Iktatószám:692/2023

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Az Informatikai Biztonsági Szabályzat 2023.12.07-én lép hatályba. Az eddig a dátumig érvényes informatikai szabályzat hatályát veszti.

Kelt, Budapest 2023.12.07. napján

Ügyvezető

1. A szabályzat célja

Az Információbiztonsági Szabályzat (továbbiakban: IBSZ) célja, hogy az ERöMŰVHÁZ Nonprofit Kft. (továbbiakban: Társaság) által kezelt adatok és információk biztonságát megteremtse, továbbá intézkedéseket, szabályokat, követelményeket fogalmazzon meg, mellyel az információbiztonsági követelményeket a Társaság hatékony működés mellett biztosítani tudja.

2. A szabályzat hatálya

Az IBSZ alanyi hatálya kiterjed az összes, a Társaságnál fő- és mellékállásban foglalkoztatott alkalmazottra, valamint a szerződéses jogviszonyban álló, vállalkozói és egyéb szerződés keretében foglalkoztatott munkavállalóra (a továbbiakban: felhasználók).
A fő és mellékállásban foglalkoztatottak körét az **1. számú melléklet** tartalmazza.

A Szabályzat kiterjed minden nemű adatra és információra, mely a Társaság informatikai vagy egyéb eszközén tárolódik, továbbítódik, beleértve minden papíron található adatot és információt mely a Társasághoz vagy a Társaság tevékenységéhez, működéséhez köthető és összhangban van a szervezet GDPR szabályzatával.

A Szabályzat kiterjed a Társaság által használt valamennyi informatikai rendszerre, eszközre, amely felhasználja, eléri, tárolja, felügyeli, feldolgozza, továbbítja, vagy megőrzi a Társaságnál keletkező, illetve felhasznált adatokat, információkat és kommunikációt.

3. Módosítási előírások

Jelen IBSZ naprakészségét a jogszabályi, funkcionális, szervezeti, technológiai, valamint egyéb változásokra tekintettel a **Rendszergazda** az Ügyvezetővel egyeztetve szükség szerint felülvizsgálja és jóvá hagyatja a módosítási javaslatait.

4. Jogszabályi környezet

A Társaság tevékenységét szabályozó jogszabályok, kormányrendeletek, felügyeleti és egyéb előírások az alábbiak:

- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.),
- Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete - a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet - GDPR).

5. Az információbiztonság szabályozása

5.1. Az információbiztonság belső szervezete

A szerepek és felelősségek meghatározása kiemelt fontosságú az információbiztonság fenntartása érdekében a Társaságnál. Annak érdekében, hogy ne alakuljanak ki összeférhetetlen szerepkörök, a felelősségeket teljeskörűen definiálni szükséges.

Az ***Ügyvezető*** felelős az alábbiakért az információbiztonsággal összefüggésben:

- Az informatikai környezethez hozzáférő munkatársak kiválasztási folyamatában az információbiztonsági követelmények teljesülésének biztosításában;
- Az információbiztonság kulcsszereplőinek foglalkoztatásával kapcsolatos feladatok és felelősségek meghatározásáért a **Rendszergazdával** együttműködve; **A kulcs** szereplők körét, jogviszony, munkakör bontásban az 1. sz. melléklet tartalmazza
- Az alkalmazások tekintetében a felhasználói hozzáférési jogosultságok visszavonásának kezdeményezésében egy felhasználó távozásakor, illetve szervezeten belüli mozgásakor;
- A biztonságtudatosság képzési és oktatási feltételeinek meghatározásában és menedzselésében.

A ***Felhasználók*** felelősek az alábbiakért az információbiztonsággal összefüggésben:

- Az informatikai erőforrások rendeltetésszerű használata
- Az általa használt alkalmazások felhasználói ismerete
- A kezelésében álló alkalmazói rendszerekkel és informatikai eszközökkel kapcsolatos, illetve az általános információbiztonsági oktatásokon való részvétel. Az oktatáson résztvevő körét a Szabályzat melléklete tartalmazza, oktatás gyakorisága szükség szerint kerül meghatározásra.
- IT biztonsági események azonnali jelentése a Rendszergazda felé.

5.2. Vagyontárgyak kezelése

5.2.1. Adatok osztályozása

A Társaságnál tárolt és kezelt adatok védelme érdekében ki kell alakítani osztályozási és kezelési módszertant. Az adatok kategorizálásánál figyelembe kell venni az adat sértetlenségét, bizalmasságát és rendelkezésre állását.

A Rendszergazda felelőssége az adatok osztályba sorolása alapján a megfelelő szintű kezelése

- a rendszereket és alkalmazásokat bizalmassági osztályokba kell besorolni:
  - nyilvános adatok (Szolgáltató központok elérhetősége, nyitva tartása)
  - belső adatok (szerződéses állományok)
  - bizalmas adatok (pénzügyi és human erőforrásra vonatkozó)
- a rendszerek besorolása a NEIH-OVI tábla alapján történik, annak eredménye határozza meg a rendszerek biztonsági besorolását (lsd. melléklet);
- minden harmadik félre vonatkozó bizalmas adatot úgy kell kezelni, mintha a Társaság bizalmas adatai lennének;
- személyes adatokat csak indokolt esetben kell tárolni, kezelni, valamint a GDPR-ban megfogalmazottak szerint kell eljárni velük.

5.2.2. Informatikai eszközök leltározása

A Társaságnál használt informatikai eszközöket nyilvántartásba kell venni.

A Rendszergazda felelőssége:

- a Társaság informatikai vagyontárgyairól vagyonleltárt készítsen;
- évenként felülvizsgálja az informatikai vagyonleltárt, amelyet a Szabályzat melléklete tartalmaz

Az informatikai leltárnak az alábbiakat tartalmaznia kell (ahol értelmezhető az adott paraméter):

- a vagyontárgy típusa (szoftver, hardver);
- a vagyontárgy fellelhetőségének helye;
- a vagyontárgy telepítésének, használatbavételének idejét;
- a vagyontárgyhoz kapcsolódó licence információkat;

5.2.3. A vagyontárgyak elfogadható használata

Informatikai eszközök kezelése, használata

A beszerzést és nyilvántartásba vételt követően az informatikai eszközök üzembe helyezését kizárólag a Rendszergazda vagy az általa megbízott munkatárs végezheti.

Az eszközök elvárt kezelésénél minden felhasználónak legalább az alábbiakat kötelezően be kell tartania:

- Hiba esetén azonnal kötelesek jelezni a hibát a Rendszergazda felé az alábbi elérhetőségeken: informatika@smith.hu; 06-70-776-1888
- Kötelesek betartani a munka és tűzvédelmi, biztonsági előírásokat, szabályokat;
- Tilos az eszközöket megbontani, felbontani, nem rendeltetésszerű használat alá kitenni;

5.3. Személyi biztonság

A megfelelő munkaerő kiválasztása fontos része az informatikai biztonság fenntartásának. Új munkaerő felvételnél fontos ellenőrizni, hogy a jelölt képes e megfelelően betartani az információbiztonsági elvárásokat, melyet a Társaság elvár.

5.3.1. Átvilágítás

Tekintve, hogy a Társaság jogilag nem kötelezett semmilyen típusú átvilágításra a munkaerőt figyelembe véve, a Társaság felelős azért, hogy meghatározza mikor szükséges részletesebb háttérvizsgálat egy-egy új jelentkező esetében a foglalkoztatást megelőzően, a betöltendő munkakör kockázataival arányos mértékben. A Társaság nemzetbiztonsági átvilágítást nem végez, arra nem jogosult. A belépés során a munkavállalótól erkölcsi bizonyítvány bemutatását kérheti, azonban azt nem tárolja valamint másolatot sem készít róla.

5.3.2. A foglalkoztatás feltételei

A ***Ügyvezető*** felelős azért, hogy

- a munkavállalóval kötendő szerződésben rögzítésre kerüljenek a kockázatokkal arányos titoktartási követelmények és a foglalkoztatás egyéb kikötései.
- A foglalkoztatás során megköveteljék az információbiztonsági szabályzatokban meghatározott előírások betartását és végrehajtását. Az új belépő munkavállalóknak meg kell ismerniük az IBSZ szabályzat rájuk vonatkozó részét.

5.4. Hozzáférés menedzsment

5.4.1. Hozzáférés menedzsment üzleti követelményei

- A hozzáférési jogosultságok kialakítását, szabályozását az informatikai oldal elvárásai, és a Társaság feladatai összehangolásának figyelembevételével kell meghatározni.
- A használt rendszerekben gondoskodni kell a felhasználók egyedi azonosításáról.

- Külső személyek (támogatók stb.) számára ideiglenes jogosultság biztosítása szükséges.

A kialakított követelményrendszer aktualitását legalább évente egyszer vizsgálni kell és a változásoknak megfelelően módosítani szükséges.

Az ellenőrzés során vizsgálni kell:

- a felhasználók nem rendelkeznek-e több vagy kevesebb joggal, mint amit a munkakörük megkíván;
- az ideiglenesen kiosztott jogok, kilépett dolgozók jogosultságai visszavonásra kerültek-e.

5.4.2. Hozzáféréssel kapcsolatos igények kérésének módja

A munkavállalók részére a számítógépes rendszerekhez történő hozzáférést, annak módosítását az **Ügyvezető** vagy az általa írásbeli utasításban felhatalmazott személy kérheti. Az igénylés minden esetben írásban történik a **Rendszergazda** felé, aki köteles a létrehozást/módosítást/törlést indokolatlan késedelem nélkül, de maximum 1 munkanap alatt elvégezni. A kilépő munkatárs számítógépes hozzáférésének megszüntetési kérelmét szintén az **Ügyvezető** kezdeményezi.

- Jogosultság csak a munkaköri feladatok ellátásához igényelhető.
- A felhasználó munkaviszonyának megszűnése esetén jogosultságait a munkaviszony megszűnésének ismertté válásakor azonnal korlátozni kell, illetve a munkában töltött utolsó nap végén véglegesen vissza kell vonni.
- A személyhez köthető jogosultságokat a munkaviszony megszűnésének napján vissza kell vonni, a felhasználói adatok (pl usernév) más személy részére még ideiglenes jelleggel sem kiadhatóak.
- A felhasználó által használt informatikai eszközöket – más megállapodás hiányába – legkésőbb az utolsó munkában töltött napon a felhasználónak vissza kell szolgáltatnia a munkáltatói jogokkal rendelkező személynek. A **Rendszergazdának** az eszközön tárolt infomációkat újbóli felhasználás előtt törölnie kell.

5.4.3. Jelszómenedzsment

A Társaság informatikai rendszereihez való illetéktelen logikai hozzáférések megakadályozására bejelentkezési jelszavakat kell létrehozni mind a felhasználók, mind a rendszergazdák számára. Ezek tárolása tűzálló, zárható páncél szekrényben kell, hogy történjen.

- A jelszókövetelmények meghatározása, kockázatarányos módon, az adott rendszer technikai lehetőségeit figyelembe véve a **Rendszergazda** feladata
- A jelszavak kiosztása minden esetben zártan kell, hogy történjen.

A felhasználói jelszavak meghatározásának a következő kritériumok figyelembe vételével kell történnie:

- Minimális hossz: 8 karakter;
- A jelszavak komplexitásánál az alábbiak közül valamennyi elvárásnak teljesülnie kell
  - Kisbetű;
  - Nagybetű;
  - Szám;
- A jelszavakat legalább évente meg kell változtatni;

A Rendszergazdának az alábbiakra kell felhívni a munkavállalók figyelmét a jelszó választásánál és használatánál:

- tartsa titokban a jelszavait;
- a jelszavak papírra rögzítése tilos;
- mindannyiszor és mindakkor cseréljen jelszót, ha bármi jel mutat arra, hogy a rendszer vagy jelszó veszélyeztetve van;
- nem alapoz olyanra, amelyet bárki könnyen kitalálhat, vagy az illető személyével kapcsolatos adatokból kinyerhet, például nevekből, telefonszámokból, születési adatokból stb.
- nem tartalmaz azonos karaktereket, illetve sem csupa számokból, sem csupa betűkből álló csoportokat
- egyes rendszerek esetében a technológia nem támogatja a megfelelő komplexitású jelszavak használatát, illetve a rendszeres kikényszerítet változtatást. Ezekben az esetekben is a **Felhasználó** felelőssége a fenti szabályok betartása

Kiemelt felhasználók jelszavaira vonatkozó szabályok

Kiemelt felhasználónak minősül minden olyan személy, aki a szervezetnél kiemelt döntési körrel vagy a rendszerekre vonatkozóan kiemelt jogosultságokkal bír vagy kritikus besorolású rendszerekhez, erős hozzáféréssel rendelkezik. Ilyen például az Ügyvezető és a Rendszergazda.

Esetükben a következő kritériumok figyelembevételével kell történnie:

- Minimális hossz: 12 karakter;
- A jelszavak komplexitásánál az alábbiak közül valamennyi elvárásnak teljesülnie kell
  - Kisbetű;
  - Nagybetű;
  - Szám;
  - Különleges karakter

- A jelszavakat legalább félévente meg kell változtatni;

Adminisztrátori jelszavak tárolása

- A kiemelt jogosultságokkal rendelkező adminisztrátori jelszavakat a Társaság erre a célra kijelölt páncélszekrényében kell tárolni.
- Az elzárt jelszavakhoz kizárólag az **Ügyvezető** rendelkezhet hozzáféréssel és felhasználás esetén annak tényét dokumentálni köteles a kialakított Jelszó menedzsment alapján.

5.4.4. Felügyelet nélkül hagyott informatikai eszközök

A Társaság munkavállalóinak az informatikai biztonság megtartása érdekében felelősséggel kell bánniuk a munkaeszközeikkel, valamint környezetükkel.

Ennek érdekében a következő szabályokat kell betartaniuk:

- A munkaállomást jelszavas képernyővédővel kell védeni. A képernyővédő indításának maximum 15 perc kihasználatlanság után meg kell történnie.
- Ha a felhasználó a munkaidő végén távozik, a munkaállomást mindig ki kell kapcsolnia. Ez alól kivételt képeznek a hosszan futó adatfeldolgozások, valamint a távoli elérésű számítógépek. Ezekben az esetekben azonban a munkaállomást zárolni kell.

5.4.5. Mobil eszközökre vonatkozó szabályok

A Társaságnál használatban levő laptopok esetében a biztonsági követelmények magasabbak, mint a Társaság épületeiben használt PC-k esetében, mivel fizikailag könnyebben elérhetőek a támadók számára.

- Jelszavas képernyővédő használata 5 perc elteltével szükséges.
- A hordozható számítástechnikai eszközöket szigorúan óvni kell. Gondoskodni kell az eszközök fizikai védelméről és nyilvános helyen (például személygépkocsiban, nem szemmel látható helyen sem) nem szabad felügyelet nélkül hagyni őket.
- A számítógép eltulajdonítása esetén azonnal értesíteni kell a(z) **(illetékes hatóságot és a munkahelyi vezetőt) Rendszergazdát,** aki intézkedik a megfelelő személyek értesítéséről.

5.4.6. Okostelefon használatra vonatkozó szabályok

A készülékeken nincsen korlátozva az alkalmazások telepítése, a felhasználó felelőssége, hogy milyen alkalmazásokat telepít az eszközökre, azonban nem megbízható forrásból a telepítés tilos. Kizárólag a hivatalos alkalmazás-boltokból engedélyezett az alkalmazások beszerzése.

- Az eszközökön az operációs rendszerek frissítése kötelező. Ezek a frissítések valamennyi esetben biztonsági javításokat is tartalmaznak, ezért ezek nem telepítése veszélyezteti a telefon biztonságát.
- A felhasználó kötelessége megelőzni a készülék eltulajdonítását. Amennyiben ez mégis megtörténik, azt haladéktalanul jelezni köteles a(z) **(illetékes hatóságnak és munkahelyi vezetőnek) Rendszergazda** felé.
- Nyilvános Wi-Fi-k használata nem javasolt, kizárólag, ha a felhasználó teljesen megbizonyosodott, hogy az megbízható forráshoz tartozik (pl.: ügyfél, állami hivatal). Hotelek, éttermek és egyéb nyilvános helyeken a Wi-Fi-k használata nem engedélyezett.
- Amennyiben a telefonról céges rendszerek elérhetőek vagy a telefonon céges adatokat tárolnak, úgy a **Felhasználónak** a készület automatikusan lezáró jelszavas védelemmel (vagy más ezzel egyenértékű védelemmel) kell ellátnia, az adatlopás megelőzése érdekében.

5.5. Üzemeltetés biztonsága

5.5.1. Üzemeltetési szabályzatok

A Társaság informatikai rendszereinek üzemeltetéséért és adminisztrálásáért, a **Rendszergazda** van kijelölve.

5.5.2. Vírusvédelmi tevékenységek szabályozása

Az informatikai infrastruktúra és az adatok védelmének biztosítására szolgáló eljárások között alapvető a hatékony vírusvédelem kiépítése és folyamatos működtetése, amely megvédi az informatikai rendszereket a rosszindulatú, romboló hatású programok elterjedése ellen.

A Társaság vírusvédelmét a Microsoft beépített rendszere valósítja meg.

Ez a modul felelős a friss vírusadatbázisok letöltéséért, azok kliens gépekre való telepítéséért. Az aktív védelem kikapcsolása tilos a felhasználók számára. A hordozható számítógépek vírusadatbázisainak frissítéséért a számítógép felhasználója felelős. A Társaság hálózatára való csatlakozásakor a vírusadatbázis-frissítés és - ellenőrzés automatikusan megtörténik. Amennyiben a gép internetre csatlakozásakor a frissítés automatikusan nem történne meg, a frissítést manuálisan kell kezdeményezni és erről értesíteni kell a rendszergazdát.

A **Rendszergazda** ezzel kapcsolatos feladatai:

- a vírusdefiníciós állományok naprakészen tartása,
- új program üzembe helyezése, mentett adatállomány visszatöltése, valamint vírusfertőzés alapos gyanúja esetén rendkívüli vírusellenőrzés végrehajtása,
- vírusfertőzés esetén a felhasználók értesítése, a vírusirtás elindítása és lezárása, az ő vezetésével történik a fertőzött számítógépek vírusmentesítése,

- vírusfertőzés esetén ellenőrizni kell mindazon adathordozót, amelyek a számítógéppel a vírusfertőzésig kapcsolatba kerültek. Ha a **Rendszergazda** olyan adathordozót talál, amely eltávolíthatatlan vírussal fertőzött, azt meg kell semmisíteni, kivéve akkor, ha nyomozati okokból a rosszindulatú szoftver elemzésére van szükség. Ebben az esetben az adathordozót az érintett gépből ki kell szerelni.

5.5.3. Szoftverek kezelése

Az informatikai biztonság megvalósításához hozzájárul a szoftvereszközök jogszerű használata, valamint szoftverek biztonságos kezelése. Szoftver leltárt a Szabályzat melléklete tartalmazza.

A számítógépeken kizárólag a **Rendszergazda** bír telepítési jogosultsággal, így azokra új szoftvert kizárólag a **Rendszergazda** tud telepíteni.

A felhasználókra nézve kiemelt fontosságú, hogy a felhasználók kizárólag jogtiszta szoftvereket használhatnak, melynek elmulasztása fegyelmi eljárást vonhat maga után, valamint figyelmeztetést.

5.5.4. Mentések, file-ok védelme az archiválási mentési koncepció alapján történik

- Az adatfeldolgozás után biztosítani kell az adatok mentését.
- A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (**felhasználók**) feladata.
- A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban a **Rendszergazda** segítséget nyújt.
- A Társaság rendelkezik központi filemegosztó és tároló szolgáltatással, így az adatok biztonságos tárolása ezen környezetben kell, hogy történjen. Üzletititkoat tartalmazó információkat kizárólag a filemegosztón lehet tárolni.
- Az archiválási mentési koncepció alapján szükséges heti rendszerességgel a teljes szerver adatállomány mentése a szervertől független hordozóra (NAS) amelyet fizikailag is máshol szükséges tárolni.

5.6. Kommunikáció biztonsága

5.6.1. Cserélhető adathordozók

Üzleti titkot, személyes adatot, vagy egyéb nem nyilvános adatot USB tárolóra, CD-re, vagy DVD lemezre csak titkosítva szabad másolni az illetéktelen hozzáférés megakadályozása céljából. Erről a munkahelyi vezetőnek tájékoztatni kell a munkavállalókat.

Adathordozók tárolására vonatkozó szabályok:

- figyelembe kell venni a gyártó által meghatározott tárolási környezetre vonatkozó paramétereket, a tároló helynek tűzbiztos, elektromágneses hatásoktól védett helynek kell lennie.

5.6.2. Elektronikus levelezés biztonsága

Az elektronikus levelezés lehetővé teszi az alkalmazottak és partnerei közötti adatcserét és információáramlást. Annak érdekében, hogy levelező rendszer használatából eredő támadások lehetősége minimálisra csökkenjen, a Társaság felhasználói csak a **Rendszergazda** által engedélyezett szoftvert használhatják, akiknek biztosítania kell a ki- és bemenő levelek vírusellenőrzését. Az informatikai piacon aktuális vírus és zsaroló vírus betörésvédelem ellenőrzésére alkalmas szoftverről a rendszergazda ad tájékoztatást az ügyvezetőnek.

A beállítások megvalósítása a **Rendszergazda** feladata.

- A felhasználók kötelesek naponta ellenőrizni e-mail üzeneteiket.
- A levelet csak akkor szabad megnyitni, ha a levél megbízható feladótól származik. Nem szabad megnyitni például az angol nyelven írt, nyereményekre és ismeretlen, megrendelt küldeményekre utaló leveleket, ezeket haladéktalanul törölni kell. Ha a felhasználó bizonytalan a levéllel kapcsolatos teendőt illetően, köteles a **Rendszergazda** segítségét kérni.
- A felhasználóknak tilos láncleveleket készíteni és továbbítani. Tilos továbbá más felhasználóktól, illetve külső hálózatról kapott támadó vagy „szemét" („junk") jellegű, a hálózat túlterhelését célzó e-mailek megnyitása, továbbítása.
- A felhasználóknak tilos a Társaság nevében olyan e-mailt küldeni, csatolt fájlt megjelentetni elektronikus hirdetőtáblákon vagy egyéb fórumokon, melyek:
    - a Társaság hírnevét, vagy az ügyfelekkel való kapcsolatát ronthatják, illetve annak ügyfeleinek érdekét sérthetik,
    - a Társaság bizonyos területekre vonatkozó álláspontját képviselik, fejezik ki,
    - szerzői jogokat sérthetnek,
    - vírusokkal fertőzhetnek meg bármely hálózatot.

- A felhasználók az céges e-mail címükkel semmilyen levelezőlistára, hírcsoportra nem iratkozhatnak fel, nem jelentkezhetnek be.
- A felhasználók személyes levelezésre a Társaság levelező szoftverét nem használhatják, hivatalos, a munkájukkal kapcsolatos ügyeket kizárólag a Társaság levelezési rendszerén keresztül bonyolíthatják.
- A felhasználó által küldött elektronikus leveleket a felhasználónak saját nevével, azonosítható módon kell aláírnia.
- A felhasználók üzleti titkokat tartalmazó levelet, dokumentumot nyilvános levelező rendszer felé (pl.: gmail.com) küldeni, továbbítani, csak üzleti folyamathoz kapcsolódóan lehet. A felhasználók munkavégzéshez kapcsolódó anyagokat saját nyilvános levelezőrendszerükre és nyilvános fájlmegosztó szolgáltatások tárhelyeire nem küldhetnek.
- Nagy számú személyes adatokat tartalmazó leveleket és csatolmányokat kizárólag titkosított formában lehet továbbitani (például Zip tömörítés és jelszavas védelem). Ebben az esetben a titkosításhoz tartozó jelszót – lehetőség szerint – más csatornán (mint például élőszó vagy SMS) kell eljuttatni a címzetthez. Az erre vonatkozó szabályzásról tájékoztatni kell a munkavállaókat a soron következő IBSZ-szel kapcsolatos oktatáson.

5.6.3. Internet szolgáltatások

A Társaság informatikai rendszereit fenyegető veszélyek száma nő az Internetre való kapcsolódással. Az így keletkező veszélyforrások kiküszöbölése a szükséges technikai feltételek megteremtésével és az előírások betartásával lehetséges.

A böngésző Internet biztonságát közepesnél alacsonyabbra állítani tilos.

A **felhasználókra** vonatkozó szabályok:

- az Internetes szolgáltatásokat kizárólag a **Rendszergazda** által lehetővé tett módon, hálózaton keresztül vehetik igénybe.
- az Internetről csak a munkavégzéshez szükséges adatállományok, táblázatok, tölthetők le, a hálózatra csatlakoztatott gépre, amelyeket a vírusvédelmi rendszernek automatikusan kell ellenőriznie.
- file-ok letöltése nem megengedett abban az esetben, ha a számítógép „Nem biztonságos hely"-et jelez.

5.7. Információbiztonsági incidensek kezelése

Informatikai biztonsági incidensek észlelése esetén a legfontosabb, hogy a bejelentés indokolatlan késedelem nélkül megtörténjen a felhasználók felől, melynek módja a következő:

A felhasználóknak azonnal jelenteni kell az alábbi esetekben a **Rendszergazdának, az alábbi elérhetőségeken: informatika@smith.hu, 06-70-776-1888**:

- bármilyen elektronikus adat sérülését, kiszivárgását, vagy jogszerűtlen belső használatát fedezték fel, vagy ennek gyanúja áll fenn;
- felismert vagy felismerni vélt védelmi gyengeséget, sérülékenységet, hiányosságot, biztonsági rést fedeztek fel.

A felhasználóknak telefonon vagy e-mailen szükséges értesíteni a **Rendszergazdát**, mely során tájékoztatják az incidens paramétereiről. A Rendszergazdának haladéktalanul értesítenie kell az ügyvezetőt az incidens megtörténtéről. A bejelentés anonim módon is történhet, mely során szükséges jelezni, hogy a felhasználó szeretne anonim maradni. Ebben az esetben a **Rendszergazda** nem adja tovább a bejelentő adatait.

Az összegyűjtött információk alapján a **Rendszergazda** megvizsgálja az incidenst, hogy valóban valós-e, valamint elhárításra szorul. Továbbá azt is ellenőriznie szükséges, hogy az incidens informatikai biztonsági eseményből származik-e.

5.7.1. A biztonsági események kategorizálása

A biztonsági események kategorizálása az alábbi szempontok szerint történik:

- az esemény által érintett rendszerek kritikussága;
- az esemény által érintett munkaállomások, foglalkoztatottak száma;

- az esemény által érintett adatok;
- az esemény által kialakult károk és esetleges károk és hatások mértéke.

5.7.2. Az incidensek kategorizálása

- alacsony kategória
  - kevés foglalkoztatottat érint
  - csak támogató rendszert érint
  - csak nyilvános adatot érint
  - kár értéke minimális
- magas kategória
  - sok foglalkoztatottat érint
  - üzletileg kritikus rendszert is érint
  - bizalmas adatot is érint
  - kár értéke jelentős
- személyes adatokat érintő incidens
  - alapértelmezettként magas kategóriába tartozik
  - bármilyen személyes adatot érint

5.7.3. Kategóriák szerinti intézkedés

Alacsony kategória esetén: A **Rendszergazda** eszkalálja a probléma megoldását az általa kijelölt dolgozó felé. A kijelölt személy javaslatot tesz a probléma megoldására, melyet a **Rendszergazda** jóváhagy. Jóváhagyás esetén a korábban kijelölt személy folytatja az incidens elhárítását, kivéve, ha a **Rendszergazda** mást jelöl ki az incidens megoldására.
Minden kategória esetén: A **Rendszergazda** vezeti az elhárítását az incidensnek, mely során magasabb beosztású vezetők bevonása is szükséges lehet. A későbbi – hasonló – incidensek megelőzése érdekében megoldási javaslatot a **Rendszergazdának** kell tennie, melyet a **Ügyvezetőnek** is jóvá kell hagynia. Jóváhagyás esetén a **Rendszergazda** az általa kidolgozott módon kezdi meg az incidens alap okainak elhárítását.
Szüksége esetén az incidens kivizsgálásába be kell vonni az érintett szállítót is.
Személyes adatokat érintő incidens esetén: A **Rendszergazdának** azonnal értesíteni szükséges az **Ügyvezetőt és az Adatvédelmi tisztviselőt** az incidens mértékéről, és az érintett személyes adatokról, mely után a továbbiakat az **Ügyvezető és az Adatvédelmi tisztviselő** bevonásával szükséges folytatni a magas kategóriában megfogalmazottak alapján.

Az incidensről minden esetben jegyzőkönyvet kell készíteni a mellékletben található sablon alapján.

6. Weboldalakhoz tartozó biztonsági előírások

A Társasághoz tartozó weboldalak üzemeltetését és fejlesztését külső szerződéses partner látja el. A weboldalakon megjelenő tartalmakért a Társaság tartozik felelősséggel. A honlap szakszerű és biztonságos működtetéséért a külső szerződéses partner teljeskörűen felel.

Az weboldalakon lévő adatok védelmére a külső szerződéses partnernek megfelelő biztonsági szintű rendszert és felügyeletet kell üzemeltetnie. Követelmény a magas szinten védett szerverek, valamint a folyamatos biztonsági mentések megléte.

7. Záró rendelkezések

Az Informatikai Biztonsági Szabályzatban érintett dolgozókat évente továbbképzés formájában dokumentált módon tájékoztatni kell a feladataikról és kötelezettségeikről.

Mellékletek

Osztályba sorolás

Megnevezés	Kockázati osztály
Bank	3
Ügyfélkapu	3
Benefit portál	2
Simplepay	2
Jegy.hu és jegyX1.hu	2
Szamlazz.hu	2
Facebook, Instragram	1
Word, Excel, Outlook, Office	1

Melléklet: Biztonsági Incidens jegyzőkönyv

A biztonsági esemény kategórizálása

Érintett rendszer megnevezése:
Érintett rendszer biztonsági osztálya:
Érintett munkaállomások/felhasználók száma:
Érintett adatok köre:

Az incidens kategórizálása

Incidens kategóriája (alacsony, magas):
Személyes adatot érint-e (igen/nem):
Ha igen akkor
érintett adatok köre:
érintett adatok számossága:
hatóság felé jelenteni szükséges (igen/nem):
érintetti tájékoztatás szükséges (igen/nem):

Incidens észlelésének ideje:
Incidens bekövetkezésének ideje:
Incidens elhárításának ideje:
Incidens elhárításában résztvevő személyek:

Incidens leírása:

Incidens hatása:

Incidens közvetlen elhárítására tett intézkedések:

Incidens jövőbeni bekövetkezésének elkerülésére tett intézkedések: