Szent István Egyetem

INFORMÁCIÓBIZTONSÁGI FELHASZNÁLÓI ÚTMUTATÓ

2014. február

Tartalom

1. AZ ÚTMUTATÓ CÉLJA ÉS HATÁLYA

1.1. Az útmutató célja

Az „Információbiztonsági felhasználói útmutató” (továbbiakban útmutató) célja, hogy a Szent István Egyetem (továbbiakban: SZIE) munkatársai, hallgatói, szerződéses partnerei megismerjék azokat a feltételeket, szabályokat, amelyek betartása szükséges a SZIE vezetése által az MSZ ISO/IEC 27001:2006-os szabvánnyal összhangban megfogalmazott információbiztonsági célok megvalósításához. Az útmutató további célja, hogy a felhasználók általános információbiztonsági oktatása alapjául szolgáljon. „Felhasználó” alatt a SZIE informatikai eszközeit és erőforrásait használó dolgozóit és hallgatóit, szerződéses partnereit együttesen értjük. Ahol a felhasználói csoportokra eltérő szabályok és folyamatok vonatkoznak, azokat külön tárgyaljuk.

Az útmutató elolvasásával a felhasználók viszonylag gyorsan tájékozódhatnak az informatikai szolgáltatások igénybevételének, és az eszközök használatának alapvető szabályairól is.

Az üzemeltetők számára a részletes információbiztonsági szabályozást a SZIE Információbiztonsági Szabályzata tartalmazza.

1.2. Az útmutató minősítése

Az útmutató nyilvános használatú dokumentum. A nyilvános használatú dokumentumot a SZIE munkatársai, hallgatói és szerződéses felei megismerhetik és birtokolhatják. (A hallgatókra vonatkozó jogokat és kötelességeket a Tanulmányi és Vizsgaszabályzat *(is)* tartalmazza.).

1.3. Az útmutató hatálya

Az útmutató a SZIE informatikai eszközeit és erőforrásait használó valamennyi felhasználóra vonatkozik. Minden felhasználó személyesen felel a rábízott, vagy általa használt tulajdon és erőforrás védelméért, valamint a SZIE anyagi és szellemi értékeinek megőrzéséért. A SZIE vagyonát érintő sérelemről, vagy sérelem bekövetkezésének közvetlen veszélyéről a közvetlen felettest, vagy az információbiztonsági felelőst tájékoztatni kell. Jogszabályba ütközik, és ezért kártérítési felelősséggel jár minden olyan, a SZIE vagyoni érdekeit sértő magatartás, amely nemcsak a munkatársaktól és hallgatótól elvárt viselkedés normáit sérti, hanem a SZIE-nek kárt is okoz.

Külső cégek munkatársa által végzett tevékenységért a SZIE oldali szerződéskötő a felelős. A külső cégekkel kötött szerződéseknek tartalmazniuk kell, hogy jelen Útmutatót a külsős felhasználók magukra nézve elfogadják és betartják. Külsős felhasználó esetén külön ellenőrizni kell, hogy az igényelt, illetve kiadott jogosultság nem haladja-e meg a munkája elvégzéséhez szükséges mértéket.

1.4. A Dokumentum elosztása

A jelen útmutató aktuális változata a SZIE jelszóval védett honlapján keresztül érhető el, kiadásának bejelentése e-mail-en és/vagy a honlapon keresztül történik. Azon dolgozók, akiknek nincs hálózati hozzáférése, a közvetlen felettesüktől kapnak tájékoztatást.

1.5. Fogalmak

Információbiztonság: Az információ bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzése; továbbá, egyéb tulajdonságok, mint a hitelesség, a számon kérhetőség, a letagadhatatlanság és a megbízhatóság, szintén ide tartozhatnak. [ISO/IEC 17799:2005]

Az információ lehet papír alapon rögzítve, illetve valamely elektronikus adathordozón tárolva.

Sértetlenség (integritás): Az adatok eredeti állapotának, tartalmának, teljességének és hitelességének biztosítása. Az információkat, adatokat, alkalmazásokat csak az arra jogosultak változtathatják meg, és azok véletlenül nem módosulhatnak.

Rendelkezésre állás: Az a tényleges állapot, amikor az információs rendszer eredeti rendeltetésének megfelelő szolgáltatásokat – amely szolgáltatások különbözőek lehetnek – nyújtani tudja (funkcionalitás) meghatározott helyen és időben (elérhetőség), és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.

2. ÁLTALÁNOS TUDNIVALÓK

2.1. Információbiztonsági szervezet

Egyetemi szinten az információbiztonsági feladatokat a főtitkár, a karokon a Hivatalvezető, ennek hiányában a kinevezett rendszergazda látja el, akik az papír alapú információk felügyeletét is ellátják. Kifejezetten informatikai kérdésekben egyetemi szinten az informatikai igazgató az Informatikai központtal (IK), kari szinten a kampusz rendszergazdák (kari informatika) látják el az információbiztonsági irányítási feladatokat.

2.2. Kapcsolattartás az információbiztonsági szervezettel

Információbiztonsági kérdésekben általánosan az információbiztonsági felelőst kell értesíteni. Amennyiben a kommunikáció elsődlegesen informatikai kérdéseket érint, akkor az Informatikai Központtal vagy a kari informatikával kell felvenni a kapcsolatot.

Az elsődleges és kizárólagos érintkezési felület a felhasználók és az IK, illetve a kari informatika között a HelpDesk, ahova a felhasználók, informatikával, információ biztonsággal kapcsolatos problémájukkal, igényükkel fordulhatnak. A HelpDesk elérhető munkanapokon 7:45-16:10 között. A levelező rendszeren keresztüli bejelentés folyamatosan megtehető. A munkaidőn túl érkező bejelentések esetén legkésőbb következő munkanap reggelén kezdi meg a hibaelhárítást az IK vagy a kari informatika.

A HelpDesk elérhetőségei:

- helpdesk@ih.szie.hu
- Központi HelpDesk telefonszám: 28/522 000, 1205 mellék
- Személyesen: Gödöllői Kampusz, Főépület, Forrásközpont 122

További információbiztonsági bejelentések esetében használandó elérhetőségi adatok az _1. számú mellékletben találhatóak.

2.3. Információk osztályozása

A SZIE-nél kezelt adatok osztályba vannak sorolva, annak érdekében, hogy az egyes adattípusokhoz különböző védelmi intézkedéseket lehessen rendelni. Az információk

osztályozását bizalmasság, sértetlenség, és rendelkezésre állás szempontjából osztályozni kell, amelyet az alábbi három szinten kell megvalósítani.

Osztályozási szintek	Bizalmasság	Sértetlenség	Rendelkezésre állás	Adatkezelés alapvető előírásai
1. Nyilvános	Nyilvános	Nem védett	Általános	Központi tároló helyen kell/lehet tárolni
2. Bizalmas	Bizalmas (belső használatra)	Védett	Fontos	Személyes, vagy korlátozott hozzáférésű mappában/dossziéban (elzárva) kell tárolni.
3. Titkos	Titkos	Fokozottan védett	Kritikus	Titkosított mappában/dossziéban (elzárva) kell tárolni.

Az egyes biztonsági osztályba sorolt adatokhoz, és az adatokhoz tartozó adatkezelő-rendszerekhez, infrastrukturális elemekhez különböző szintű védelmi intézkedések vannak hozzárendelve.

Az adatkezelés részletes szabályozását a SZIE Információbiztonsági szabályzata, illetve a SZIE Adatvédelmi szabályzata határozza meg.

Az oktatói, oktatástámogató adatok besorolását a 2. számú melléklet mutatja be. Részletesebb információt az információbiztonsági felelős adhat, illetve a besorolás magán a dokumentumon, adathordozón kerül feltűntetésre.

3. HOZZÁFÉRÉS IGÉNYLÉSEK MENETE

3.1. Dolgozói jogosultság igénylés

A SZIE dolgozói számára a rendszerhez való hozzáférési jogosultságot elektronikus vagy papír alapon, a SZIE iktatási és dokumentum-kezelő rendszerében rögzítetten, a munkavállaló felettese igényelhet.

A központi jogosultságigénylés menete a következő:

1. Igénylés elküldése az adott rendszer adatgazdájához;
2. Igény elbírálása, pozitív döntés esetén továbbítása az IK-hoz;
3. Jogosultság beállítása, visszajelzés az igénylőnek.

Nem a szabályozott csatornán és formában érkező igényeket az IK nem hajtja végre.

A kari üzemeltetésben lévő szolgáltatásokhoz jogosultságok igénylése az érintett kar Dékáni Hivatalában történik.

3.2. Hallgatói jogosultság igénylés

A tanulmányi rendszerben aktív jogviszonnyal rendelkező hallgatók automatikusan hozzáférést kapnak a központi azonosítást használó rendszerekhez (pl.: webmail, e-learning, WiFi, egyetemi honlap, kari honlapok). Ezt az egységes SZIE azonosítóval tudják elérni, ami megegyezik a Neptun kóddal. Hallgatók esetében is biztosított az „egy felhasználó - egy felhasználói azonosító” elv. A hallgatói azonosítókra és jelszavakra is vonatkoznak a SZIE dolgozói azonosítókra, jelszavakra vonatkozó előírások és szabályozások, amelyek részletesen a SZIE Informatikai Biztonsági Szabályzatában találhatóak meg.

4. INFORMATIKAI ESZKÖZÖK HASZNÁLATA, FELHASZNÁLÓI MAGATARTÁS

4.1. Számítógépek és tartozékaik

A SZIE a dolgozói számára biztosítja a munkaköri leírásukban foglalt feladataik elvégzéséhez szükséges informatikai eszközöket.

Az Egyetem minden hallgatója számára biztosítja a tanulmányok folytatásához szükséges informatikai erőforrások elérését a SZIE által felszerelt oktató és nyilvános termeiben.

Az Egyetem által biztosított informatikai eszköz munkaeszköznek minősül, átvétele után a felhasználó felel annak épségéért. Bármi nemű műszaki rendellenességet, sérülést, alkatrészek hiányát a felhasználó köteles haladéktalanul jelezni telefonon/személyesen az illetékes informatikai rendszergazdának.

A SZIE tulajdonában lévő informatikai eszközöket tilos személyes célra felhasználni.

A SZIE által az alkalmazottak, vagy a csoportok munkájához biztosított informatikai eszközöket csak a SZIE tevékenységi és érdekeltségi körébe tartozó célokra szabad használni. Minden olyan elektronikus dokumentum, amely a munkahelyi feladatok ellátása folyamán keletkezik, a SZIE tulajdonát képzi. Az informatika indokolt esetben hozzáférhet a rendszerein tárolt dokumentumokhoz, levelezéshez. A hozzáférés idejéről, okáról jegyzőkönyvet kell felvenni. Ilyen indok lehet pl. biztonság probléma, jogi követelmény.

Az Egyetem tulajdonában lévő, a fixen telepített illetve a felhasználó által használt informatikai eszközök fizikai helyének, konfigurációjának megváltoztatása (pl. alkatrészek cseréje, hozzáadása, átkábelezés) csak az IK vagy a kari informatika jóváhagyásával, felügyeletével történhet. A SZIE fenntartja a jogot rendszerei felügyeletére, a szabályszerű használat biztosítása, elszámolás, és a biztonsági szabályok megszegésének felderítése végett.

A mobil eszközök (pl. notebook, netbook, palmtop, tablet, mobil illetve okos telefon, pendrive, külső merevlemez stb.) hordozhatósága miatt a rajta tárolt – bizalmas és/vagy titkos – adatok igen veszélyeztetettek, ezért ezen eszközöket megkülönböztetett figyelemmel kell kezelni, hogy azok ne kerülhessenek illetéktelen kezekbe. Használója felelős a berendezés megfelelő tárolásáért és a rajta található adatok biztonságáért.

4.2. Nyomtatók

Az elektronikusan rendelkezésre álló iratokat elektronikusan kell továbbítani, ezért csak a legszükségesebb esetben szabad azokat kinyomtatni. Ilyen esetben is törekedni kell a költség-kímélő megoldások (kétoldalas nyomtatás, festékkímélő üzemmód) használatára.

Tilos a SZIE tulajdonában lévő nyomtatók magáncélú használata.

4.3. Kommunikációs eszközök használata (telefon, mobiltelefon, telefax, telex, videokonferencia)

Tilos belső, bizalmas adatok közlése, megvitatása titkosítatlan csatornákon.

Bizalmasnak vagy titkosnak minősülő adatokat soha ne küldjünk sms, mms vagy fax üzenetben. Az Egyetemen belül tilos bármilyen adat faxon történő továbbítása.

5. SZOLGÁLTATÁSOK ÉS ALKALMAZÁSOK IGÉNYBEVÉTELE

5.1. Alkalmazások igénybevétele

5.1.1. Alkalmazások, szoftverek használata

A felhasználók alapértelmezésben az IK vagy kari informatika által egységesen telepített programcsomagot kapnak számítógépükre. Egyéb alkalmazást, illetve az ahhoz való hozzáférést a 3.1. pontban leírtak szerint lehet igényelni. A használattal kapcsolatos kérdéseket, eset-leges oktatási igényeket a HelpDesk, kari informatika felé kell jelezni.

A SZIE minden dolgozója számára biztosítja a munkavégzéshez szükséges szoftverhasználatot. A szerzői jog által védett számítógépes szoftverek bármilyen illegális, a jogtulajdonos engedélye nélküli használata, másolása törvénybe ütköző cselekedet, és mint ilyen határozottan ellenkezik a SZIE szoftverhasználati politikájával. (Ebbe bele tartozik az időkorlátos programok időn túli használata és az időkorlát kijátszása is). Ezért a SZIE tulajdonában lévő, bárhol üzemeltetett számítógépeken csak olyan engedélyezett, jogtiszta szoftvereket szabad használni, amelyeket a SZIE bocsát a felhasználók rendelkezésére.

A számítógépre történő szoftvertelepítést csak a kari rendszergazdák, illetve az IK munkatársai, végezhetik el. A munkavállalók gépükre szoftvereket önállóan nem telepíthetnek, nem másolhatnak fel. Az IK nyilvántartást vezet a telepített szoftverekről és csak az általa telepített, legális szoftverekkel kapcsolatosan vállal felelősséget és nyújt felhasználói támogatást.

A SZIE által vásárolt felhasználási-, vagy tulajdonjoggal rendelkező (licensz) szoftverek a SZIE vagyonát képezik, ezért tilos ezeket az Egyetem telephelyeiről adathordozón kivinni, külső személy vagy cég részére átadni, másolni, vagy hozzáférhetővé tenni - beleértve a hálózaton vagy Interneten való hozzáférés lehetőségét is - kivéve, ha erről a SZIE-vel kötött szerződések másként rendelkeznek.

Az IK a telepített szoftvereket bármikor ellenőrizheti, és az illegálisan telepített szoftvereket a számítógépről és a hálózatról előzetes figyelmeztetés nélkül törölheti és erről a felhasználót, valamint a felhasználó felettes vezetőjét utólag értesíti.

5.1.2. Jelszavak kezelése

A felhasználók az alkalmazásokhoz, szolgáltatásokhoz való hozzáférés kiadásakor felhasználó-azonosítót és jelszót kapnak. A kapott jelszót a felhasználónak az első belépés alkalmával meg kell változtatnia. A felhasználó köteles titokban tartani jelszavát, és kompromittálódás gyanúja (ha a jelszót más is megismerhette) esetén azonnal meg kell változtatnia.

A jelszavaknak meg kell felelnie az alábbi alapkövetelményeknek:

- A jelszavak tartalmazzanak numerikus és alfabetikus karaktereket (betűket és számokat egyaránt).
- Ne tartalmazzon ékezetes betűket és szóközöket, bármilyen nyelvű szót szótári alakban.
- Ne egyezzen meg a felhasználó nevével, felhasználói azonosítójával, egyik telefonszámával sem, engedélyének számával, személyi számával vagy dolgozói kódjával, valamint a felhasználóhoz kötődő bármely karaktersorozattal (pl. születési dátum, lakcím, gépkocsi rendszám, stb.).

- Ne egyezzen meg személynévvel, irodalmi, színházi, televíziós, közéleti személyek nevével és egyéb közismert szavakkal, kifejezésekkel.
- Ne tartalmazzon azonos, vagy ismert logika szerint egymást követő karaktereket (pl. 11111, qwert, stb.).
- Ne utaljon a felhasználóra, munkakörére, munkahelyére.

A jelszóhasználat további szabályai:

- A felhasználóknak meg kell változtatniuk a jelszavukat, amikor első alkalommal használják felhasználói azonosítójukat.
- A rendszer megtagadja a hozzáférést 6 hibás jelszó megadása után.
- A hibás próbálkozásokat követően a rendszer 30 percre blokkolja a fiókot.
- Hálózatba kötött, vagy bizalmas adatok tárolására használt informatikai eszközök esetében félévente a jelszó változtatása kötelező.

Amennyiben a felhasználó a jelszót elfelejti, a HelpDesk-hez fordulhat, aki intézkedik az új jelszó kiadásáról, amelyet a felhasználónak - akár a belépésekor kapott jelszót – az első belépés alkalmával meg kell változtatnia.

Más felhasználó hozzáférési jogosultságával (jelszavával) való visszaélés, az engedélyezett jogosultságtól eltérő használat kísérlete a SZIE alaptevékenységét és jogos gazdasági érdekeit veszélyezteti, amelynek súlyos jogi következményei is lehetnek.

5.2. Távoli elérés

Távoli hozzáférés a SZIE Internet kapcsolatain keresztül üzemeltetett biztonságos, virtuális magánhálózat kialakításával (VPN) valósulhat meg.

Távoli hozzáférési jogosultságot a 3.1. pontban ismertetett módon lehet igényelni. Távoli hozzáféréssel történő munkavégzés szabályai:

- A távoli elérés csak működő személyi tűzfal, illetve vírusvédelmi szoftver mellett kezdeményezhető.
- A távoli elérés alatt tilos más - nem az aktuális munkával kapcsolatos - tevékenység folytatása. A távoli elérés alatt használt erőforrásokat csak szükséges időtartamra szabad foglalni. A nem használt hozzáféréseket be kell zárni.

A távoli elérés során a vírusvédelemmel kapcsolatos információkat a 6.5. pont foglalja magában.

5.3. A levelezőrendszer használata

A SZIE valamennyi dolgozója, hallgatója számára biztosítja a levelezőrendszer használatát. A jogosult felhasználók rendelkeznek saját postafiókkal, amihez felhasználónév és jelszó tartozik, amelyeket a felhasználó a jogosultság életbelépésekor kap meg. Minden postafiókkal rendelkező felhasználó megtalálható a címlistában, amelyben egyéb adatok (pl.: telefon, szervezeti egység, beosztás, stb.) is megtekinthetőek.

A postafiókok mind a belső, mind az Internetes (külső) levelek fogadására, küldésére alkalmasak. A SZIE postaláda a SZIE hivatalos feladatait, alaptevékenységét szolgálja.

Az IK minden SZIE e-mail címre érkezett, és arról küldött levélhez hozzáférhet hivatalos belső vizsgálat esetén.

Az elektronikus levelezéssel kapcsolatos tiltó rendelkezések az alábbiak:

- Szigorúan tilos a közízlést sértő, a SZIE jó hírnevét veszélyeztető, erkölcstelen, vagy politikai tartalmú e-mail elküldése.
- Tilos a levelező rendszert „Titkos” minősítésű fájlok, dokumentumok kijuttatására használni.
- Tilos a SZIE hivatalos ügyeket nem egyetemi levélcímen intézni. Tilos olyan levelek továbbítása a SZIE levelező rendszerében, amelyek bármilyen nyelven arra szólítanak fel, hogy a levelet minél több címre kell továbbítani (lánclevél). Ha lánclevelet vagy vírusfigyelmeztetést kapunk, ne továbbítsuk azt másoknak! Küldjünk értesítőt vagy másolatot a HelpDesk-nek, kari informatikának, akik a kellő intézkedéseket meg fogják tenni.
- Tilos válaszolni olyan levelekre, amelyek arra szólítanak fel, hogy a SZIE biztonsági rendszeréről, vagy a felhasználó saját hozzáférési adatairól (felhasználónév, jelszó) adjon tájékoztatást. Ha e-mailt küldünk vagy továbbítunk az Internetre, tilos bármely SZIE felhasználói azonosítót vagy jelszót mellékelni.
- Tilos a nem SZIE-és e-mailszolgáltatás (pl.: Freemail, Gmail, Yahoo, Hotmail, stb.) használata hivatalos vagy bizalmas információ küldésére vagy fogadására.
- Gyanús e-mailekről (pl.: szokatlan küldő, tárgy, csatolt fájl) azonnal, még megnyitásuk előtt értesíteni kell a HelpDesk-et, kari informatikát.

A bejövő és kimenő leveleken a rendszer automatikus vírusellenőrzést hajt végre. A vírusfertőzés bekövetkezésének csökkentése érdekében a levelekhez csatolt különböző fájlok is ellenőrizhetőek.

5.4. Az Internet használata

5.4.1. Hozzáférés

Az Internet használatát a SZIE a munkavégzéshez, tanuláshoz biztosítja a jogosult felhasználók számára.

A SZIE a tanulmányi és ehhez kapcsolódó adminisztrációs feladatok ellátásához hallgatói számára, az NIIF hálózaton keresztül, Internet hozzáférést biztosít.

5.4.2. Használat szabályai

A megtekintett oldalak, letöltések, illetve azok naplófájlja az IK számára hozzáférhető, azok alapján az IK jogosult az Internet forgalom követésére, mérésére, és a vezetőség kérésére arról részletes, az egyes munkaállomásokra, felhasználókra vonatkozó kimutatást készíteni.

Felmerülő igény esetén a felhasználónak közvetlenül a HelpDesk-hez, kari informatikához kell fordulnia. A felhasználóknak csak a munkához, tanuláshoz szükséges dokumentumok letöltése engedélyezett.

Ha az Internetet a szie.hu vagy más kifejezetten SZIE-es címről érjük el:

- Soha se adjuk ki magunkat másnak.
- Csak olyan szolgáltatásokat vegyünk igénybe, melyekre jogosultak vagyunk. Előzetes feljogosítás nélkül ne próbáljunk meg Internetes rendszereket vagy szerver pontokat elérni.

- Tilos biztonsági tesztberendezéseket és programokat használni, bármely Internetes rendszer vagy szerver ellen.

5.4.3. További rendelkezések

Tilos az Interneten olyan oldalak látogatása, illetve anyagok elhelyezése vagy küldése, melyek helytelennek, sértőnek vagy másokkal szemben tiszteletlennek tekinthetők. Szigorúan tilos a SZIE érdekeit sértő, erkölcstelen oldalak látogatása, bővebb szabályozást a SZIE Informatikai Szabályzat tartalmaz, mely hivatkozik a Nemzeti Információs Infrastruktúra Fejlesztési Program Felhasználói Szabályzatára (http://www.niif.hu/niif_intezet/aup).

Szigorúan tilos internetes illegális tevékenységek folytatása, amelyek más jogi személyek adatainak, alkalmazásainak bizalmasságát, sértetlenségét, vagy rendelkezésre állását sértheti (hack, crack, flood, stb.). Szigorúan tilos minden, a közízlést sértő, erkölcstelen állomány letöltése.

A SZIE fenntartja a jogot, hogy biztonsági okokból technikai szűréseket és korlátozások rendeljen el az informatikai igazgató által.

5.5. Vezeték nélküli hálózatok

A SZIE dolgozói, hallgatói számára az intézmény területén vezeték nélküli (WiFi) hálózatok használatát biztosítja, ahol erre a technikai feltételek adottak. A vezeték nélküli hálózathoz való csatlakozás hitelesítő adata a SZIE azonosító és jelszó.

5.6. A szie.hu honlap használata

Az Egyetem hivatalos honlapjának címe http://www.szie.hu, melyről elérhetőek az egyes szervezeti egységek honlapjai. A karok hivatalos weboldalaikat maguk üzemeltetik.

A „Munkatársaknak” menüpont alatt felhasználói azonosítást követően belső információkhoz juthatnak (pl.: szabályzatok, tájékoztatók stb.).

5.7. Hallgatói rendszerek (Netpun, e-learning portál) használata

A SZIE-nél alkalmazott hallgatói rendszerek a hallgatók adminisztrációs és tanulmányi munkáját segítik. A rendszerek többféle szolgáltatással segítik a gyors ügyintézést, mint például vizsgára való jelentkezés, fizetés kezdeményezése, adatok megosztása, stb. A rendszerek igénybevételére azonosítást követően kerülhet sor.

A tanulmányi rendszerekben a hallgató egyértelmű azonosítása, a hallgató számára kiadott, egyedi felhasználói azonosító és jelszó alapján történik. A felhasználói azonosító és jelszó illetéktelen kezekbe kerülve visszaélésekre adhat alkalmat, ezért fokozottan javasoljuk, hogy a hallgatók saját érdekükben ezeket bizalmasan kezeljék. A hallgatói azonosítókkal való visszaélésekből származó következményekért a SZIE semmilyen felelősséget nem vállal. Bármilyen módon (véletlenül vagy akár jó szándékkal, tudatosan) kiadott vagy kitudódott jelszó esetén azonnal meg kell változtatni a jelszót és kötelező értesíteni az illetékes tanulmányi hivatalt!

A helyes jelszóhasználattal kapcsolatban további információt nyújt az 5.1.2-es pont. A hallgatói rendszerekben alkalmazott jelszó- és adatkezelésre az érvényben lévő törvényi és a SZIE Informatikai Biztonsági Szabályzatában meghatározott rendelkezések vonatkoznak.

A hallgatói rendszerekre csak olyan anyagok, információk tölthetőek fel, amelyek tartalma megfelel a SZIE értékrendjének, közízlést nem sért, és összhangban van a SZIE hivatalos nyilatkozataival. A SZIE jó hírét veszélyeztető, erkölcstelen vagy politikai tartalmú anyagok feltöltése tilos.

5.8. Alkalmazotti munkaállomásokra vonatkozó előírások

A munkaállomások képernyőit úgy kell elhelyezni, hogy a képernyőkön megjelenésre kerülő adatokat illetéktelen személyek ne tudják leolvasni.

Munkaállomást csak abban az esetben szabad felügyelet nélkül hagyni, ha a munkaállomáson jelszó védelemmel rendelkező képernyővédőt alkalmaznak, vagy a munkaállomást zárolják.

Rendszergazda jogosultságú felhasználóval csak az ilyen jogosultságú feladat elvégzésének idejére szabad bejelentkezni a munkaállomásra, ezután ki kell jelentkezni. A feladat elvégzése alatt a munkaállomást felügyelet nélkül hagyni, vagy a munkaállomáson egyéb tevékenységet folytatni szigorúan tilos.

„Üres asztal – tiszta képernyő" szabály

- A papíranyagokat és adathordozókat zárható szekrényben kell őrizni/tárolni, amikor éppen nincsenek használatban, főként a munkaidőn kívüli időszakban.
- Amennyiben sajátos információbiztonsági előírások vannak érvényben egy szervezeti egységnél, akkor a dokumentumokat azon előírások alapján kell tárolni.

6. ADATBIZTONSÁG, ADATHORDOZÓK

6.1. Adatok kezelése, tárolása

A felhasználónak adattárolásra a következő eszközökön van lehetősége:

- Hálózati meghajtók (központi fájlszerver);
- A helyi számítógép meghajtója;
- Floppy, CD, DVD, Pen Drive (USB kulcs) és egyéb hordozható adattárolók.

Az IK és a kari informatika kizárólag a hálózati meghajtókon tárolt adatok biztonságáért vállal felelősséget. A helyi meghajtókon, és az adathordozókon tárolt adatok biztonságáért, bizalmasságáért a felhasználó tartozik felelősséggel!

Emiatt általában is, de a SZIE számára fontos állományok esetében különösen javasolt a hálózati meghajtók használata a biztonságos adattárolás érdekében.

A SZIE informatikai eszközein csak a felhasználó munkájával, tanulmányaival kapcsolatos adatok tárolhatók. Minden ilyen adat a SZIE tulajdonának minősül. Az adatok védelme az adathordozó fajtájától független. A rendszerből papírra kinyomtatott, fájlba exportált adatokhoz való hozzáférés szintjének meg kell, hogy egyezzen a rendszerbeli adatbiztonsági szintjével. Valamely rendszerhez jelszavas hozzáféréssel rendelkező felhasználó a rendszerből nyomtatott adatokat, exportált fájlokat nem tarthatja, tárolhatja hozzáféréssel nem rendelkező felhasználók által elérhető helyen.

A SZIE megköveteli a fokozottan védett adatok titkosítását, amennyiben azok az Interneten, nyilvános hálózatokon vagy vezeték nélküli berendezéseken kerülnek továbbításra.

Amennyiben más cég bizalmas adatait kapjuk meg, kötelesek vagyunk betartani annak a cégnek az adatvédelmi utasításait is. Bármely adatvédelemmel kapcsolatos kérdést a vezetőkkel, az információbiztonsági felelőssel vagy a jogi iroda munkatársaival egyeztesse.

Megszűnő jogviszonyú felhasználó és ideiglenesen a SZIE-nél dolgozó külső szakértő távozása esetén az általa használt és tárolt adatok fontosak lehetnek az adott területen tovább

dolgozók számára. A távozó személy adatainak kezeléséért, azok további elhelyezéséért a felhasználó felettese, illetve külső szakértő esetén a szerződéskötő vagy kapcsolattartó a felelős.

6.2. Adatok védelme

Egyre több alkalmazott dolgozik külső munkakörnyezetben. Az alábbi lista összefoglalja mindazon feltételeket, szempontokat és ajánlásokat, melyek a SZIE belső szellemi tőkéjének védelmére vonatkoznak. Az adott körülményektől függően további erőfeszítések is szükségesek lehetnek.

- Zárjunk el minden bizalmas információt tartalmazó eszközt, adatot és anyagot, amikor nem használjuk. Munkaállomásunkat védjük jelszóval. Zároljuk munkaállomásunkat, ha felügyelet nélkül hagyjuk.
- Csak a SZIE IK és kari informatika által jóváhagyott vezeték nélküli hálózati és mobiltechnológiát használjunk.
- Soha ne hagyjunk bizalmas üzeneteket hangposta rendszereken.
- A SZIE Informatikai rendszerhez és hálózathoz való külső kapcsolódáshoz, jóváhagyott távoli hozzáférési jogosultsággal kell rendelkeznünk. Az IK és kari informatika segíthet a biztonságos és stabil kapcsolat kialakításában.
- ***Az adatok fokozott védelme érdekében a mobil eszközöket havonta legalább egy alkalommal, a SZIE hálózatára kell csatlakoztatni.*** Ekkor a vírusvédelmi rendszer, valamint a telepített alkalmazások frissítését végre kell hajtani. Ugyanekkor az adathordozók vírusellenőrzését is el kell végezni.

6.3. Bizalmas és titkos adatok kezelése

A személyhez kötődő információ gyűjtését, tárolását, felhasználását, közlését és továbbadását adatvédelmi törvény szabályozza. Ide tartoznak az alkalmazottakról szóló személyes információk, és a SZIE alaptevékenysége során másokról megszerzett adatok is (pl. dolgozói vagy hallgatói adatok).

Minden bizalmas adatot kezelő SZIE dolgozó, akinek az informatikai rendszerekhez, alkalmazásokhoz jogosultsága van, írásban nyilatkoznak a SZIE vezetése által meghatározott adatvédelmi és titoktartási szabályok betartásáról. Az adatvédelmi és titoktartási szabályok be nem tartása jogi felelősségre vonást von maga után.

A bizalmas és titkos dokumentumok kezelésében minden munkatársnak kötelessége a SZIE biztonsági irányelvei alapján eljárni. Az üzleti titkokat tartalmazó dokumentumokat, vagy elektronikus adathordozókat szemétbe dobni tilos! Azokat iratmegsemmisítővel meg kell semmisíteni illetve használhatatlanná kell tenni.

A SZIE tulajdonában levő minősített adatokat (bizalmas, illetve titkos) a minősítésnek megfelelően kell kezelni. Az adatokat a SZIE Információbiztonsági Szabályzatában és a SZIE Adatvédelmi Szabályzatában leírtak szerint kell kezelni.

6.4. Mentés, archiválás

A hálózati szervereken tárolt adatokról az IK és kari informatika rendszeresen mentéseket készít, így adatvesztés esetén az adatok visszaállítása lehetséges. Ilyen jellegű kérésekkel a HelpDesk-hez, kari informatikához kell fordulni.

Az adatok védelme érdekében minden a munkakörrel összefüggő dokumentumot a fájlszerverre (közös könyvtár) kötelező felmásolni.

Az IK és kari informatika csak a központi erőforrásokon (hálózati meghajtók) tárolt adatokról készít mentéseket, így a helyi és hordozható adattárolókon tárolt adatok visszaállítására nincs lehetősége.

A helyi és hordozható adattárolókat érintő adatvesztéskor az adatok helyreállítása, korábbi állapotra való visszatérés a felhasználó felelőssége és feladata.

6.5. Vírusvédelem

A SZIE-nél a vírusvédelem központilag irányított folyamat. A vírusellenőrzés és irtás automatikus a levelezés, Internet-használat, és a fájl-műveletek során. A felhasználóknak nincs semmilyen teendőjük a rendszer működtetésével. Az IK és kari informatika által felügyelt számítógépeken a vírusellenőrző szoftver vírusdefiníciós állománya automatikusan frissül. Az IK és a kari informatika által közvetlenül nem felügyelhető számítógép (pl. otthon használt saját gép) vírusvédelméért a felhasználó a felelős.

A vírusirtó szoftver futása időnként a számítógép lassulását eredményezheti, azonban a vírusirtó szoftver eltávolítása, működésének megakadályozása semmilyen körülmények között nem engedélyezett. Az ebből eredő károkért (pl. vírusfertőzés, adatvesztés) a rendszer működését akadályozó felhasználó a felelős.

A felhasználóknak tilos a munkaállomásukon, hordozható számítógépükön alkalmazott vírusvédelmi szoftver aktív védelmének kikapcsolása, vagy a védelmi beállítások megváltoztatása.

Vírusfertőzés gyanúja esetén a felhasználóknak kötelességük a HelpDesk-hez, illetve az adott kari informatikához fordulni.

7. RENDKÍVÜLI ESEMÉNYEK, INCIDENSEK KEZELÉSE

A SZIE biztonsági incidensnek tekint minden, az informatikával kapcsolatba hozható rendellenes működést, fenyegetést, amely az adatok bizalmasságát, sértetlenségét, vagy rendelkezésre állását veszélyezteti.

Ha megtörtént, vagy folyamatban lévő biztonsági incidenst észlelünk, fontos hogy azonnal cselekedjünk, és értesítsük az IK-t. A felhasználóknak tilos megkísérelni a támadóval szembeni nyomozást vagy ellenlépéseket tenni kivéve, ha kifejezetten erre utasítja a SZIE IT szervezete. Az IT megfelelő gyakorlattal és képzettséggel rendelkezik arra, hogy helyreállítsa a biztonságot, csökkentse a következményeit és lefolytatassa a vizsgálatot, ami akár a bizonyítékok beszerzését vagy a lehetséges jogi eljárást is magában foglalhatja.

Minden felhasználó köteles az általa észlelt hibás program, illetve informatikai eszköz működését a HelpDesk-nek, kari informatikának bejelenteni.

8. DOLGOZÓI, HALLGATÓI FELELŐSSÉGVÁLLALÁS

Az adatok, dokumentumok és informatikai eszközök megfelelő használata közvetve vagy közvetlen védelmet nyújt az információvesztés vagy az információ jogosulatlan személyhez való kerülése ellen. A dolgozói, hallgatói felelősségvállalás a rendszerhez való hozzáférés egyik alapfeltétele.

A felelősségvállalás célja a felhasználókban tudatosítani, hogy munkájuk során a lehető legnagyobb gondossággal járjanak el a SZIE információs rendszereiben tárolt információk használatakor, annak érdekében, hogy az adatok bizalmassága, sértetlensége, és rendelkezésre állása a felhasználó szándékos, vagy gondatlan magatartásából ne sérüljön, illetve a felelősségük számon kérhető legyen.

Ennek érdekében felhasználóinkat tájékoztatjuk információbiztonsági kötelezettségükről, szükséges esetén képzést szervezünk.

Az Informatikai felhasználói útmutatóban leírtak megszegése munkajogi, kártérítési és büntetőjogi felelősséggel jár. Az előírások súlyos megsértése esetén kártérítési, büntetőjogi eljárás indulhat a szabálysértő személyével szemben.

A „Információbiztonsági felhasználói útmutató” megismerését és elfogadását „Felhasználói nyilatkozatban” (5. számú melléklet) kell dokumentálni, mely a személyi dossziéban kerül lefűzésre.

9. KAPCSOLÓDÓ DOKUMENTUMOK

- SZIE Információbiztonsági Szabályzat
- SZIE Informatikai Szabályzat
- SZIE Adatvédelmi Szabályzat

Hatályba léptető rendelkezések

Jelen módosított Információbiztonsági felhasználói útmutatóban foglaltakat 2014. február 26-tól kell alkalmazni, egyúttal a 2012. november 1. napjától hatályos útmutató módosított rendelkezései hatályon kívül kerülnek. Az útmutatóban előírtakat a hatálybalépéstől folyamatosan kell alkalmazni a felhasználói nyilatkozattétellel összhangban.

Gödöllő, 2014. február 25.

Dr. Tőzsér János
rektor

1. SZÁMÚ MELLÉKLET

Információbiztonsági elérhetőségek:

SZIE Kar	Telefon	E-mail	Terület
SZIE RH Gödöllő	28/ 522-000 mellék: 1010; mobil: 30 256 0313	magyar.ferenc@fh.szie.hu	papír alapú adatkezelés
SZIE IK Gödöllő	28/ 522-000 mellék: 1911; mobil: 30 894 8178	gal.gyorgy@fh.szie.hu	informatika
SZIE IK Gödöllő	28/ 522-000 mellék: 1290; mobil: 20 4916580	lajber.zoltan@ih.szie.hu	informatika
SZIE GK Békéscsaba	66/ 524-700 mellék: 1024	karolyi.andras@gk.szie.hu	papír alapú adatkezelés
SZIE GK Békéscsaba	66/ 524-700 mellék: 1016	streit.janos@gk.szie.hu	informatika
SZIE GK Szarvas	66/ 311-511 mellék: 2230	otta.endre@gk.szie.hu	informatika
SZIE GK Gyula	66/ 561-620 mellék: 122	sandor.papp@gk.szie.hu	informatika
SZIE ABPK Szarvas	66/ 311 511 mellék: 3137	almasi.zoltan@abpk.szie.hu	papír alapú adatkezelés, informatika
SZIE ABPK Jászberény	57/ 502-444	bagi.zsolt@abpk.szie.hu	informatika

Adatok aktualizálva: 2014-01-24

2. SZÁMÚ MELLÉKLET

Oktatói, oktatástámogatói, kutatói adatok besorolása (a megadott listák nem teljes körűek):

Nyilvános/Nem védett	Bizalmas/Védett	Titkos/Fokozottan védett
▪ Jogszabályi előírások ▪ Szabályzatok ▪ Integrált irányítási kézikönyv ▪ Munkatársak elérhetősége ▪ Szakalapítás, szakindítás dokumentumai ▪ Órarendek ▪ Hallgatói hirdetmények ▪ Képzési tájékoztatók ▪ Tantárgyi programok ▪ Álláspályázatok ▪ Elfogadott költségvetés, beszámoló ▪ Jelentkezési lapok formái ▪ A Szent István Egyetem lapja ▪ …	▪ Oktatók asztali számítógépein tárolt oktatáshoz kapcsolódó anyagok, tananyagok ▪ Nem nyilvános kutatási eredmények ▪ Elfogadott intézményfejlesztési terv, kidolgozás alatt lévő stratégiák ▪ Számítógépen tárolt zárthelyi és vizsgadolgozatok, dolgozatok ▪ Belső előíró dokumentumok (pl.: eljárások, utasítások) ▪ Iratminták ▪ Szenátusi ülések jegyzőkönyvei, határozatok ▪ Terheléstáblák ▪ …	▪ Munkatársak és hallgatók személyi anyagai ▪ Leckekönyvek, személyes iratgyűjtők tartalma ▪ Tanulmányi adatok ▪ Felvételi adatok ▪ Hallgatói email lista dpr-hez ▪ Irattári dokumentumok ▪ Oktatók hallgatói véleményezésének eredménye ▪ Titkosított szakdolgozatok ▪ Titkosított kutatási eredmények ▪ Vagyonleltár, kockázatértékelések, vészhelyzeti tervek ▪ Központi címtár (LDAP) ▪ …

3. SZÁMÚ MELLÉKLET

Jogosultság igénylő űrlap	
Szolgáltatás (igénylő tölti ki)	
Szolgálgatás megnevezése	
Jogosultsági szint/szerepkör	
Jogosultság indoklása	
Mikortól, meddig éljen a jogosultság -tól -ig	
Igénylő adatai (igénylő tölti ki)	
Igénylő neve	
Igénylő szervezeti egység	
Igénylés dátuma	
Jogosultság alanya (igénylő tölti ki)	
Munkavállaló neve	
SZIE azonosítója (3betű 4 szám)	
Szervezeti egység, amire a jogosultság vonatkozik	
Elbírálás adatai (szolgáltatás adatgazdája tölti ki)	
Elbírálás dátuma	
Elbírálás	
Elutasítás esetén Indoklás	Jóváhagyva Elutasítva Módosított jogkörrel jóváhagyva
Elbíráló neve	
Beállító adatai (jogosultság beállító tölti ki)	
Beállítás dátuma	
Beállító	

4. SZÁMÚ MELLÉKLET

Központi szolgáltatások adatgazdái:

Szolgáltatás	Adatgazda	E-mail
EOS	Biró Terézia	Biro.Terezia@gfh.szie.hu
Gólya	Dr. Tóth Tamás	oktatasi.rektorhelyettes@szie.hu
KIR3	Buza Erika	Buza.Erika@gfh.szie.hu
Kontroller2	Magyar Ferenc Attila	fotitkar@szie.hu
Moodle/e-learning	Berze Lajos	Berze.Lajos@lib.szie.hu
Neptun	Dr. Tóth Tamás	oktatasi.rektorhelyettes@szie.hu
Nexon	Buza Erika	Buza.Erika@gfh.szie.hu
SZIE honlap	Slániczné Molnár Ildikó	Slaniczne.Molnar.Ildiko@fh.szie.hu

Adatok aktualizálva: 2014-01-24

5. SZÁMÚ MELLÉKLET előlap

FELHASZNÁLÓI TÁJÉKOZTATÓ

(A SZIE Információ Biztonsági Rendszerének alkalmazásához)

A SZIE informatikai rendszerének felhasználási feltételei szabályozottak, melyek betartása minden munkatárs számára kötelező. A szabályzatok a SZIE intraneten valamennyi munkatárs számára hozzáférhetőek, azonban azok külső terjesztése nem engedélyezett.

A SZIE Informatikai szabályzat rögzíti:

- az egyetemi felhasználói jogokat, kötelességeket, tilalmakat és szankciókat,
- a SZIE számítógépes hálózatának (SZIENET) működését, használati rendjét, szolgáltatásait,
- a számítástechnikai eszközök használatának rendjét, illetve
- az elektronikus szolgáltatásokat (pl. elektronikus levelezés, honlap, portál szolgáltatások, elektronikus hallgatói nyilvántartó rendszer).

A felhasználókra vonatkozó előírások gyakorlati támogatására készült az Információbiztonsági fel-használói útmutató, melynek betartása szintén valamennyi munkatárs számára kötelező. Az információbiztonsági felhasználói útmutató szabályozza:

- a dolgozói jogosultságok igénylésének és visszavonásának rendjét (A SZIE informatikai rendszere csak az engedélyezett jogosultságok szerinti hozzáférést biztosítja a munka-, megbízási-, illetve tanulmányi-szerződésben meghatározott időtartamra.),
- az informatikai eszközök és szolgáltatások alkalmazási rendjét, az eszközök és szolgáltatások használata során elvárható felhasználói magatartás módját (pl. telefon, mobiltelefon, telefax, videokonferencia, levelezőrendszer, internet),
- a jelszóhasználattal kapcsolatos előírásokat,
- az "Üres asztal – tiszta képernyő" szabályt,
- az informatikai rendszerekben tárolt adatok biztonságát, védelmét, a mentés és archiválás rendjét,
- a bizalmas és személyes adatok kezelési módját,
- a vírusvédelemmel kapcsolatos felhasználói felelősséget
- az informatikai problémák, incidensek kezelésének rendjét.

A felhasználói problémák és igények jelzésére az Informatikai központ HelpDesk-jét, illetve a kari rendszergazdákat kereshetik. Valamennyi felhasználó kötelessége, hogy a már megtörtént, vagy folyamatban lévő biztonsági incidens észlelésekor azonnal cselekedjen, és értesítse a SZIE informatikai szervezetét. Minden felhasználó köteles az általa észlelt hibás program, illetve informatikai eszköz működését a HelpDesk-nek haladéktalanul bejelenteni.

Az Informatikai felhasználói útmutatóban leírtak megszegése munkajogi, kártérítési és büntetőjogi felelősséggel jár. Az előírások súlyos megsértése esetén kártérítési, büntetőjogi eljárás indulhat a szabálysértő személyével szemben.

A „Felhasználói tájékoztató” megismerését és elfogadását „Felhasználói nyilatkozatban” kell dokumentálni, mely a személyi dossziéban kerül lefűzésre.

5. SZÁMÚ MELLÉKLET hátlap

FELHASZNÁLÓI NYILATKOZAT

(A SZIE Információ Biztonsági Rendszerének alkalmazásához)

Alulírott (munkatárs neve) _____

(születési hely, dátum) _____

(SZIE azonosító, ha van[1]) _____

nyilatkozom, hogy a „Felhasználói tájékoztatót” a mai napon átvettem, az abban foglaltakat megismertem és magamra nézve kötelező érvényűnek tekintem.

Dátum:

_____

aláírás

A nyilatkozata a személyi dossziéban kerül lefűzésre.

A nyilatkozatot átvette: (olvasható név valamint aláírás)

Átvétel időpontja:

[1] *Webmailes bejelentkezési azonosító (Három betű, négy szám)*