teszi, hogy a felhasználó kapcsolatba lépjen a gép fizikai egységeivel. Lehetővé teszi a meghatározott célok érdekében telepített programok futtatását, értelmezését a gépi logika, a processzor számára. A gépek alapvető, kötelezően létező programja, amelyből sokféle van (pl. DOS, Windows, Linux, Unix, OSX).

50. Rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

51. Rendszerprogram: olyan alapszoftver, amelyre szükség van valamely informatikai rendszer hardvereinek használatához és az alkalmazói programok működtetéséhez. A rendszerprogramok nagy részét az operációs rendszerek alkotják.

52. Sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.

53. Szoftver: az informatikai rendszer logikai része, amely a működés vezérléséhez szükséges.

54. Tartomány: számítógépek olyan csoportja, amely egy hálózatrészt alkot és közös címtáradatbázist használ. A tartomány felügyelet szempontjából egy egységet képez, amelyre közös szabályok és eljárások vonatkoznak. Minden tartománynak egyedi neve van.

55. Tartományvezérlő: a tartomány működésének biztosítására szolgál.

56. Biztonsági csoport: a szervezeti egység a tartományi hierarchiát biztosítja. Az biztonsági csoportok adnak a tartománynak az adminisztrációt megkönnyítő hierarchiát, segítségükkel az Active Directory struktúrájára leképezhető a vállalat szervezeti felépítése vagy földrajzi elhelyezkedése.

57. Kilépett OU: olyan Organizational Unit, amely a letiltott felhasználókat tartalmazza.

58. Vezető: A munkáltatói jogkör gyakorlója, felel a vezetése, irányítása alatt álló szervezet területén és/vagy kezelésében lévő informatikai eszközök szabályszerű használatáért, működtetéséért, a jelen szabályzatban foglaltak betartásáért és betartatásáért. Az adatokhoz (alkalmazásokhoz) történő hozzáférés megadását biztosító folyamatban a vezetőnek javaslattételi, az alaphozzáférést tekintve pedig engedélyezési joga van, azaz meghatározza, hogy az irányítása, vagy vezetése alatt álló munkatársnak a munkagelyi vagy projekt feladatainak elvégzéséhez milyen adatokhoz szükséges hozzáférnie.

62. Vírus: a számítógépes vírus olyan program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Többnyire rosszindulatú, más állományokat használhatatlanná, sőt teljesen tönkre is tehet. A vírusok jellemzően pendrive vagy e-mail útján terjednek, az internetes böngészés mellett, valamint a megbízhatatlan oldalakról történő letöltések által.

63. VPN (Virtual Private Network): virtuális magánhálózat.
64. Policy: a felhasználók, a számítógépek és a felhasználói munkakörnyezetek viselkedésének és jogosultságainak szabályai.
65. Group Policy Management: a Microsoft operációs rendszereinek egy funkciója, amivel megoldható a felhasználók, a számítógépek és a felhasználói munkakörnyezetek viselkedésének és jogosultságainak szabályozása. A csoportházirend Active Directory környezetben lehetővé teszi az operációs rendszerek, alkalmazások és a felhasználók beállításainak központosított konfigurálását és menedzsmentjét.
66. Group Policy Object (GPO): a csoportházirend építőkövei.
67. AD profil: címtartomány felhasználói fiók.

2.§

Üzemeltetési szabályok

(1) Az informatikai referens alapvető feladatai:

- Az informatikai infrastruktúra működőképességének biztosítása a szerződött informatikai partner segítségével.
- A felhasználói igényeket kielégítő, szabványos telepítési eljárások kidolgozása, a hardverek, szoftverek átvétele a szállítótól,
- A szoftverek biztonsági másolatainak elkészítése és a másolatok védelmi előírásoknak — megfelelő tárolása,
- Az aktualitásukat vesztett, tovább nem alkalmazható szoftverek selejtezésének kezdeményezése,
- A Centrum szintű alkalmazások működését befolyásoló informatikai és távközlési eszközök (pl. szerverek, rack szekrény stb.) szünetmentes tápegységekkel való ellátása,
- Az informatikai eszközök és berendezések folyamatos használata és rendelkezésre állásának biztosítása érdekében:
    - specifikációban javasolt időközönként el kell végezni a berendezések karbantartását,
    - a berendezések kezelését és javítását csak megfelelő szakképzettséggel rendelkező személyek végezhetik,
- A felhasználók szoftver üzemeltetési problémáinak megoldása folyamatos szakmai tanácsadással, helyszíni hibaelhárítással
- A munkaállomásokon végzett munkát alapszolgáltatás biztosításával támogatja. Az alapszolgáltatás biztosítása a szabványos informatikai munkakörnyezet létrehozását, folyamatos működésének biztosítását és a kapcsolódó szolgáltatások ellátását jelenti.

Szerverekkel kapcsolatos feladatok

- Felhasználók létrehozása, karbantartása, jelszavak beállítása és kezelése, jogosultságok kiosztása kezelése
- Mappaszerkezet kialakítása
- Felhasználók tájékoztatása a mappa struktúrákról és a fájlok tárolási helyéről, ezek használatának megkövetelése és ellenőrzése

Microsoft 365 rendszer

- Új felhasználók hozzáadása, meglévő fiókok módosítása és törlése, valamint jelszavak alaphelyzetbe állítása
- A letiltott felhasználók visszaállítása új jelszó beállítása
- Elvégzi az évente szükséges felhasználói adminisztrációkat.
- Beállítja a többtényezős hitelesítést (MFA)
- E-mail és kommunikációs eszközök kezelése: Az Exchange Online és a Microsoft Teams beállításainak kezelése, beleértve a csoportok és naptárak kezelését

(2) A szerződéses informatikai partner feladatai:

1. A szerződéses informatikai partner feladata az informatikai rendszereinek megbízható üzemeltetése, amely kiterjed az informatikai rendszer erőforrásainak és szolgáltatásainak folyamatos biztosítására, új elemek üzembe helyezésére, az esetlegesen jelentkező hibák kijavítására, a mentések, illetve helyreállítások végzésére és a rendszer használatával kapcsolatos gyorssegély ellátására.
2. A szerződéses informatikai partner feladata az üzemeltetett rendszerek rendszeres mentése és a biztonsági archiváláshoz tartozó feladatok ellátása, a rendszer és az adatállományok visszaállíthatóságának biztosítása.
3. Üzemelteti a Centrum intézményeiben működő Informatikai rendszereinek azon részét, mely a kiszolgáló és hálózati infrastruktúra részei (pl. routerek, szerverek, switch-ek, NAS-ok fizikai és logikai üzemeltetése), tehát távolról is felügyelhetők, a beavatkozásokjó részéhez nem kell a helyszínen lenni.
4. Távfelügyeleti és bejelentéskezelő rendszert üzemeltet, informatika biztonsági szolgáltatást nyújt a Centrum számítógépeinek védelmére.

Routerek üzemeltetése

- a forgalmi statisztikákat folyamatosan gyűjti, időszakosan megőrzi
- működési paramétereket folyamatosan ellenőrzi
- Routereket igény szerinti teljes körűen konfigurálja
- A router-ek szoftverének frissítését havonta, kritikus biztonsági javítás megjelenése esetén soron kívül elvégezi, a konfigurációkat naprakészen menti

Microsoft 365 rendszer üzemeltetése

- szakmai támogatást nyújt az Intézmények rendszergazdái részére és közreműködik az esetleges problémák azonosításában és megoldásában.
- Napi rendszerességgel ellenőrzi a kockázatos felhasználókat és a kockázatos bejelentkezéseket
- A feltört felhasználói fiókot haladéktalanul letiltja és e-mailben értesítést küld a hozzá tartozó intézmény rendszergazdájának.

Szerverekkel kapcsolatos feladatok

- fizikai szerver hardver állapot folyamatos figyelése
- virtuális szerver futási állapot folyamatos figyelése
- szoftverek, szolgáltatások folyamatos figyelése
- igényelt szolgáltatások telepítése, konfigurációja
- mentések felügyelete és ellenőrzése
- A szerverek (fizikai és virtuális) operációs rendszerének frissítése havonta, vagy kritikus biztonsági javítás megjelenése esetén soron kívül végzi
- A konfiguráció és adatmentések naponta

NAS eszközökkel kapcsolatos feladatok

- hardver állapot folyamatos figyelése szoftverek folyamatos figyelése
- A NAS-ok operációs rendszerének, szoftvereinek frissítését havonta, vagy kritikus biztonsági javítás megjelenése esetén soron kívül elvégezi

- A konfiguráció mentések naponta

(3) **Alapszolgáltatás**

- Az alapszolgáltatást csak a felhasználói jogosultsággal rendelkező személyek vehetik igénybe a helyi címtartományon (centrum.internal) belül
- Az alapszolgáltatástól eltérő, szakmailag indokolható igényeket a vezető írásos hozzájárulása alapján biztosíthat a felhasználónak az informatikai referens.
- Jelen szabályzat keretében alapvető munkakörnyezetnek a következőket tekintjük:
    - felhasználó részére biztosított munkaeszköz: számítógép, opcionálisan: munkahelyi illetve otthoni használatra laptop operációs rendszer, valamint irodai programcsomag,
    - a centrumban kialakított informatikai hálózatban adatállományok tárolását végző rendszer (fájlszerver),
    - a szerver végzi
        - a felhasználók azonosítását (címtár szolgáltatás),
        - a felhasználókra és a munkaeszközökre érvényes, kötelezően alkalmazandó szabályrendszer kikényszerítését (csoportházirendek alkalmazása),
        - a hálózati erőforrásokhoz való hozzáférés szabályozását előre meghatározott jogosultsági rendszer alapján.
- Az alapvető munkakörnyezetnek biztosítania kell a következőket:
    - minden felhasználó részére elérhetők legyenek a szervezeti egységének adatállományai.
    - minden felhasználó részére elérhetők legyenek a szervezeti egységek azon nyilvános adatállományai, amelyeket az adott szervezeti egységek közzétételi szándékkal az adott tárhelyen (fájlszerver) megosztanak,
    - egy elkülönített tárhelyet (fájlszerver) a felhasználónak, hogy a napi munkaanyagait tárolja,
    - egy elkülönített tárhelyet a fájlszerveren a felhasználónak, hogy a hálózati lapolvasás (szkennelés) következtében keletkezett adatállományokat ideiglenesen tárolja.
- A fent felsorolt megadott tárhelyeket a felhasználónak a saját munkaeszközébe való bejelentkezésekor elérhetővé kell tenni. A hálózati tárhelyeket hálózati meghajtóként fel kell csatolni.
- Az informatikai alapszolgáltatáshoz tartozik a nyomtatási és biztonságos szkennelés biztosítása.

3.§

Helyi szerver, címtartomány (centrum.internal)

(1) A fájlok tárolását és a megfelelő hozzáférések kezelését a Centrumban kialakított központi címtartomány (centrum.internal), és az ehhez tartozó kiegészítő fájlszolgáltatás adja. A címtár és fájl szerver szolgáltatást erre dedikált Windows Server 2022 Standard operációs rendszerrel ellátott szerver nyújtja.

(2) A Centrum vezetőinek döntése alapján, külön biztonsági csoportokat kell létrehozni, a szervezeti egységben dolgozó kollégákat ezen csoportokba kell sorolni.
(3) Az egyes csoportok jogosultságait a vezetők döntik el.
(4) Az Informatikai referens feladatköréből adódó jogosultságai:

a. új felhasználók rögzítése,
b. új felhasználók jogosultságainak, hozzáféréseinek, csoporttagságainak beállítása,
c. meglévő felhasználók jogosultságainak, hozzáféréseinek, csoporttagságainak módosítása, karbantartása,
d. felhasználók attribútumainak karbantartása, különös tekintettel a munkakör, osztály, telefonszám mezők helyes kitöltésére, naprakészen tartására,
e. távozó felhasználók jogosultságainak, hozzáféréseinek letiltása,
f. elfelejtett jelszó esetén új jelszó adása,
g. levelező fiókokkal kapcsolatos feladatok ellátása,
h. Group Policy Management (Policy létrehozása, szerkesztése, törlése, naprakészen tartása)

4.§

Vírusvédelem

(1) A Centrum az informatikai partner közreműködésével központi vírusvédelmi menedzsmentet biztosít, amelynek telepítése a helyi gépeken és az otthon használt laptopokon is kötelező.

5.§

Nyomtatás

(1) A Centrumba a nagyteljesítményű központi nyomtatókon történő munkavégzés az engedélyezett. Asztali lokál vagy hálózati nyomtatók kizárólag indokolt esetben használhatóak. A nyomtatók, fénymásolók működtetése üzemeltetési szerződés keretében történik.

(2) A szkennelés a nagyteljesítményű nyomtatókon keresztül történik, a szkennereken beállított helyekhez való hozzáférést a biztonsági csoport jogosultság adja. A szkenneléshez tartozó célmappákból a szkenneléseket azonnal el kell távolítani a saját mappákba, a szkennelési mappák minden nap 0:30 perckor automatikusan törlésre kerülnek.

6.§

Szerverterem, szerverszoba

A Centrum hálózati eszközeit, szervereit és további hálózat működését szolgáló eszközöket tárolni kizárólag a Centrum használatában lévő, beazonosítható szerverteremben, szerverszobában, vagy azok elhelyezésére szolgáló, kulccsal, kártyával vagy kóddal zárt külön nevesített helyiségben (a továbbiakban: informatikai helyiség) lehet.

7. §

Az internet, intranet használat szabályai

1) A Centrum internet szolgáltatását a Telekom Zrt. látja el.

2) A szakmai feladatok hatékony ellátásához szükséges információkhoz, szolgáltatásokhoz való hozzáférés érdekében az Intézmény valamennyi felhasználója jogosult a munkahelyi internet és elektronikus levelezés használatára.

3) Minden felhasználó saját felelősségére használja az internetet, mint szolgáltatást.

4) A tiltott tartalmú weboldalakra irányadó szabályokról az 8. § rendelkezik.

5) Az internet szolgáltatás eléréséhez kizárólag a Centrumban rendszeresített internetes alkalmazások (Google Chrome, Microsoft Edge, Mozilla Firefox) valamelyike használható.

6) Alapelv, hogy minden weblap és internetes szolgáltatás elérése engedélyezett, amíg annak tartalma nem ütközik semmilyen jogszabályi előírásba.

7) Tekintettel arra, hogy az internethasználat a Centrum által biztosított infrastruktúrán, és szolgáltatási költségen valósul meg, a Centrum jogosult bármikor, bármilyen weblap, internetes szolgáltatás elérésének ideiglenes vagy teljes korlátozására. Ezen weboldalak nem ütköznek semmilyen jogszabályi előírásba, letiltásuk a hálózat leterheltségének kezelhetőségére, a munkaidő hatékony kihasználására irányul.

8) A hálózat számára nagy terhelést jelentő képi- (pl. grafikus fájl, video) és hangi- (pl. *.mkv, *.mp3, *.avi, *.wav. stb.) információkat tartalmazó anyagok letöltése, továbbítása csak az Informatikai referenssel előre egyeztetve tehető meg.

9) A felhasználók az Centrum nevében nem tölthetnek fel engedély nélkül az internetre, közösségi portálokra adatot és anyagot (pl. honlap, hirdetmények).

10) Az Centrum tulajdonát képező szoftverek interneten vagy e-mailen keresztül történő továbbítása, mások részére való hozzáférhetővé tétele — előzetes külön engedély hiányában — nem engedélyezett.

8. §

Tiltott tartalmú oldalak:

1) szexuális tartalmú oldalak, különösen az alábbi tartalmakkal:
2) kiskorúak veszélyeztetése,
3) erőszak,
4) pornográfia,
5) marketing molesztáló jellegű formái (felhívás ilyen jellegű oldalak látogatására),
6) az emberi méltóság megsértése,
7) rasszizmus,
8) szexuális beállítódás, vallás, nemzetiség vagy etnikai származás miatti megkülönböztetés,
9) gazdasági bűnözés fogalma alá eső cselekmények,
10) csalás,
11) tiltott kereskedelmi tevékenység,
12) hitelkártyával való visszaélésben való közreműködés,
13) rémhírterjesztés,

14) információbiztonság veszélyeztetése,
15) rossz szándékú hackertámadás,
16) hacker, cracker technológiák és leírásuk, eszközök terjesztése, használata,
17) vírusprogramok terjesztése, írása,
18) a magánszféra megsértése,
19) személyes adatokkal való visszaélés,
20) elektronikus zaklatás,
21) a személyiségi jogok megsértése,
22) rágalmazás,
23) meg nem engedett összehasonlító reklám,
24) a szellemi tulajdon megsértése,
25) tiltott szerencsejáték,
26) a szerzői jog által védett digitális anyagok (művek, szoftverek, zenék stb.) jogosulatlan terjesztése,
27) bombák készítéséhez adott segítségnyújtás,
28) illegális kábítószer használat, előállítás és terjesztés,
29) nemzetbiztonsági szempontból tiltott tartalmú oldalak,
30) terrorista tevékenység.

9. §

Webes megjelenés, tartalmak kezelése

(1) A Centrum és az intézményei a fenntartó által biztosított weboldalt használja. A fenntartó feladata a weboldal elérhetőségének és biztonsági frissítéseinek biztosítása.
(2) A Centrum központi honlapjára történő tartalomfeltöltés a Centrum vezetősége, kommunikációs területéért felelős munkatársa és az Informatikai referens együttes feladata.
(3) A NVSZC weboldala a www.nmszc.hu címen érhető el.

10. §

Az elektronikus levelezés általános szabályai – Microsoft 365 rendszer

(1) A Centrumon belül kizárólag a tisztaszoftver elérés keretében ingyenesen biztosított Microsoft 365 levelező és csoportmunka támogató rendszer használata engedélyezett.
(2) Az elektronikus levelezés zavartalan működését, a mindenkori igényeknek és forgalomnak megfelelő hardver és szoftver erőforrások meglétét, szakszerű szolgáltatását a Centrum biztosítja.
(3) Minden dolgozó és tanuló belépéskor, a jogviszony idejére megkapja a Microsoft 365 fiók hozzáférését.
(4) A jogviszony megszűnésekor azonnal törölni kell a felhasználói fiókokat.
(5) A távozó felhasználó postafiókjáról a vezető döntése alapján archivált állomány készül. Az archív leveket tartalmazó állományt az informatikai referens a szerveren kialakított, dedikáltan a levelezéseket tartalmazó adatállományok tárolására használt tárhelyre másolja. Ezen

adatállományokat a tárolókapacitás függvényében, azonban lehetőség szerint legalább 2 évig a szerveren kell tárolni.

11. §

(1) A Centrum a felhasználó részére névre szóló postafiókot biztosít. A postafiókok távolról, az Outlook Web Access szolgáltatásán keresztül is elérhetők az www.office.com címen.
(2) Az e-mail címek képzési szabálya: "vezetéknév. utónév@NVSZC.hu". Amennyiben az e-mail cím már foglalt, úgy a vezetéknévhez a következő szabad sorszámot kell illeszteni, pl. "vezetéknév. utónév2@nmszc.hu".
(3) A Microsoft 365 rendszerbe csak kétfaktoros hitelesítés után lehet belépni.
(4) A felhasználói postafiók mérete 50 Gb. Amennyiben a postafiók a megadott méretet eléri vagy meghaladja, a felhasználók e-mailt küldeni és fogadni sem tudnak. A postafiókok méretének rendszeres időközönként történő karbantartása a felhasználó feladata. A felhasználó a rendszer által automatikusan küldött levélben értesül róla, hogy a postafiókja megtelt.
(5) Az elektronikus levél maximális mérete korlátozott, 25 MByte.
(6) A Centrum levelezési szolgáltatását igénybe vevő felhasználók munkaállomásainak alkalmasnak kell lenniük a ZIP formátumú, tömörített állományok kezelésére. A mérethatárt túllépő állományokat a rendszert képező Onedrive felhő alapú tárolásra és megosztásra használat szoftver segítségével valósíthatjuk meg.
(7) A levélnek kötelező tárgyat és szövegtörzset tartalmaznia. A levél tárgyának röviden, de értelmezhető módon utalnia kell annak tartalmára.
(8) A levelek automatikus aláírását a levelező rendszerben be kell állítani. Az aláírásnak a hivatali adatok közül tartalmaznia kell az aláíró
- A centrum logóját,
- nevét,
- munkakörének megnevezését,
- telefonszámát — amennyiben ilyennel rendelkezik,
- mobiltelefonszámát — amennyiben ilyennel rendelkezik,
- e-mail címét.

(9) Az elküldött levelek tartalmáért a küldő felel.
(10) A Centrum bármely postafiókján külső e-mail címre történő továbbítási szabályt beállítani tilos.
(11) Tilos olyan levelek továbbítása a Centrum levelező rendszerében, amelyek bármilyen nyelven arra szólítanak fel, hogy a levelet minél több címre kell továbbítani.
(12) Tilos válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy a felhasználó a Centrum biztonsági rendszeréről, vagy saját hozzáférési adatairól (tartománynév, felhasználónév, jelszó) adjon tájékoztatást.
(13) A szervezeti működés megkönnyítése érdekében vezetői jóváhagyás után megosztott postaládát készítünk, amelyet egyszerre több kijelölt felhasználó használhat.
(14) A megosztott postaládát az informatikai referens hozza létre, a 3. sz. mellékletben található Megosztott postaláda igénylő lapon megjelölt adatok alapján.
(15) A megosztott postaládára is vonatkoznak a saját e-mail fiókra vonatkozó szabályozások.

12. §

(1) Az elektronikus levelező rendszerben megjelenő információk, dokumentumok, elektronikus levelek a Centrum tulajdonát képezik, figyelembe véve a személyes adatok kezelésére vonatkozó hatályos adatvédelmi szabályokat, eljárásokat.

(2) A Centrum által a felhasználó részére biztosított, a munkavégzését segítő elektronikus levelező postafiókot magáncélra használni tilos, különös tekintettel tilos az e-mail címmel közösségi portálra regisztrálni, nem munkahelyhez kötött hírlevélre szolgáltatásra feliratkozni, egyéb nem munkahelyi feladatok ellátásához használt weboldalakra a címmel regisztrálni.

(6) A munkatársak kérhetik a Centrum által biztosított levelezésnek a tulajdonukban lévő, és a munkáltató által engedélyezett mobil eszközre való beállítását.

13. §

(1) Amennyiben a vállalati levelezés saját tulajdonú mobil eszközre lett beállítva, úgy ezen az eszközön is alkalmazni kell a Centrum által előírt biztonsági intézkedéseket (PIN kód, jelszavas képernyőzár). Ezek hiányában az Informatikai Referens a vállalati levelezés beállítására irányuló kérést köteles megtagadni.

(2) A Centrumtól távozó felhasználó postafiókjának archiválásáról, megszüntetéséről, valamint a megszüntetéséig a betekintési jogosultak köréről a vezetőség jogosult dönteni.

(3) A távozó felhasználó postafiókjáról a vezetőjének döntése alapján archivált állomány készül. Ezen adatállományokat a tároló kapacitás függvényében, azonban lehetőség szerint legalább 2 évig a szerveren kell tárolni.

(4) A felhasználó postafiókjának teljes vagy részleges tartalma a felhasználótól elkérhető, vagy szükség esetén az Informatikai referens bevonásával lekérhető az alábbi körülmények fennállásakor:

a) a Belső Ellenőrzés, által folytatott eljárások esetén az eljárás lebonyolításához szükséges információk megszerzésére vonatkozóan:
   - a vizsgálat célzott, így az adatok bekérése is (vizsgált időperiódus vagy egyéb konkrét feltétel),
   - első lépésben a postafiók leveleinek fejlécét, a fejléci információk alapján pedig a vizsgálatot végző szervezeti egység a vizsgálat céljának megfelelően kiválasztott levelek nyomtatott verzióját, beleértve a levél mellékleteit is,
   - levelezésből kinyert információk kezelésére, tárolására és megsemmisítésére a szervezeti egységek belső szabályai, valamint a Centrum adatvédelmi és adatkezelési szabályai az irányadóak,

b) külső nyomozati szerv által történt nyomozati cselekményben való részvétel, hivatalos megkeresése esetén a nyomozati szerv által kért részletességgel

14.§

(1) Az elektronikus levelezés során a postafiókokat vírusvédelmi rendszer védi. Az elektronikus postafiókba érkező, ismeretlen feladótól (gyanús, értelmezhetetlen vagy külföldi) származó, nem szokványos formátumú, gyanús csatolmányt tartalmazó, vagy idegen nyelvű küldeményekkel — a fennálló vírusveszély miatt — fokozott óvatossággal kell eljárni.

(2) A gyanús küldemény érkezésekor, valamint a vírusvédelmi rendszer riasztása esetén haladéktalanul értesíteni kell az Informatikai referens munkatársat. A csatolmányt ilyen esetben tilos megnyitni.
(3) Tilos lánclevelek indítása vagy továbbítása.
(4) A felhasználó elektronikus levelezési címével beregisztrálni bármely, az interneten lévő webes rendszerbe, vagy külső szervezet rendszerébe csak szakmailag indokolt esetben és a közvetlen vezetője hozzájárulásával engedélyezett.

15.§

Jelszavak képzése, kezelése

(1) A felhasználó a rendszerbe való első belépéshez ideiglenes jelszót kap, amelyet az első lehetséges alkalommal köteles megváltoztatni. Az ideiglenes jelszót az Informatikai referens generálja.
(2) A felhasználói azonosítás kulcseleme a jelszó. A Centrum teljes informatikai hálózatában használatos jelszavaknak az alábbi feltételeknek kell megfelelniük:

- A jelszónak minimum 12 karakterből kell állnia
- A jelszó nem tartalmazhatja még részleteiben sem a felhasználó nevét (se a vezeték - ,se a keresztnevét), valamint a rendszerhez használatos felhasználónevét.
- A jelszó érvényességi idejét, ezzel együtt a jelszócsere gyakoriságát az informatikai rendszer központi szabályozása vagy a használt rendszer működése határozza meg, amely jelenleg 1 év.
- Amennyiben az informatikai rendszer lehetővé teszi, törekedni kell arra, hogy a jelszócsere kikényszerítésre kerüljön, és a felhasználó e-mailes értesítést kapjon a jelszócsere szükségességéről.
- Egy aktuális jelszó maximális élettartama 365 nap.

16.§

(1) A rendszerek, illetve szoftverek telepítése után az alapértelmezett jelszavakat meg kell változtatni.
(2) A felhasználói jelszavakat bizalmasan kell kezelni. Szigorúan tilos jelszavakat nyilvánosan vagy más felhasználókkal megosztani.
(3) Jelszavak elfelejtése, illetve más által történő megismerése esetén új jelszót kell igényelni.
(4) A felhasználó a számítógépre csak saját nevében és jelszavával léphet be, és az alkalmazásokat csak saját nevében használhatja. Előbbiektől eltérően csak indokolt esetben, az illetékes vezető írásos engedélyének birtokában lehet eljárni.
(5) A jelszókezelés szabályai:

- jelszavak nem hozhatók nyilvánosságra,
- a jelszavak biztonságának megőrzéséért a felhasználó személyesen felel,
- a felhasználó a jelszavát nem oszthatja meg senkivel,

- amennyiben a felhasználónak a legkisebb gyanúja is felmerül a jelszó biztonságának integritása felől, azt köteles azonnal megváltoztatni és gyanújáról az informatikai referenst
- más felhasználó azonosítóját átmeneti jelleggel sem szabad használni, valamint a felhasználó köteles a jelszavát az előírt gyakorisággal és módon megváltoztatni.

(6)

Informatikai jogosultság

17.§

Új felhasználói jogosultság létrehozása

(1) A vezető igényli a belső és külső felhasználó jogosultságait. A felhasználó foglalkoztatotti jogviszonyát érintő változásról (kinevezés, áthelyezés, felfüggesztés, munkaviszony megszűnése, a jogviszony alapjául szolgáló szerződés megszűnése és a titoktartási nyilatkozat visszavonása stb.) a vezető köteles, illetve egyéb igény esetén jogosult a kitöltött jogosultságigénylő lapot (1. melléklet) benyújtani az Informatikai referensnek

(2) A vezető által jóváhagyott jogosultságigény kizárólag az informatikai hálózat, illetve erőforrásai üzemeltetésének veszélyeztetése esetén, megfelelő informatikai szakmai indokolással utasítható el.

(3) Amennyiben új kolléga érkezik az Informatikai Referens feladata a munkavállaló AD profiljának létrehozása, e-mail fiók elkészítése, valamint a jogosultság igénylő alapján a különböző hozzáférések beállítása.

(4) Az informatikai referens a kialakításra kerülő rendszer jogosultságait a Centrum vezetők jóváhagyásával dokumentálja, továbbá a jogosultság igénylő és jogosultság megszüntető lapok segítségével naprakészen vezeti, évente ellenőrzi a dokumentáció és az Active Directory egyezőségét.

18.§

Felhasználói jogosultság megszüntetése

(1) A Centrummal foglalkoztatotti jogviszonyban álló személy jogviszonyának megszűnése esetén a közvetlen felettes kezdeményezi a dolgozó jogosultságainak megszüntetését, amelyet informatikai jogosultság megszüntető űrlap (2. melléklet) útján tesz meg.

(2) A felhasználót megillető jogosítványok megszüntetése az űrlap adatai alapján történik.

(3) A postafiókok megszüntetése és archiválása az Informatikai Referens feladata

(4) A tartományi jogosultságok megszüntetése:

Az Informatikai Referens blokkolja a kilépő kolléga AD profilját, a levelezőfiók archiválásra kerül, majd automatikus válaszüzenet kerül beállításra, amiben a feladó tájékoztatva lesz, hogy a kolléga kilépett, a postafiókját más nem olvassa és a feladatait átvevő személy elektronikus elérhetősége is megadásra kerül, akit ez alapján a feladó meg tud keresni.

19.§

Speciális hozzáférések

1) A felhasználók az NVSZC rendszeréhez távolról kizárólag titkosított kapcsolaton keresztül férhetnek hozzá. A munkatársak távolról való bejelentkezése munkavégzés céljából szükséges lehet, de kizárólag indokolt esetben szabad a jogosultságot megadni a fokozott informatikai biztonsági kockázat miatt.
2) Távolról való bejelentkezésre az informatikai referens jóváhagyásával kizárólag az kancellár, vezető adhat engedélyt
3) Távoli, otthoni munkavégzésre a munkahely által biztosított laptopot az informatikai referens állíthatja be a belső hálózat elérésére.
4) Az NVSZC belső hálózatát kizárólag a cég által biztosított laptopról lehet használni, a céges hálózathoz való kapcsolat kizárólag a munkavégzés idejére használható, munkavégzés céljából.

20.§

Felhasználók jogai, kötelezettségei, a rájuk vonatkozó tilalmak

1) A felhasználó jogosult: a Centrum informatikai infrastruktúráját a hálózati azonosító nevéhez hozzárendelt jogosultságok alapján munkaköri feladatai ellátásához használni,
2) A felhasználó köteles:
   - a felhasználókra vonatkozó szabályokat betartani,
   - az informatikai hálózatot rendeltetésszerűen és megfelelően használni,
   - az üzemeltető személyzet szóbeli, írásbeli tájékoztatását elfogadni,
   - a felfedezett informatikai problémákat az informatikai referens felé jelezni
   - a hibabejelentés rögzítéséhez szükséges, rendelkezésre álló minden adatot, információt megadni,
   - a saját hálózati azonosító nevét használni és az ehhez tartozó jelszót bizalmasan kezelni,
   - A Centrumon kívüli forrásból származó adatokon, vagy alkalmazásokon (CD, USB meghajtó stb.) a munkaállomásra, vagy a hálózatra való feltöltés előtt vírusellenőrzést végezni,
   - a vírusfertőzésre utaló jelek észlelését azonnal jelenteni és egyidejűleg a számítógépes munkavégzést felfüggeszteni,
   - a munkája során számítógépet használó felhasználó köteles az általa használt számítógépet és az ahhoz csatlakoztatott eszközöket:
     - rendeltetésüknek megfelelően, munkavégzés céljából,
     - a Centrum érdekeit szem előtt tartva jelen szabályzatban meghatározott módon használni
   - az informatikai eszközök használata során tilos:
     - az eszközt illetéktelen személynek átengedni,
     - az eszköz közelében folyadékot, éghető anyagot, és felette, alatta vagy rajta az eszköz rendeltetésétől eltérő anyagot, tárgyat elhelyezni és tárolni,
     - az eszközt a telepítési helyéről elmozdítani és elvinni (pl. irodai belső költözés) a kijelölt informatikus engedélye és közreműködése nélkül (kivételt képeznek a mobil eszközök), valamint

- az eszközök burkolatát megbontani tilos. Alkatrészt csak az informatikai referens helyezhet be az eszközbe, vagy szerelhet ki onnan.

21.§

A felhasználókra vonatkozó tilalmak:

- az informatikai szolgáltatások igénybevétele során jogszabályokba ütköző cselekmények megvalósítása, így különösen mások személyiségi jogainak megsértése, szerzői jogok megsértése,
- a hálózat, illetve erőforrásai működését megzavaró, veszélyeztető események szándékos előidézése,
- a hálózatot, illetve erőforrásait indokolatlanul, vagy pazarló módon igénybe vevő funkciók elindítása,
- a hálózat erőforrásaihoz, a hálózaton elérhető adatokhoz történő illetéktelen hozzáférés, azok illetéktelen használata, illetve az erre irányuló kísérlet,
- a hálózat erőforrásainak, a hálózaton elérhető adatoknak illetéktelen módosítására, megrongálására, vagy megsemmisítésére irányuló tevékenység végzése,
- a hálózat biztonságát veszélyeztető információk kiszolgáltatása, illetve programok terjesztése,
- jogszabályokba ütköző, mások vallási, etnikai, politikai vagy más jellegű érzékenységét sértő tevékenység végzése,
- mások munkájának indokolatlan és túlzott mértékű zavarása vagy akadályozása, különösen kéretlen levelek küldése,
- más felhasználók magánjellegű adatainak vagy dokumentumainak illetéktelen megtekintése, másolása,
- bármilyen jelszót másokkal megosztani,
- az informatikai eszközök meghibásodása esetén a hiba kijavítását megkísérelni, ennek érdekében meg kell tennie mindazokat az intézkedéseket, amelyekkel az infrastruktúrát további károsodásoktól megóvja. Ilyen esetben haladéktalanul értesíteni kell központ esetén az informatikai referenst.
- a felhasználónak — egyéb jogszabályi feltételek fennállása esetén — kártérítési kötelezettség terhe mellett
    - tilos a gépeket megbontani, a hardver konfigurációkat megváltoztatni
    - az informatikai berendezések közelébe nagyfeszültségű vagy erősen mágneses eszközt még időlegesen is elhelyezni,
    - a berendezéseket hőforrás mellé helyezni vagy bármilyen más módon sugárzó hőhatásnak kitenni,
    - a munkaállomásokon futó víruskeresőt leállítani vagy kiiktatni.

22.§

Mentések rendje

1) A Centrum fájlmegosztásra vonatkozó mentési folyamatok:
   A központi fájlmegosztón lévő adatokról az Informatikai Referens és a szerződött informatikai partner együtt biztosítja a mentést:
   a. Napi inkrementális mentés biztosítása:
      i. A mentés külön, a szervertől független hálózati tárolóra történik
      ii. A mentés nem fájlszintű, teljes virtuális szerverkép kerül mentésre. Az első mentés teljes, az utána következő mentések inkrementáltak.
      iii. A mentésből a fájlok azonnal visszaállíthatóak.
      iv. A biztonsági mentések megtartása: 14 napig minden napra teljes mentés, 8 hétig a heti utolsó mentés, 6 hónapig a havi utolsó mentés és 1 év utolsó mentése kerül megtartásra.
   b. Informatikai partner céghez történő mentés:
2) A Centrum által fenntartott weboldalakról (kivéve az NVSZC.hu weboldal) az informatikai referens készít és tárol el 6 hónapig havi biztonsági mentést.
3) A Centrumban található hálózati eszközök beállításainak mentéséről az informatikai referens és az informatikai partner cég közösen gondoskodik. Az informatikai partner gondoskodik a szerverek havi trezor mentéséről.

23.§

Szoftverek és hardver berendezések telepítése és folyamatos üzemeltetése

1) A Centrum számítógépes hálózatának szerverein, munkaállomásain csak jogtiszta szoftver telepítésére kerülhet sor.
2) Szoftvertelepítési feladatot az Informatikai Referens végezheti.
3) Az alapszolgáltatástól eltérő szoftverigényeket a vezető az Informatikai referens felé írásban jelezheti.
4) Szabad felhasználású szoftver esetén esetében az Informatikai Referens elvégzi a telepítést és a szoftver nyilvántartásba vételét.
5) Külső szállító cég szoftvertelepítést csak az Informatikai Referens felügyelete mellett végezhet.

24.§

1) A beszerzett hardver berendezések telepítésre történő előkészítése és a rendeltetési helyére való telepítése, a szükséges hardverbővítés, illetve csere az Informatikai Referens feladata. A feladatot indokolt esetben átadhatják a szállító részére, az Informatikai Referens felügyelete mellett.
2) A munkaállomások, nyomtatók, szkennerek hálózatba kapcsolásának, megbízható üzemeltetésének, működtetésének biztosítása az Informatikai Referens feladata.

25.§

Az informatikai hálózat fejlesztése és folyamatos üzemeltetése

1) A Centrumban az Informatikai Referens és az informatikai partner cég biztosítja az informatikai hálózatnak, mint rendszernek a megbízható működését, amely
   - a hálózati eszközök rendszeres ellenőrzésének és felügyeletének,
   - a hálózati topológia folyamatos megjelenítésének és a fizikai vagy virtuális LAN-ok működése áttekintésének, tervezésének,
   - hálózati eszközleltár elkészítésének és naprakészen tartásának,
   - a hatáskörébe tartozó berendezésekkel kapcsolatos hibabejelentések fogadásának és azok elhárításának,
   - a hálózati berendezések megelőző karbantartásának, tisztításának, valamint a szükséges konfiguráció módosításoknak az elvégzését jelenti.

Egyéb hálózati szolgáltatások

26.§

1) A Centrum által biztosított hálózaton csak az Informatikai referens üzemelhet be végpontokat, WIFI eszközöket.
2) A Centrum által üzemeltetett WIFI vendég hálózatot a Centrum dolgozói és vendégei használhatják.

27.§

Mobil eszközök használata

1) A mobil informatikai eszközről az arra felhatalmazott személy részére történő átadásakor az Informatikai referens átadás-átvételi nyilatkozatot készít, amely tartalmazza az eszköz szükséges adatait, az átadás-átvétel adatait.
2) Az informatikai referens a kiadott mobil eszközön elvégzi a Centrum hálózatának eléréséhez szükséges beállításokat.
3) A mobil eszközöket használó személyeknek:
   a. kötelező a SIM kártya PIN kódos védelem, valamint az időzárás és kizárólag jelszóval, PIN kóddal vagy biometriai azonosítóval feloldható képernyőzár használata, amennyiben a telefonon működő operációs rendszer rendelkezik erre alkalmas funkcióval (általános védelem).
   b. nem engedélyezett az eszközt gépjárműben, idegen helyen felügyelet nélkül hagyni,
   c. a Centrum területén kívül, idegen helyen történő tárolás esetén fokozott figyelmet kell fordítaniuk a jogosulatlan hozzáférés, az adatok esetleges módosítása, megrongálása, vagy ellopása elleni védelemre,
   d. nem engedélyezett az eszköz engedély nélküli átruházása vagy adatainak közlése,

e. nem engedélyezett megfelelő védelem nélkül idegen hálózathoz csatlakoztatni az eszközt, [pl. jelszó nélkül elérhető vezeték nélküli (Wi-Fi) hálózatok],

f. a mobil eszköz átadása más felhasználó (vagy illetéktelen személy) részére tilos, ezzel ellenkező esetben a felhasználó teljes felelősséggel tartozik a Centrummal szemben,

g. nem engedélyezett az eszközt bármilyen indokolatlan veszélynek kitenni vagy nem rendeltetésszerűen használni.

4) A Centrum informatikai rendszerébe kapcsolt munkaállomásokon csak olyan adathordozót lehet használni, arról adatokat beolvasni, amelyen előtte a rendszeresített és telepített víruskereső programmal vírusellenőrzést végeztek.
5) A mobil infokommunikációs eszközök, mobil adathordozók felhasználói felelősek az eszközön található adatok esetleges kiszivárgásáért, az eszköz elvesztéséért, eltűnéséért, megsérüléséért. A mobil infokommunikációs eszközök, mobil adathordozók eltűnése, ellopása esetén annak tényét a felhasználónak haladéktalanul jelentenie kell a szükséges intézkedések megtétele érdekében.

28.§

INFORMÁCIÓBIZTONSÁGI ELJÁRÁSOK

Általános irányelvek

1) Az egyes felhasználói azonosítókhoz rendelt jogosultságok minden esetben csak az adott munkakör, feladat ellátásához szükséges minimális funkcióelérést biztosíthatják.
2) Amennyiben a felhasználó jogviszonya előreláthatólag három hónapot meghaladóan szünetel, vagy a felhasználó a munkavégzésben előreláthatóan ennyi ideig nem vesz részt, a hozzáférést megalapozó jogviszonyából eredő feladatát tartósan nem látja el, a felhasználói azonosítóját fel kell függeszteni (inaktiválni kell) a munkába állás, az adott tevékenység folytatása napjáig. Az inaktiválást a közvetlen vezető, illetve a szerződéskötést kezdeményező tagintézmény vezetőjének hatásköre. A felhasználói azonosító újra aktiválási igényének felmerülésekor a hozzáférés helyreállítását szintén a közvetlen vezető, illetve a szerződéskötést kezdeményező vezetőjének hatásköre.
3) A felhasználók szervezeten belüli áthelyezése kapcsán felmerülő jogosultsági változásokat a felhasználó vezetője intézi.
4) A számítógépes munkaállomások képernyőit (monitor) úgy kell elhelyezni, hogy az azon megjelenő információkat illetéktelen személy ne láthassa.
5) A munkaállomás beállításait adminisztrátori jelszóval kell védeni módosítás ellen.

29.§

Az informatikai biztonsági események felismerése, jelentése

1) Minden felhasználó kötelessége – amennyiben kellő gondossággal eljárva azt felismerhette – a lehetséges legrövidebb időn belül közvetlen vezetőjének bejelenteni

minden olyan veszélyforrást, amely az elektronikus információbiztonságra nézve érdemi fenyegetést jelent vagy jelenthet.

2) A felhasználó részéről különösen a következő veszélyforrások jelzése kötelező:
   - az Informatikai szabályzatban, a vonatkozó jogszabályokban előírt elektronikus információbiztonsági rendszabályok lényeges megszegése, illetve ennek gyanúja,
   - a felismert vagy felismerni vélt, az elektronikus információbiztonságot lényegesen veszélyeztető esemény, ezen belül különösen:
     1. nem nyilvános adat illetéktelen személy általi megismerése,
     2. informatikai rendszerekben tárolt adatok illetéktelen személyek általi megváltoztatása, törlése vagy hozzáférhetetlenné tétele,
     3. informatikai rendszer működésének, használatának jogosulatlan akadályozása,
     4. nem engedélyezett vagy licenc-szel nem rendelkező szoftver telepítése,
     5. felhasználói jelszavak egymás közötti megosztása, hozzáférhetővé tétele,
     6. vírusfertőzés, kémprogramok, billentyűzetleütést figyelő alkalmazások megjelenése,
     7. informatikai rendszereket érintő (vagy vele összefüggésbe hozható) bármilyen esemény (betörés, tűz, víz, villámcsapás lopás, elvesztés stb)

fentiek bármelyikére tett kísérlet (a továbbiakban együtt: biztonsági események).

30.§

1) Nem számít informatikai biztonsági eseménynek az informatikai hiba, meghibásodás vagy rendszeresemény, amely nem érinti az informatikai szolgáltatások minőségét és azt az üzemeltetők képesek megoldani.
2) A bejelentés során minimálisan megadandó információk:
   a. az informatikai biztonsági esemény pontos leírása,
   b. érintett informatikai szolgáltatás pontos megnevezése,
   c. érintett informatikai eszköz gyári száma, leltári száma, típusa,
   d. tagintézmény neve, pontos címe (emelet, ajtó),
   e. észlelő neve, elérhetősége (opcionális),
   f. A vezető által kijelölt helyszíni kapcsolattartó neve, elérhetősége.

31.§

Biztonsági események kivizsgálása

1) A biztonsági eseményeket soron kívül ki kell vizsgálni. A vizsgálatot az Informatikai referens folytatja le, szükség szerinti mértékben bevonva az NVSZC szervezetét.
2) A vizsgálat eredményét az Informatikai referens írásban dokumentálja, amelyből 1-1 példányt kap a Centrum, illetve a biztonsági eseményben közvetlenül érintett(ek).

31.§

A biztonsági szabályok megszegésének következményei

1) Az informatikai biztonsággal kapcsolatos szabályok megszegése esetén a szabályszegőkkel szemben érvényesítendő jogkövetkezmények tekintetében elsősorban annak súlyosságára tekintettel vagy etikai, vagy munkáltatói fegyelmi jogkörben kell eljárni.
2) Az információbiztonsággal kapcsolatos szabályok súlyos megszegése vagy annak gyanúja esetén az Informatikai referens javaslatára az érintett foglalkoztatott közvetlen vezetője, illetve az utasítási joggal rendelkező vezető véleményének kikérésével – az Kancellár jogosult a megfelelő jogkövetkezmények érvényesítése érdekében eljárást indítani, illetőleg eljárás megindítását kezdeményezni.

32.§

Oktatás

3) A foglalkoztatottakat a Centrumban végzendő tevékenység megkezdése előtt informatikai biztonsági képzésben kell részesíteni.
4) Az informatikai biztonságra vonatkozó jogszabályi környezet megváltozásakor, továbbá ha az NVSZC informatikai biztonságát, illetve a szabályzat tartalmát érintő jelentős változás következik be, a változását követő 60 napon belül a felhasználókat informatikai biztonsági továbbképzésben, a külső felhasználókat informatikai biztonsági tájékoztatásban kell részesíteni (a továbbiakban együtt: oktatás).
5) Az oktatás tematikájának összeállításáért az Informatikai referense felelős, az oktatás megszervezéséért, végrehajtásáért a Centrum vezetője a felelős.
6) Az oktatást végző személy az oktatáson részt vett személyekről olvashatóan kitöltött Jelenléti ívet készít, melyet az Centrum vezetőjének átad.
7) Az NVSZC informatikai rendszereihez, a rendszerekben tárolt adatokhoz kizárólag a Biztonsági oktatásában részesült személyek férhetnek hozzá. Az oktatás hiányában hozzáférési jogosultság nem kérhető.
8) A külső felhasználók e szabályzattal való megismertetése a szerződéskötést kezdeményező szervezeti egység vezetőjének feladata és felelőssége.

33.§

Záró rendelkezések

A szabályzat 2025. március 31-én lép hatályba.
Az érintett dolgozók munkaköri leírásában szerepeltetni kell a nevesített felelősségi, hatás és jogköröket, melyek elkészítéséért a kancellár a felelős.
A szabályzat kiadásáért és aktualizálásáért a kancellár a felelős.

A szabályzat megismertetése A Nógrád Vármegyei Szakképzési Centrum Belső Kontrollrendszer Szabályzatának megfelelően a Nógrád Vármegyei Szakképzési Centrum hivatalos honlapján történő közzététellel történik.

Salgótarján, 2025. március 31.

Gembiczki Ferenc
kancellár

1.sz melléklet

Jogosultság igénylő/módosító a Nógrád Várvármegyei Szakképzési Centrumban dolgozó részére

Név:
Beosztás:
Telefonszám:

Felhasználónév	
Csoportok	□TITKÁRSÁG, □GAZDASÁGI, □TITKÁRSÁG-GAZDASÁGI, □REFERENSEK, □FELNŐTTKÉPZÉS, □VIZSGAKÖZPONT, □MŰSZAKI, □ESZKÖZ, □RRF, □AKK, □N-KORT, □GINOP, □FELNŐTTEK OKTATÁSA, □INFORMATIKA, □VEZETŐI, □TITKÁRSÁG-FELNŐTT
E-mail cím	
Office 365 dolgozói hozzáférések	
Egyéb hozzáférések (Poszeidon, SAP, KIRA stb…)	□Poszeidon, □SAP, □KIRA, □Kréta, □Posta, □FAR, □KEF portal, □IDPR, □Educert, □Front-end, □KKVTR, □Egyéb
VPN használat	

Salgótarján, ...

.....
Vezető

Az igényelt jogosultságok létrehozása megtörtént, a jelszavak átadása megtörtént a felhasználó részére. A kért VPN használat beállításra került a felhasználó számítógépén.

Salgótarján,

....
Átvevő Informatikai referens

2.sz melléklet

Jogosultság törlő a Nógrád Várvármegyei Szakképzési Centrumban dolgozó részére

Név:
Beosztás:
Telefonszám:

Felhasználónév	
Csoportok	□TITKÁRSÁG, □GAZDASÁGI, □TITKÁRSÁG-GAZDASÁGI, □REFERENSEK, □FELNŐTTKÉPZÉS, □VIZSGAKÖZPONT, □MŰSZAKI, □ESZKÖZ, □RRF, □AKK, □N-KORT, □GINOP, □FELNŐTTEK OKTATÁSA, □INFORMATIKA, □VEZETŐI, □TITKÁRSÁG-FELNŐTT
E-mail cím	
Office 365 dolgozói hozzáférések	
Egyéb hozzáférések (Poszeidon, SAP, KIRA stb…)	□Poszeidon, □SAP, □KIRA, □Kréta, □Posta, □FAR, □KEF portal, □IDPR, □Educert, □Front-end, □KKVTR, □Egyéb
VPN	

Salgótarján, ...

.....
Vezető

Az igényelt jogosultságok törlése, felfüggesztése és az e-mail fiókok tartalmának és a felhasználó dokumentumainak mentése megtörtént.

Salgótarján,

.....
Átvevő

.....
Informatikai referens

3.sz melléklet

Megosztott postaláda igénylő lap

Megosztott postaláda neve:	
Megosztott postaláda címe:	
Megosztott postaládához hozzáadandó felhasználó	
Megosztott postaládából eltávolítandó felhasználó	

Salgótarján, ...

.....
Vezető

Az igényelt megosztott postafiók létrehozása megtörtént, a felhasználók hozzáadásra/törlésre kerültek.

Salgótarján,

.....
Informatikai referens