A

Református EGYMI

INFORMATIKAI BIZTONSÁGI SZABÁLYZATA

2025

Tartalomjegyzék

A szabályzat célja

A jelen **Informatikai Biztonsági Szabályzat** (a továbbiakban: IBSZ) célja, hogy a Református EGYMI-ben működő informatikai rendszerek, eszközök üzemeltetését, használatát, ellenőrzését, valamint az információbiztonság fenntartását egységes szabályrendszer keretében szabályozza.

Hatálya kiterjed minden, az Intézmény tulajdonában vagy használatában lévő eszközre, szoftverre, azokon történő adatkezelésre, valamint minden felhasználóra, aki az Intézmény informatikai erőforrásait igénybe veszi.

A szabályzat az Általános Adatvédelmi Rendelettel (GDPR), a Református EGYMI Adatvédelmi Szabályzatával, valamint az Iratkezelési Szabályzattal összhangban került kialakításra.

Ha az Intézmény lehetőséget biztosít harmadik félnek informatikai rendszereit, eszközeit használni, számára is kötelező ezen szabályzatban foglaltakat betartani.

A felhasználók a szolgáltatások, eszközök használatának során a személyes adatok kezelésével kapcsolatban az Általános Adatvédelmi Rendelet[1] és a Református EGYMI Adatvédelmi és Adatkezelési Szabályzatában foglaltaknak megfelelően került kialakításra. Egyéb adatvédelmi kérdés az előbb említett dokumentumban található.

Ezen dokumentumban nem szabályozott kérdésekben a Református EGYMI Iratkezelési szabályzata, és a Református EGYMI Honvédelmi Intézkedési Tervében foglaltak szerint kell eljárni. További kapcsolódó szabályozások, amelyeket összhangban kell alkalmazni ezen dokumentummal:

- Szervezeti és működési szabályzat
- Pedagógiai program
- Munkaterv
- Házirend
- Különös közzétételi lista

[1] https://net.jogtar.hu/jogszabaly?docid=A1600679.EUP

Tárgyi hatálya

Az IBSZ tárgyi hatálya kiterjed

- minden, az Intézmény tulajdonában álló vagy általa használt informatikai eszközre (PC, notebook, szerver, router, modem, tűzfal, okostelefon, táblagép);
- a használt operációs rendszerekre, szoftverekre, felhasználói programokra;
- a felhasználó által végrehajtott hardveres vagy szoftveres módosításokra;
- az adatmentési és visszatöltési eljárásokra;
- az Intézmény informatikai rendszereit használó külső felekre.

Értelmező rendelkezések[2]

Székhelyintézmény: az alapító okiratban meghatározott, a köznevelési intézmény alaptevékenységének ellátását szolgáló feladatellátási hely, ahol a köznevelési intézmény képviseleti jogának gyakorlására jogosult vezető munkahelye található.

Tagintézmény: a székhelyen kívül (ez lehet azonos is és más településen is, továbbá saját vagy bérelt tulajdonú) működő, azonos vagy különböző feladatot ellátó intézményegység, ha a székhelytől való távolság, a feladatok jellege miatt az irányítási, képviseleti feladatok a székhelyről nem, vagy csak részben láthatók el.

Telephely és munkaállomás: a székhelyen kívül, az alapító okiratban meghatározott (saját vagy bérelt tulajdonú), működő szervezeti egység (kihelyezett osztály, oktatási csoport, műhelyfoglalkozás stb.) elhelyezését szolgáló feladatellátási hely.

Gazdasági Hivatal biztosítja az intézmény gazdasági és pénzügyi tervezését, ellátja és koordinálja a gazdálkodást, a számvitelt, és az ezek alapjául szolgáló bizonylati rendszert, valamint az ezzel kapcsolatos ügyvitelt.

Munkaügyi Csoport biztosítja az intézmény munkavállalói részére a bérekkel kapcsolatos információk összegyűjtését, ellenőrzését és feldolgozását, valamint a munkavállalóknak járó bérek és egyéb juttatások kiszámítását.

Személyi számítógép (PC): olyan számítógép, amely nem egy központi számítógép terminálja (munkaállomása), hanem önálló, egyetlen személy (az ún. végfelhasználó)

[2] Forrás: https://hu.wikipedia.org/

által kezelt, kisebb méretű gép saját billentyűzettel, egérrel, processzorral, operatív memóriával és monitorral.

Laptop, notebook: ezek teljes értékű PC-k, az asztali változatokhoz képest a lényegi különbség a kompakt formai kivitelezésben és a hordozhatóságban rejlik. Ugyanazokat a funkciókat betöltő alkatrészekből épülnek fel, azonban jellemzően kisebb méretűek.

Szerver: az informatikában olyan (általában nagy teljesítményű) számítógépet vagy szoftvert jelent, ami más számítógépek számára a rajta tárolt vagy előállított adatok felhasználását, a szerver hardver erőforrásainak (például nyomtató, háttértárolók, processzor) kihasználását, illetve más szolgáltatások elérését teszi lehetővé.

Okostelefon: Okostelefonnak nevezzük a fejlett, gyakran PC-szerű funkcionalitást nyújtó mobiltelefonokat.

Táblagép, tablet: hordozható számítógép, amelyet leginkább tartalomfogyasztásra fejlesztettek ki. Ezeknek az eszközöknek a legfeltűnőbb jellegzetessége a lapos formai kialakítás és az igen nagy kijelzőfelület.

Operációs rendszer: OP rendszernek nevezzük a számítástechnikában a számítógépeknek azt az alapprogramját, mely közvetlenül kezeli a hardvert, és egy egységes környezetet biztosít a számítógépen futtatandó alkalmazásoknak.

Hardver: a számítógép fizikailag megfogható részeinek összességét értjük. A számítógép működéséhez alapvetően hardver és szoftver szükséges.

Szoftver: alatt a legszűkebb értelemben elektronikus adatfeldolgozó berendezések (például számítógépek) memóriájában elhelyezkedő, azokat működtető programokat értjük.

Fájl: adatállománynak, állománynak vagy fájlnak nevezzük a logikailag összefüggő adatok halmazát, tömbjét. Adatfájl például egy képfájl, egy szövegfájl vagy egy adatbázisfájl.

Tűzfal: célja a számítástechnikában annak biztosítása, hogy a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás.

Felhasználó: az a személy, aki a hardver és szoftver elemeket munkájához használja, adatokat rögzít, tárol, keres, feldolgoz.

Legális szoftver: az a kereskedelmi forgalomban vásárolt program, amelyet a felhasználó érvényes licenc jogokkal használ.

Licenc: a számítógépes programokat szerzői jogi törvény védi, amely kimondja, hogy az ilyen műveket tulajdonosának engedélye nélkül tilos másolni. A szoftver licenc jogosítja fel a felhasználót a szoftver alkalmazására. A felhasználó csak a használat jogát birtokolja, és nem magát a szoftvert.

Freeware: ingyenesen használható szoftver.

Illegális szoftverhasználat: azt jelenti, hogy valaki egy számítógépes programot jogosulatlanul másol le, használ, terjeszt, ezzel megsértve a szerzői jogi törvényt, valamint a szoftver licenc-szerződésben leírt feltételeket. Aki szoftvert illegálisan használ, az a szerzői jogi törvény értelmében, törvénybe ütköző cselekedetet követ el.

Weblap (vagy weboldal) egy olyan számítógépes dokumentum, mely megfelel a World Wide Web számára, és alkalmas arra, hogy egy webböngésző megjelenítse. A webböngésző a weblapot monitoron vagy mobil eszközön jeleníti meg. A weboldal általában a dokumentum látható elemeit foglalja magába, de a weblap szó jelentheti magát a számítógépen tárolt fájlt is, melyet általában HTML vagy más hasonló leíró nyelven írtak meg.

Személyes adatnak minősül egy természetes személlyel kapcsolatba hozható minden adat, valamint az adatból levonható, az érintettre vonatkozó következtetés.

TeamViewer[3] egy távelérési és távirányítású számítógépes szoftver, amely lehetővé teszi a számítógépek és egyéb eszközök karbantartását. (Regisztrált márkanév, a TeamViewer a német TeamViewer AG cég tulajdonában áll)

OpenVPN (Virtual Private Network, azaz a virtuális magánhálózat rövidítése) biztonságos kapcsolatot hoz létre a székhelyintézmény és a felhasználó között. VPN csatlakozás esetén, az internetes tevékenység titkosítva van, így az adatfeldolgozás során megbízhatóan töltődnek fel a központi szerverre a fájlok a távoli tagintézményekből/telephelyekről.

[3] https://www.teamviewer.com/hu/

Feladatellátási helyek

A Református EGYMI egységei a következő épületekben találhatók meg:

Név	Cím	Státusz
Székhelyintézménye	2314 Halásztelek, Hold utca 6.	Székhelyintézmény
Gazdasági Hivatala	2314 Halásztelek, Hold utca 4.	Munkaállomás
Munkaügyi Csoport	6400 Kiskunhalas, Székely u. 3. 2/23.	Munkaállomás
Csurgói Telephelye	8840 Csurgó, Csokonai utca 22.	Telephely
Makói Telephelye	6900 Makó, Tulipán utca 3/A.	Telephely
Verőcei munkaállomása	2621 Verőce, Rákóczi út 41.	Telephely
Miskolci Tagintézménye	3531 Miskolc, Füzes utca 27.	Tagintézmény
Miskolci Telephelye	3527 Miskolc, Éder György utca 1.	Telephely
Tatai Tagintézmény	2890 Tata, Agostyáni utca 7.	Tagintézmény
Tatai Telephelye	2890 Tata, Agostyáni utca 1-3	Telephely
Debreceni Tagintézménye	4032 Debrecen, Bartha Boldizsár utca 9.	Tagintézmény
Békési Telephelye	5630 Békés, Petőfi Sándor utca 6.	Telephely
Tiszafüredi Telephelye	5350 Tiszafüred, Bajcsy-Zsilinszky út 50/a.	Telephely
Berettyóújfalui Telephelye	4100 Berettyóújfalu, Herpály utca 3.	Telephely
Nagyhalászi Telephelye	4485 Nagyhalász, Arany János utca 75.	Telephely
Budapesti Tagintézménye	1093 Budapest IX. kerület, Bakáts utca 1-3. félemelet 4.	Tagintézmény
Kiskunhalasi Tagintézménye	6400 Kiskunhalas, Szabó Ervin utca 15.	Tagintézmény
Igali Tagintézménye	7275 Igal, József Attila utca 45.	Tagintézmény

**A nem saját internetes hálózattal rendelkező épületek esetében, a létesítményben már meglévő szakember/rendszergazda által felügyelt/létrehozott hálózatot használják a munkavállalók.*

A Református EGYMI biztonsági szintje

A 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló rendelet alapján, a Református EGYMI biztonsági szintje:

a 2. biztonsági osztályba sorolható.

Informatikai menedzsment

Az Intézmény informatikai tevékenységének szabályozását és koordinálását megfelelő végzettséggel és tapasztalattal rendelkező belső munkatársak látják el.

Feladatuk a fejlesztő-nevelő oktató munkatársak, adminisztrátorok, pedagógiai munkát segítők támogatása telefonon, e-mailen, egyéb elektronikus formán keresztül, mely elősegíti munkájuk elvégzését, esetleges elakadásuk esetén segít a probléma elhárításán, továbbá az Intézmény informatikai biztonsági követelményeinek betartatása. Egyéb feladatai:

- a hozzáférési jogosultságok megadásának és visszavonásának kezdeményezése ***(4. melléklet)***;
- a felhasználók saját maguk által telepített szoftverek ellenőrzése (legális, nem legális szoftverhasználat felderítése, esetlegesen illegális fájlcserélés felfedése);
- részvétel a rendellenes használattal kapcsolatos ügyek kivizsgálásában;
- tájékoztatás a tagintézmény-igazgatója felé, majd ezt követően a főigazgató felé.

Hatásköre a biztonsági és egyéb informatikai üzemeltetési kérdésekre, továbbá az informatikai hálózati szolgáltatások (hálózat, wifi, tűzfal) szakmai felügyeletére is kiterjed. További feladatai:

- kiadott programjavítások telepítése;
- kapcsolattartás a support cégekkel;
- adatmentések kezelése, végrehajtása;
- operációs rendszerek telepítése, szerverek alapkonfigurációjának beállítása;

- hálózati konfigurációk, tűzfalszabályok kialakítása;
- hálózati címkiosztási rend, alhálózatok meghatározása;
- következtetések levonása, javaslattétel a Főigazgató és Gazdasági Hivatal felé.

Felelősség-, feladat- és hatáskörök

Az összes üzemeltett eszköz, számítógép esetében az IBSZ-nek való megfelelés az adott Intézményi egység (székhelyintézmény, tagintézmény, telephely, munkaállomás) vezetőjének, vezetőhelyettesének, egységvezetőnek a felelőssége.

A Református EGYMI stratégiájába illő nagyobb fejlesztések, beruházások, informatikai szolgáltatások körébe tartozó döntéshozó tevékenység kizárólag a Főigazgató és a Gazdasági Hivatal igazgatójának közös határozatával történik.

Az Intézményi informatikai hálózatok igénybevétele során elkövetett bűncselekményekért, illetve egyéb jogsértésekért a szolgáltatást, eszközt igénybe vevő felhasználó büntetőjogi felelősséggel tartozik.

A Református EGYMI Adatkezelési és Adatvédelmi Szabályzatában foglaltaknak megfelelően az Intézmény tulajdonában lévő internetes hálózatán (tűzfalán) nem gyűjt, tárol személyes adatot, továbbá nem naplózza a megtekintett weboldalakat. A munkavállalóhoz kötődő személyes adat, adatfájl kizárólag a felhasználó számítógépén keletkezik, melyet a Református EGYMI nem tekint meg, továbbá ezeket nem tárolja; viszont, ha a munkaviszony megszűnik, a teljes merevlemez törlésére sor kerül. Kivételt képez a törlés alól a munkájával összefüggésbe hozható fájl, adatbázis mentése.

Ezen szabályzatban foglaltak megsértése esetén – az esemény súlyától függően – az alábbi szankciók sújthatják a felhasználót:

1. Eszköz visszaszolgáltatása az Intézmény részére, használatának megtagadása
2. Okozott anyagi, szellemi kár megtérítése
3. Eljárás kezdeményezése a Református EGYMI fegyelmi szabályzata alapján
4. Polgári jogi eljárás kezdeményezése, vagy büntető feljelentés megtétele

A fentebb felsorolt szankciók csak akkor történhetnek meg, ha az Intézmény Főigazgatója dokumentáltan bejelentette a szankció elrendelését, és ennek kiváltó okát.

Nem büntetőjogi események bejelentése közvetlenül is történhet a tagintézmény-igazgatónak, továbbá az informatikai menedzsment részére is.

Azonosítás és hitelesítés (intézményen belüli felhasználók)

Az intézmény hálózati erőforrásai által nyújtott szolgáltatások azonosításának és hitelesítésének a módját (hitelesítés módja, alkalmazott eszközök, fiókzárolás, munkamenetek kezelése) az Informatikai Menedzsment határozza meg.

A Székhelyintézményben és a Munkaügyi Csoportban valamennyi elektronikus információs rendszernek egyedileg kell azonosítani és hitelesítenie az Intézmény valamennyi felhasználóját, és a felhasználók által végzett tevékenységeket.

Ennek érdekében egyénre szóló felhasználói azonosítókat kell létrehozni, a csoportos azonosítók használata nem engedélyezett a „kiemelt felhasználói szoftverek”[4] esetében.

Azonosító kezelés

Az elektronikus információs rendszerekhez történő hozzáférést biztosító azonosítókat az Informatikai Menedzsment hozza létre. Az azonosítók ismételt felhasználása nem engedélyezett.

Hitelesítésre szolgáló eszközök kezelése

A jelszavak a felhasználó számítógépes szolgáltatásokhoz való hozzáférési jogosultságának hitelesítésére szolgálnak. A jelszókezelő rendszernek hatékonyan és interaktívan kell biztosítani a megfelelő színvonalú jelszavak használatát.

A hálózati adattároló jelszókezelő rendszere feleljen meg a következőknek:

a) tegye lehetővé a felhasználók számára jelszavuk kiválasztását és megváltoztatását
b) kényszerítse ki a megfelelő minőségű jelszavak használatát
c) tiltsa meg a korábban használt jelszavak ismételt felhasználását
d) beíráskor ne jelenítse meg a jelszavakat a képernyőn

[4] ezen szabályzat „Adatmentések kezelése és végrehajtása” pontjában felsorolt alkalmazások

e) jelszóadatbázist kódolva tárolja.

Jelszógondozási folyamattal kell a jelszavak kiosztását ellenőrizni úgy, hogy:

a) szükség esetén a felhasználók kötelezhetők arra, hogy nyilatkozatban vállalják a számukra kiadott, vagy általuk képzett jelszavak titokban tartását
b) biztosítani kell, hogy a kezdeti vagy végleges jelszavak is biztonságos körülmények között kerüljenek a felhasználóknak átadásra.

A felhasználói jelszavak képzéséhez az alábbi szabályokat kell betartani:

a) a jelszó legalább nyolc karakter hosszú legyen, és – ahol ez műszakilag megengedett – törekedni kell arra, hogy tartalmazzon a kisbetűkön kívül nagybetűt és számot
b) zárolás esetén előre beállított időtartam eltelte tán engedélyezze vissza a felhasználói fiókot.

Felhasználó felelősségi köre jelszóhasználat során

A jelszavak használatának részletes szabályai a következők:

- a felhasználó a jelszavát köteles titokban tartani
- a felhasználó felelőssége, ha jelszavának megismerése révén valaki a nevében visszaélést követ el az elektronikus információs rendszerben
- a jelszót tilos leírni
- ha bármilyen jel arra mutat, hogy a jelszó illetéktelen kézbe jutott, azonnal meg kell változtatni és értesíteni kell a felettest, majd az Informatikai Menedzsmentet
- a jelszó nem tehető egy automatikus bejelentkezési folyamat részévé (pl. makróra, vagy egyéb előre beállítható funkció billentyűre)

A jelszó minél összetettebb, annál kisebb a valószínűsége, hogy a nevünkben visszaélést követnek el. Ennek érdekében az alábbi szempontokat kell betartani:

- könnyen megjegyezhető ellenben nehezen kitalálható legyen
- semmi olyasmin ne alapuljon, aminek alapján valaki kitalálhatja (saját név, telefonszám, születési dátum)
- ne legyen a gép közelében címkén, egyéb papíron leírva

A fenti szabályok az elektronikus információs rendszerek által technikailag kikényszeríthető részét az Informatikai Menedzsmentnek kell beállítani.

A felhasználó felelőssége, ha jelszavának neki felróható mulasztása miatti megismerése révén, valaki a nevén visszaélést követ el.

Felhasználó jogai, feladatai

A felhasználó alanyi jogon rendelkezik:

- a felhasználói nevével és jelszavával a jogosultsági szintjének megfelelő Intézményi informatikai erőforrásokhoz való hozzáféréssel (létezik olyan munkakör az Intézményben ahol nem kap a felhasználó semmilyen jogosultságot);
- a @refegymi.hu e-mail címmel, és az ezen címet kiszolgáló levelező rendszer használatával;

A felhasználó feladatai:

1. **IT hálózati rendszerek megfelelő használata, részletezve:**
   1.1. tilos a vezetékes vagy vezetéknélküli hálózat adatforgalom figyelése, ebből következően profilalkotása, jelszó eltulajdonítása, személyes adatok lemásolása
   1.2. tilos túlterheléses támadás indítása
2. **az Intézmény által biztosított eszközök megfelelő használata; továbbá:**
   2.1. tilos a számítógép házának felnyitása
   2.2. tilos a hardveres elemek eltávolítása, kicserélése, rongálása
   2.3. tilos folyadék öntése szándékosan az elektronikai eszközre
   2.4. tilos hirtelen hőmérsékletingadozások kitenni a berendezéseket
   2.5. tilos a szellőzőnyílások eltakarása, elzárása
3. **az Intézmény által biztosított szoftverek megfelelő használata, mely részletezve:**
   3.1. csak jogtiszta szoftverek használatára jogosult a felhasználó
   3.2. tilos szerzői jogvédelem alatt álló fájlok cserélését lehetővé tévő szoftverek telepítése
   3.3. egyéb nem munkájához köthető szoftverek rendszeres használata
   3.4. a Microsoft Windows operációs rendszer allicenc kulcsának felfedése, ennek terjesztése, értékesítése
   3.5. a Microsoft Office irodai programcsomag allicenc kulcsának felfedése, ennek terjesztése, értékesítése
   3.6. nem alkalmazhatja személyes családi fotók, videók, egyéb fájlok (munkájához nem köthető) hosszantartó tárolására
   3.7. tilos kriptovaluta bányászatra használni az erőforrásokat

Asztali számítógép, laptop használata

1. Intézményünkben leggyakrabban használt típus a hordozható számítógép, a munkatársak ezen keresztül veszik igénybe a hálózatot, érik el az internetet, nyomtatót, tartják a kapcsolatot egymással
2. Minden eszköz esetében az operációs- és vírusvédelmi rendszer frissítését el kell végezni, melyet automatikusan kínál fel az eszköz, ennek elhalasztása a felhasználó által tilos, ha nem tudja végrehajtani, akkor a Székhelyintézménybe kell szállítani az eszközt, és az informatikai menedzsment feladata ennek elvégzése
3. Külső hálózatok elérése az adott tagintézmény központi tűzfalán keresztül lehetséges, ha ilyen nem található, akkor az internetszolgáltató által biztosított modem/router segítségével történik
4. Hardverbeépítés vagy csere esetén az informatikai menedzsmenttel egyeztetve kell eljárni
5. A felhasználók eszközeiket kötelezően el kell látniuk jelszóvédelemmel, ha ez a jelszó nem az informatikai menedzsment által kiadott, akkor írásbeli tájékoztatást kell adnia a munkavállalónak, hogy az eszköz felügyeletét, frissítését el lehessen látni
6. Az eszközöket zárolni kell, ha a felhasználó felügyelet nélkül hagyja számítógépét
7. Egyéb munkakör ellátásához, gyermek fejlesztéséhez szükséges szoftver telepítését az informatikai menedzsment közreműködésével szükséges végrehajtani (licenc meglétének ellenőrzése után)
8. Az eszközök merevlemezén személyes adatot csak a feldolgozás ideje alatt lehet tárolni, a munka befejezése, vagy hosszabb időre történő megszakítása esetén az adatokat az adott tagintézmény, vagy a székhelyintézmény központi rendszerében kell megfelelően tárolni, ezután a helyi merevlemezről törölni kell az adatfájlokat
9. Otthoni munkavégzés és más köznevelési intézményben történő munkavégzés megengedett, és szükséges is, az egységes módszertani intézmény és az utazó pedagógiai szakszolgálati tevékenységek felépítése miatt
10. Központi belső hálózatra távoli bejelentkezés csak az intézmény tulajdonában lévő eszközről lehetséges, melyet a nyílt forráskódú OpenVPN-nen keresztül érnek el
11. Az informatikai menedzsment fenntartja a jogot, hogy a számítógép asztalára betekintést nyerjen a TeamViewer (regisztrált márkanév) nevű szoftver segítségével, ezzel elősegítve a gyors problémamegoldást, áthidalva a nagy kiterjedésű intézményhálózat akadályait. Ezen szoftver nem gyűjt és tárol

személyes adatot (GDPR megfelelőségi nyilatkozat elérhetősége https://www.teamviewer.com/en/gdpr/), kizárólag az aktuális feladat megoldását hivatott elérni, tovább az informatikai menedzsment felelőségteljesen, és etikusan használja az említett szoftvert.

Okostelefonok használata

1. Okostelefonok kiválasztásánál az alkalmasságot is ellenőrizni kell, minimális követelmény szinteket kell meghatározni, továbbá a munkakörhöz kapcsolódó igényeket is figyelembe kell venni.
2. Főigazgatói döntés alapján egyes munkavállalók jogosultak az Intézmény tulajdonát képező mobiltelefon használatára. Egyedi elbírálást követően, átadás-átvételi (1. melléklet) nyilatkozattal vehetik át a munkavállalók a készüléket felettesétől vagy az Informatikai Menedzsmenttől, amelyért teljes anyagi felelőséggel tartoznak. Az Informatikai Menedzsment köteles az Intézmény mobiltelefon-készülékeinek nyilvántartására, amelynek tartalmaznia kell:
    a. felhasználó nevét
    b. készülék típusát
    c. készülék IMEI számát
    d. készülék SIM kártyájának számát
3. A munkavállaló kilépéskor köteles a mobiltelefont SIM kártyával együtt a felettese vagy az Informatikai Menedzsment részére átadni, ahol ellenőrzik a készülék működését és állapotát. Ezt követően kitöltik közösen, az átadás-átvevő nyilatkozat alján található "visszavét dátumát”, melyet aláírásukkal igazolnak.
4. A Főigazgató a munkakörökhöz különböző értékhatárban engedélyezi a mobiltelefon-készülék beszerzést, melyet mindig a Gazdasági Hivatal igazgatójával együttesen határoznak meg.
5. Szervezetünk engedélyezi saját mobiltelefon használatát céges SIM kártyával.
6. Saját e-mail tárhelyük elérése engedélyezett ezen eszközökről.
7. Az Intézmény informatikai hálózatából adódóan a központi szerveren tárolt fájlokat, iktatást, könyvelési adatbázist, mobiltelefon használatával elérni nem lehet. Továbbá a gyereknyilvántartásra készült I.M.S.[5]-t sem tudják használni.

[5] Pedagógiai gyereknyilvántartó alkalmazás

Ezeket kizárólag laptopról vagy asztali munkaállomásról titkosított csatornán érhetik el.

8. Ahogyan fentebb említett eszközök esetében is, a felhasználó felelőssége, ha jelszavas védelmet nem állít be, továbbá jelszavának neki felróható mulasztása miatti megismerése révén, valaki a nevén visszaélést követ el.

Adatgyűjtés

1. Az Intézmény semmilyen személyes adatot nem gyűjt a felhasználás során, adatot a központ felé nem továbbít, teljes mértékben betartva az Általános Adatvédelmi Rendeletet[6].

Információvédelem felhasználóknak

1. Ha van rá mód akkor nyilvános helyen mobilnetet kell használni és kizárólag Intézményeinkben (saját internetes hálózattal rendelkező épületekben), vagy otthon állítsuk át a telefonokat a biztonsági jelszóval ellátott Wi–Fi hálózatra.
2. Soha ne töltsünk le játékokat, ingyenes szoftvereket. További biztonsági szint növelés érhető el ha az alkalmazások kezelő paneljében beállítjuk, hogy milyen adatokhoz férhessen hozzá az adott program.

Számlázás és egyéb díjak

1. A céges mobiltelefon használatra flotta-kedvezmény jár, a munkavállalók egymás között ingyen telefonálnak.
2. A mobiltelefon számlák igazolására, kiállítására a Magyar Református Egyház Egyházi Ügyfélszolgálati Központja[7] jogosult. Teljesítése a Gazdasági Hivatal saját protokolljának megfelelően történik.

[6] Az Európai Parlament és Tanács Általános Adatvédelmi Rendelete
[7] https://refomobil.hu/

Vezetőkre vonatkozó szabályok

A Református EGYMI székhelyintézményének, tagintézményeinek, telephelyeinek, munkaállomásainak vezetője, helyettese, egységvezetője jogosult és köteles meghatározni az irányítása alá tartozó foglalkoztatottak munkavégzéséhez szükséges a használandó informatikai rendszerek és az ahhoz szükséges jogosultságok körét.

Kötelesek együttműködni az elektronikus információs rendszer biztonságáért felelős személlyel, annak informatikai biztonsági feladatai ellátása során.

A használatra kiadott eszközök feladat végrehajtásra vonatkozó indokoltságát, meglétét az engedélyező vezetőnek évente felül kell vizsgálnia, és az indokoltság megszűnése esetén gondoskodnia kell az eszköz visszavétele felől ***(1. melléklet).***

Jogosult az informatikai eszközök munkavégzéshez szükséges használatának biztosítása érdekében, eszköz és jogosultság igénylési kérelmet ***(2. melléklet)***, eljárást kezdeményezni a Gazdasági Hivatal és az Informatikai Menedzsment felé.

Köteles gondoskodni az irányítása alá tartozó foglalkoztatottak informatikai biztonsági ismereteinek naprakészen tartásáról, beleértve az IBSZ és az Adatvédelmi Szabályzatban foglaltak szükséges mértékű ismeretéről.

Az IBSZ megsértésének észlelése során köteles:

- azonnal megtenni a szükséges intézkedéseket a biztonság helyreállítása során,
- kivizsgálni a biztonsági esemény körülményeit, különös tekintettel a személyes felelősség megállapítására, ezt követően felelősségre vonást kezdeményezni.

Jogosult az irányítása alá tartozó szervezeti egység tevékenységével kapcsolatos informatikai biztonsági feltételrendszerre javaslatot tenni a Gazdasági Hivatal és az Informatikai Menedzsment felé.

Adatmentések kezelése és végrehajtása

A Református EGYMI Székhelyintézmény Gazdasági Hivatal és a Munkaügyi Csoport részére automatikus és manuális adatmentés történik.

Kiemelt felhasználói szoftverek

Kiemelt felhasználói szoftverek melyek adatmentési szempontból magas prioritásúak:

1. Iktatásra használt alkalmazás: IQtató (LÁ.VA Manager Iroda Kft.)
   Az adatbázisból egyaránt naponta és hetente készül biztonsági másolat.
2. Könyvelésre használt alkalmazás: Novitax NTAX (Novitax Számítástechnikai Számviteli Szolgáltató és Kereskedelmi Kft.)
   Az adatbázisból havonta készül másolat.
3. Bérszámfejtésre használt alkalmazás: Novitax BÉR (Novitax Számítástechnikai Számviteli Szolgáltató és Kereskedelmi Kft.) **Kifutása: 2024.12, mert a bérszámfejtést 2025.01-tól a Magyar Államkincstár végzi**
   Az adatbázisból havonta készül másolat.
4. Gyereknyilvántartásra használt alkalmazás: I.M.S. (IntraFox Kft.)
   Felhőalapú tárolás, havonta készül másolat.

A korábbi adatmentéseket csak a Főigazgató vagy a Gazdasági Hivatal írásbeli utasítására szabad törölni, nem kiemelt prioritású adatok esetén általánosan a 15 napnál régebbi fájlok kerülhetnek törlésre, de csak abban az esetben, ha már létezik legalább 12 frissebb adatmentés az állományokról.

Különleges eseménykor előforduló biztonsági előírások

A felhasználó az adatok épségét, hozzáférhetetlenségét veszélyeztető legapróbb jelet észlelve köteles értesíteni az Informatikai Menedzsmentet.

A felhasználó a veszély legapróbb jelét észlelve azonnal abbahagyja a munkát, az elmentetlen dokumentumokat elmenti és az Informatikai Menedzsmentet további utasításági nem nyúl sem a számítógéphez, sem a biztonsági másolatokat tartalmazó merevlemezhez.

Az adatvédelmi felelős (amennyiben nem azonos a rendszergazdával) saját hatáskörében és felhasználó jelzésére is dönthet úgy, hogy az adatok biztonságára nézve veszélyhelyzetnek értékeli a jeleket és tüneteket.

Az adatvédelmi felelős (Hanganov Kft.) haladéktalanul értesíti a Főigazgatóságot és a Gazdasági Hivatalt.

Az Informatikai Menedzsmenttől érkező felelős biztosítja az érintett számítástechnikai eszközök teljes leválasztását, elkülönítését.

Ebben a témakörben a további irányított szabályokat (megelőző védelmi helyzet, terrorveszélyhelyzet, rendkívüli állapot, szükségállapot vagy váratlan támadás idején), a Református EGYMI Honvédelmi Intézkedési Tervében foglaltak szerint kell végrehajtani.

Adatok visszatöltése

A biztonsági mentésekből adatokat csak az adatvédelmi felelős tudtával és írásbeli beleegyezésével szabad visszatölteni. Az adatok visszatöltéséről jegyzőkönyvet kell készíteni ***(3. melléklet)***.

Külső felhasználókra vonatkozó szabályok

A Református EGYMI informatikai rendszereihez és eszközeihez hozzáférő külső felhasználó egyedileg köteles nyilatkozatot tenni arról, hogy az IBSZ-ben foglaltakat megismerte és magára nézve kötelezőnek ismeri el.

A Székhelyintézményben történtő helyszíni munkavégzés felügyelet mellett történhet.

Az informatikai fejlesztések során a projekt teljes életciklusára nézve az egyes részeket oly módon kell dokumentálni (pl. fejlesztői- , tesztelési- , üzemeltetési dokumentáció), hogy azokból a biztonsági követelmények megvalósulása ellenőrizhető legyen.

Amennyiben a szerződés egyedi szoftverfejlesztési tevékenységre irányul, úgy csak olyan szerződés köthető, amely alapján a fejlesztett szoftver forráskódját (vagy annak megfelelően részletezett) a Református EGYMI részére átadják, és a szerzői jogi védelem alá eső szoftver esetén a vagyoni jogokat a jogszabályok által engedélyezett legszélesebb körben átruházzák. Ettől csak különös esetben lehet eltérni azzal, hogy a szerzői jogi védelem alá eső szoftver kizárólagos felhasználási joga a jogszabályok által engedélyezett legszélesebb körben a Református EGYMI részére az esetben is átruházásra kerül.

Az informatikai rendszerek fejlesztése során külső felhasználó a teszt környezetben lévő informatikai rendszerhez az Informatikai Menedzsment engedélyével távoli elérést is igénylehet. Az engedélyt elektronikus írásbeli formában kell kérvényezni a informatika@refegymi.hu címen.

Személyi biztonsági követelmények, oktatás

A munkavállalókat a Református EGYMI-ben végzendő tevékenység megkezdése előtt az Informatikai Biztonsági Szabályzatban foglaltakat szerint kellő információval szükséges ellátni (lehetőség szerint elektronikus formában előzetes, továbbá szóban az első munkanapon).

Az IBSZ-re vonatkozó jogszabályi környezet megváltozásakor, továbbá, ha az IBSZ tartalmát érintő jelentős változás következik be, az IBSZ hatályba lépését, illetve a jelentős változását követő 60 napon belül a felhasználókat informatikai biztonsági továbbképzésben (továbbiakban oktatás), külső felhasználókat tájékoztatásban kell részesíteni.

Az oktatás tematikájának összeállításáért az Informatikai Menedzsment ellátója felelős, az oktatás megszervezéséért, végrehajtásáért, ha személyesen történik, az adott egység vezetője felelős.

Az IBSZ-t elektronikus formában is ismerteti a Református EGYMI, minden munkavállalójának elérhetővé teszi saját weboldalán (https://www.reformatusegymi.reformatus.hu)

Oktatáson való részvételt, vagy elektronikus formában megismert IBSZ-t a munkavállaló aláírásával igazolja, melyet a foglalkoztatott személyes anyagában tárolunk a Munkaügyi Csoportnál.

Új felhasználó hozzáférési rendszerbe való illesztését a Református EGYMI Informatikai Menedzsmentje végzi.

A jogosultságok kiosztása előtt, amennyiben az adott munkakör, tevékenység megköveteli a tipikus jogoktól – ide nem értve a munkavégzéshez szükséges adatbázisok elérését – történtő eltérését a tagintézmény-igazgatójának hatásköre eldönteni.

A felhasználó hozzáférést megalapozó jogviszonyának megszűnésekor a munkáltatói jogkör gyakorlója, illetve a szerződéskötést kezdeményező vezető a felhasználó tájékoztatása mellett köteles rendelkezni a felhasználó által készített, munkavégzéssel kapcsolatos dokumentumainak további kezeléséről (biztonsági mentés a központban, törlés, harmadik személy általi hozzáférés).

Amennyiben a felhasználó hozzáférést megalapozó jogviszonya megszűnik, de a hozzáférés más formában továbbra is indokolt (távoli hozzáférés, tanácsadó), a felhasználói jogosultságokat meg kell szüntetni és a felhasználót új felhasználóként kell kezelni, az új jogviszonyra irányadó eljárásrend alapján.

Adminisztratív biztonsági követelmények

A rendszerek teljes életciklusát dokumentálni kell, így a tervezés és továbbfejlesztés, a tesztelés és ellenőrzés, az üzemeltetés és karbantartás, valamit a selejtezés fázisait is.

A dokumentáció teljességéért és naprakészségéért az Informatikai Menedzsment felel.

Ezen dokumentációk akkor teljesek, ha tartalmazza mind a funkcionális, mind a biztonsági megfelelőségre vonatkozó valamennyi lényeges adatot.

Az összes eszköz azonosítását, mozgásuk nyomon követhetőségét az átadás-átvétel ***(1. melléklet)***, továbbadás, selejtezés dokumentálásával biztosítani kell.

Egyéb fel nem sorolt eszközök, valamint speciális adathordozók kezelése vonatkozásában, valamint az IBSZ-ben nem szabályozott kérdésekben, állásfoglalást kell kérni a Gazdasági Hivataltól és az Informatikai Menedzsmenttől egyaránt.

A papír alapú dokumentumok előállítására alkalmas eszközök (nyomtató) használatára a „Felhasználó feladatai” részben foglaltak érvényesek.

Fizikai, technikai, szoftveres védelem

Vagyonvédelem, és fizikai biztonság

- a szerverszobát, irodákat biztonsági zárakkal kell felszerelni;
- a szerverszobába való be- és kilépés rendjét szabályozni kell;
- a szerverszoba kulcsát a helyi házi szabályzatban szerint kell tárolni, onnan csak az arra feljogosítottak vehetik fel;

- munkaidőn túl az irodákban, illetve a szerverszobában csak engedéllyel lehet tartózkodni;
- a szerverszobába történő illetéktelen behatolás tényét a Főigazgatónak, a Gazdasági Hivatal vezetőjének és az Informatikai Menedzsment vezetőjének kell jelenteni;

Adathordozók védelme

- a munkaasztalon csak azok az adathordozók lehetnek, amelyek az aktuális
- feldolgozáshoz szükségesek;
- az adathordozókat jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak;
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni;
- az adathordozók szállítása csak megfelelő módon kialakított fémdobozban történhet;
- adathordozót más intézménynek átadni csak az adatvédelmi felelős engedélyével lehet;
- az adathordozók megőrzésének idejét, ha másképp nincs rendelkezés, a felelős vezető határozza meg;
- az adathordozókat évenként ellenőrizni és tisztítani kell;
- olyan adathordozót, amelyet javíthatatlan fizikai károsodás ért, selejtezni kell. Selejtezendő: a) a fizikailag sérült, javíthatatlan; b) gyári, raktározási hibát követően felhasználásra alkalmatlan (deformálódott); c) ha a kapacitás a névleges érték 75%-ánál kevesebb; d) véglegesen elhasználódott adathordozót.

Az alkalmatlan adathordozókat fizikai roncsolással használhatatlanná kell tenni. A bizalmas adatokat, felhasználói és rendszerprogramokat tartalmazó adattárolókról törlő program segítségével kell az adatokat törölni, vagy fizikailag kell megsemmisíteni az adathordozót.

Selejtezés

A selejtezést a Selejtezési Szabályzatnak és a hivatali Iratkezelési Szabályzatának megfelelően kell lefolytatni, Az adathordozókat a Leltározási Szabályzatnak megfelelően kell leltározni.

Vírusvédelem

A munkaállomásokon és szervereken, ha másképp nincs rendelkezés, havi rendszerességgel vírusellenőrzést és vírusirtást kell tartani. A vírusvédelmi programok adatbázisát naprakészen kell tartani.

Vírusfertőzés okozta hiba gyanúja esetén azonnal szólni kell a felettesnek. Amennyiben nincs erre lehetőség (pl. munkaidőn kívül), a feldolgozásban lévő adatokat el kell menteni, majd a programból kilépve a gépet ki kell kapcsolni. A gépet addig bekapcsolni nem szabad, amíg azt az arra illetékes szakember, rendszergazda meg nem vizsgálta. A vírusfertőzést jelenteni kell a szervezeti egység vezetőjének, még akkor is, ha semmi hiba nem történt a fertőzés folyamán, valamint az Informatikai Menedzsmentnek ki kell deríteni a fertőzés lehetséges okait, és a szükséges védelmi intézkedést meg kell hoznia.

Szoftvervédelem

Az üzemeltetésért felelős rendszergazdának biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek az illetékes felhasználók számára.

Rendszerszoftver védelem

- a rendszerszoftver módosításához az illetékes engedélye szükséges;
- a módosítással egy időben a dokumentációban is át kell a változtatásokat vezetni;
- a rendszerszoftver-eseményekről és a változtatásokról nyilvántartást kell vezetni
- (eseménynapló).

Programhoz való hozzáférés, programvédelem

- A kezelés folyamán az illetéktelen hozzáférést és próbálkozást ki kell zárni.
- Gondoskodni kell arról, hogy a tárolt programok, adatállományok ne károsodjanak, a követelményeknek megfelelően működjenek
- A feldolgozás biztonságának megvalósításához naprakész állapotban kell tartani a program dokumentációt.

A programokról nyilvántartást kell vezetni, amelynek az alábbi adatokat kell tartalmaznia:

- a program azonosítója;
- a program készítőjének neve;
- a feldolgozási rendszer megnevezése.

Informatikai védelem

Az irodákban/szerverszobában a folyamatos, higiénikus munkavégzés feltételeit kell megőrizni. A szerverszobai rend megtartásáért és a biztonságos műszaki üzemeltetésért az Informatikai Menedzsment felelős.

A szerverszobába ételt, italt bevinni és ott elfogyasztani szigorúan TILOS!

A szerverszobába égő cigarettával belépni és ott dohányozni, valamint tüzet okozó tevékenységet folytatni szigorúan TILOS!

A szerverszoba takarítását csak a hivatali informatikus felügyelet mellett, a kijelölt személyek végezhetik.

A berendezések belsejébe nyúlni TILOS! Bármilyen nem a gépkezeléssel összefüggő beavatkozást csak az Informatikai Menedzsment és a szakszervizek emberei végezhetnek.

Adathordozókat csak a hivatali informatikus engedélyével lehet be- és kivinni a szerverszobából.

Az törpefeszültségű elektromos hálózatba más – nem a rendszerekhez, illetve azok kiszolgálásához tartozó – berendezéseket csatlakoztatni nem lehet.

A számítógép javításoknak, illetve bármilyen beavatkozásoknak minden esetben ki kell elégíteni a szükséges műszaki feltételeken kívül a balesetmentes használat, a szakszerűség, a vonatkozó érintésvédelmi szabályok és az esztétikai követelményeket. Nem végezhető olyan javítás, szerelés, átalakítás vagy bármely beavatkozás, amely nem elégíti ki a balesetvédelmi előírásokat. A fenti rendelkezések megsértése esetén az elkövetővel szemben a Főigazgató fegyelmi felelősségre vonást kezdeményezhet.

Logikai védelem

Elektronikus rendszerek leállítása

A székhelyintézményben az ügymenet-folytonosság tervezése során, meg kell határozni az elektronikus információs rendszerek leállítási terveit, melyek előre tervezett áramszolgáltatás kiesés, katasztrófahelyzetek kezelésére vonatkozóan tartalmaznia kell:

1. az eseményt megelőző állapotfelmérés
2. az esemény definíciója
3. a leállítás tényét meghatározó, a folyamat inicializálásért felelős személyt/személyeket
4. az akadály elhárulása utáni, újraindítási feladatokat

Elektronikus rendszerek helyreállítása, újraindítása

Az elektronikus információs rendszerekre vonatkozó leállítási, helyreállítási tervek elkészítéséről, teszteléséről és folyamatos karbantartásáról az Informatikai Menedzsment gondoskodik.

A terveket minden olyan esetben aktualizálni kell, amikor jelentősen megváltozik az infokommunikációs hálózat (új szerver beállítása, új szünetmentes tápegység csatlakoztatása, új hardverek beszerelése esetén).

Megfelelés a szabályzatnak, fenyegetettségek

A Református EGYMI fenyegetettségének elemzését és a kockázatok meghatározását évente el kell végezni.

Az IBSZ-nek megfelelő működést igény szerint, de legalább évente teljeskörűen ellenőrizni kell.

A fenyegetettségek elemzését és a kockázatok meghatározását az Informatikai Menedzsment hajtja végre, szükséges szerint kérheti külső szakértő bevonását.

Felülvizsgálat, aktualizálás

Az IBSZ-t szükség szerint – de legalább évente – felül kell vizsgálni, és aktualizálni kell, így különösen:

- súlyos informatikai biztonsági eseményeket követően, az esemény tanulságait levonva;
- a szabályozási környezet változása esetén, amennyiben az az IBSZ-ben foglaltakat érinti.

Amennyiben az IBSZ rendkívüli módosítása szükséges – a szükséges módosítás jellegétől vagy terjedelmétől függetlenül – az Informatikai Menedzsment jelzi a Főigazgató és a Gazdasági Hivatal igazgatója felé.

Mellékletek

1. sz. melléklet – átadás-átvételi jegyzőkönyv

Református EGYMI
OM: 102809
2314 Halásztelek, Hold utca 6.

ÁTADÁS-ÁTVÉTELI JEGYZŐKÖNYV

1. Készült a Református Egységes Gyógypedagógiai Módszertani Intézmény _____ ***székhelyén/tagintézményében/telephelyén/munkaállomásán.***
2. Átadó neve:
3. Átvevő neve:
4. Költséghely:
5. Átadott eszköz / eszközök:

Megnevezés	Leltári szám	Gyári szám

Aláírásommal kijelentem, hogy:

- az eszközt hiánytalanul átvettem
- elolvastam és elfogadom, továbbá betartom a Református EGYMI Informatikai és Biztonsági Szabályzatában foglaltakat;
- a jegyzőkönyv 2 példányban készült (1 munkavállaló / 1 központi irattár)

……, ……

Kiadási hely Dátum

…… ……

Átadó Átvevő

levelezési cím: 2314 Halásztelek, Pf. 44.
tel: 06-30/639-08-61, email: igtitkarsag@refegymi.hu
weblap: reformatusegymi.reformatus.hu

2. sz. melléklet – eszközigénylési lap

REFORMÁTUS EGYMI
OM: 102809
2314 Halásztelek, Hold utca 6.

ESZKÖZIGÉNYLÉSI LAP

Költséghely, indoklás:

Megnevezés	Mennyiség	Előrelátható költség (HUF)
Összesen		

Igénylő neve (nyomtatott)	
Igénylő aláírása	
Igénylés dátuma	
Engedélyező (igazgató) aláírása	
Ellenjegyző (gazd. vez.) aláírása	

Cím: 2314 Halásztelek, Hold utca 6. / Levelezési cím: 2314 Halásztelek, Pf. 44.
Tel: 06-24/519-019 Mobil: 06-30/639-08-61 Email: igtitkarsag@refegymi.hu
Weblap: reformatusegymi.reformatus.hu

3. sz. melléklet – adatvisszatöltési kérelem

REFORMÁTUS EGYMI
OM.: 102809

2314, Halásztelek, Hold utca 6.

Adatvisszatöltési kérelem

Adatvisszatöltést igénylő felhasználó:

Visszatöltés kérése a következő szoftver(ek)hez:

Megnevezés	Időszak

Visszatöltés rövid indoklása:

Adatvisszatöltési kérelmet igénylő aláírása:

Adatvisszatöltési kérelemet engedélyező személy (felettes aláírása):

Adatvisszatöltés tényleges megvalósulása

Dátum	Informatikai Menedzsment részéről igazoló aláírás

Cím: 2314 Halásztelek, Hold utca 6. Levelezési cím: 2314 Halásztelek, Pf. 44.
Tel: 06-24/519-019 Mobil: 06-30/639-08-61 Email: refegymiigazgato.titkarsag@gmail.com,

4. sz. melléklet – szoftverhozzáférési igénylőlap

REFORMÁTUS EGYMI
OM.: 102809

2314, Halásztelek, Hold utca 6.

Hozzáférési kérelem

Szoftverhozzáférési kérelem a következő munkavállaló részére:

Hozzáférés igénylése a következő szoftver(ek)hez, elektronikus levelezési felülethez:

Megnevezés	Felhasználónév	Jelszó	Megosztás

A LÁ.VA Iktató szoftveren belül a következő iktatókönyvek kezelésére adok jogosultságot:

1.
2.
3.
4.
5.

Aláírásommal a hozzáférést engedélyezem (felettes):

(aláírás)

Dátum	Hozzáférést beállította (rendszergazda)

Cím: 2314 Halásztelek, Hold utca 6. Levelezési cím: 2314 Halásztelek, Pf. 44.
Tel: 06-24/519-019 Mobil: 06-30/639-08-61 Email: refegymiigazgato.titkarsag@gmail.com,