BUDAPESTI CORVINUS EGYETEM

INFORMATIKAI SZOLGÁLTATÓ KÖZPONT

INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

2.1 Verzió
Utolsó aktualizálás: 2019. 11. 26.

Mogyorósi János
Igazgató
Informatikai Szolgáltató Központ
Budapesti Corvinus Egyetem

Tartalomjegyzék

Tartalom

A rész – Biztonsági irányelvek

I. Alapfogalmak, definíciók

Fogalom	Magyarázat
BCE	Budapesti Corvinus Egyetem
ISZK	Informatikai Szolgáltató Központ, a BCE önálló központi szervezeti egysége, amely felelős a BCE központi informatikai szolgáltatásaiért. Képviseletére és irányítására az ISZK igazgatója jogosult.
IBSZ	Az Informatikai Biztonsági Szabályzat (IBSZ) azokat a betartandó szabályokat tartalmazza, amelyek alapján az Egyetem informatikai infrastruktúrája biztonságosan üzemeltethető. Az IBSZ-ben foglaltak a felhasználók és üzemeltetők számára kötelező érvényűek, beleértve a szervezetileg az egyetemhez nem tartozó, de szolgáltatásait közvetlenül vagy közvetve igénybe vevő személyeket, beleértve a számítógépes programokon keresztül való igénybevételt is. Jelen IBSZ az ISZK biztonsági politikáját, főbb irányelveit (A rész), a konkrét szabályokat (B rész) illetve a mellékleteket és hivatkozásokat (C rész) együtt tartalmazza.

CORNET	A BCE informatikai hálózata, üzemeltetését az ISZK végzi. Részét képezik a következő típusú eszközök: • Passzív adatátviteli vonalak (Ethernet, FDDI, ATM, GigabitEthernet szegmensek, optikai és hagyományos összeköttetések, amelyek egyetemi tulajdonúak, csatlakozók stb.) • Hálózati aktív elemek (repeaterek, bridge-ek, switchek, routerek, modemek, terminál-szerverek, access pointok stb.), továbbá minden hálózatra kötött számítógépes munkahely (PC, munkaállomás, hálózati nyomtató, IOT eszközök stb.) és szerver függetlenül attól, hogy az mely egyetemi egység tulajdonában vagy használatában van. • CORNET-EAP az egyetem vezeték nélküli hálózata, melyet azonosítást követően lehet használatba venni.
EDUROAM	Nemzetközi felsőoktatási hálózat, az Eduroamhoz csatlakozott felsőoktatási intézmények hallgatói és munkatársai azonosítást követően vehetik igénybe és melynek a BCE is tagja
ÜZEMELTETŐ	Az eszköz üzemeltetője alapvetően az ISZK munkatársa, illetve néhány egyetemi egység kijelölt saját munkatársa (pl. Központi Könyvtár, kollégiumok stb.). A részlegesen önállóan üzemeltető egységek aktuális nyilvántartását az ISZK vezeti.
FELHASZNÁLÓ	Felhasználó az a személy, aki az ISZK valamely szolgáltatását igénybe veszi. Belső felhasználó az egyetemmel munkaviszonyban-, vagy hallgatói jogviszonyban álló személy (a továbbiakban felhasználó). Külső felhasználó az egyetemmel ilyen jogviszonyban nem álló személy. Külső felhasználók az egyetem publikus informatikai szolgáltatásait vehetik igénybe, egyéb szolgáltatások igénybevételére csak határozott időre szóló engedéllyel jogosultak. Ez utóbbi esetben rájuk is a belső felhasználókra vonatkozó szabályok érvényesek.
HÁLÓZATI ÉS LOKÁLIS SZOLGÁLTATÁS	Megkülönböztetünk hálózati szolgáltatásokat (számítógépes munkahelyről igénybe vehető szerverszolgáltatások, amelyek hálózati forgalommal járnak, pl. levelezés, web, ftp, wifi) és lokális szolgáltatásokat (amelyek a lokális végponton vehetők igénybe, pl. MS Office, operációs rendszer).
BIZTONSÁGI POLITIKA	Az ISZK naprakész biztonsági politikával rendelkezik, amelyet az Informatikai Biztonsági Szabályzat (IBSZ) tartalmaz. A biztonsági politikának nem az a célja, hogy konkrét és részletes cselekvési terveket és eljárásokat rögzítsen, ellenben tisztáznia kell azokat az elveket, általános elvárásokat és etikai normákat, amelyek – a hatályban lévő jogszabályokkal és a CORNET számára egyébként irányadó szabályokkal, elvekkel összhangban – a hálózat felhasználásának kereteit megalapozzák. Az aktuális problémákat, felvetéseket ez alapján lehet és kell kezelni. A Biztonsági Politika – az IBSZ részeként – kötelező érvényű az egyetemi közösségre nézve.

HBONE	A hazai akadémiai közösség számítógéphálózata. Az ISZK üzemelteti a CORNET oktatási és kutatási célú kijáratát a HBONE-ra a KIFÜ megbízásából. Az ISZK feladata, hogy érvényesítse azokat a szabályokat, amelyek a HBONE-ra és az arra kapcsolódó intézményekre vonatkoznak. Az Hungarnet a saját, (HBONE POP) interface-től kezdve üzemeltet, a CORNET szolgáltatási köre a HBONE interfacéig tart. A HBONE kapcsolatot az adott szolgáltató megbízottja üzemelteti. A BCE a HBONE tagjaként regionális központ, így hálózati szolgáltatásokat biztosít a BCE-n keresztül kapcsolódó HBONE intézményeknek, ezek azonban nem a CORNET részei. A gerinchálózatot csak az ISZK, vagy általa megbízott szervezet konfigurálhatja, üzemeltetheti.
MEGBÍZHATÓ SZÁMÍTÓGÉP	Minden olyan eszköz mely az egyetem tartományában (BKAE.hu) van, üzemeltetését, karbantartását az ISZK munkatársai végzik. A számítógép biztonságát automatizmusok garantálják. Ezekhez a gépekhez a felhasználó csak kivételes esetben, az ISZK engedélyével kaphat adminisztrátori jogosultságot. Az engedélyt az ISZK saját hatáskörben bírálja el.
NEM MEGBÍZHATÓ ESZKÖZÖK	Minden olyan eszköz mely nem tagja az egyetem tartománynak; az ilyen eszköz karbantartását, adminisztrációját a felhasználó végzi.
RENDSZERGAZDA	Az ISZK munkatársa, aki az egyetemi informatikai rendszerek üzemeltetéséért felelős.
Cusman	Centralised User Management rendszer, a BCE központi felhasználó adminisztrációs rendszere.
TARTALMI RENDSZERGAZDA	Egy egyetemi alkalmazás felügyeletéért felelős személy (pl.: Neptun, Gólya, Poszeidon, közös tárak). Felhasználói adatbázist tart karban, jogosultságokat oszt, az ezt kiszolgáló szerver üzemeltetéséért általában nem felelős. A tartalmi rendszergazda személyéről az adott szervezeti egység vezetője dönt. A tartalmi rendszergazdák elérhetőségét az ISZK tartja nyilván.
BIZTONSÁGI FELELŐS	Az informatikai biztonság hatékony megvalósításához a legfontosabb a felelőségi körök meghatározása, elhatárolása. Az átfogó, teljes szervezetet lefedő biztonsági folyamatok működtetésére összehangolására, ellenőrzésére az ISZK létrehozta, a szervezeti fából kiemelt Security Officer /Biztonsági felelős pozíciót.

VPN	Virtuális magánhálózat: a nem megbízható gépek – tipikusan otthoni gépek és az alkalmazottak egyetem területén használt laptopjaik - azonosítás után, VPN csatlakozás segítségével tudnak hozzáférni a szolgáltatások egy részéhez. Az egyetemi szolgáltatások biztonsági besorolásuknak megfelelően különböző VPN szerverekhez tartozhatnak.

II. Általános irányelvek

2.1 Az IBSZ célja

(1) Az általános cél, hogy az egyetem informatikai infrastruktúrája hosszú távon is működőképes legyen, és lehetőség szerint minél szélesebb körben kihasználásra kerüljön, figyelembe véve az egyetem oktatási, gazdasági és egyéb működési igényeit. Olyan szabályozást kell megvalósítania, amely végrehajtásával az egyetem informatikai rendszerei, a felhasználói adatok, az egyetem és az egyetemi polgárok jó híre is megvédhető. A biztonsági szabályzatnak ezek mellett összhangban kell lennie a hatályos magyar jogszabályokkal, és az egyetem internetszolgáltatójának szabályaival.

2.2 Érvényességi kör

(1) A biztonsági szabályzat érvényes az egyetem informatikai infrastruktúrájára, az azokat felhasználó személyekre és a vele kapcsolatot létesítő számítógépekre. A szabályzat érvényességének széles köre miatt fontos, hogy azt az érintettek ismerjék, a benne foglalt elveket elfogadják, és azokkal azonosuljanak. Különös jelentőséggel bír, hogy az infrastruktúra használói mellett az üzemeltetésben érintettek, az ISZK munkatársai, illetve az informatikát nagyobb mértékben használó egyetemi felhasználók – azaz akik a biztonsági szabályzatot elsősorban alkalmazzák – megismerjék azt.

(2) Az ISZK a jelen szabályzatban előírt egyetemi nyilvántartásokat vezeti, az egyéb üzemeltetők felett a szakmai felügyeletet gyakorolja. Az informatikai rendszerek rendellenes működése, meghibásodása, egyes részeinek használhatatlansága esetén az ISZK más egységek üzemeltető személyzetét utasíthatja - a hiba elhárításához szükséges mértékben - az eszközeiken szükséges teendők végrehajtására.

2.3 Nyílt rendszer

(1) Az ISZK nyitott bármely olyan technikai megoldás befogadására, amely a meglévő szolgáltatásokat nem veszélyezteti, üzembiztonsága az elvárható szintet nyújtja. Az újonnan felmerülő igényekkel kapcsolatban az ISZK illetékesével konzultálni kell; az adott rendszer üzemeltetője a szükséges technikai segítséget megadhatja, de ha nem látja biztosítottnak a rendszer működésének zavartalanságát, akkor az igényt el is utasíthatja.

III. Az IBSZ hatálya

(1) Jelen IBSZ hatálya kiterjed mind a külső, mind a belső felhasználókra, valamint az üzemeltetőkre. A felhasználók és üzemeltetők jogai és kötelességei eltérhetnek, felhasználói csoportokra sajátos szabályok vonatkozhatnak, azonban mindezeket az IBSZ-en belül, vagy az általa hivatkozott kiegészítő dokumentumokban szükséges rögzíteni.

(2) Az IBSZ visszavonásig vagy újabb változat megjelenéséig hatályos. Az ezzel megbízott személy (vagy személyek) évente egyszer kötelesek az IBSZ áttekintésére, aktualizálására, függetlenül attól, hogy az adott időszakban történt-e változás vagy sem. Az IBSZ változásainak, aktuális változatának kihirdetése az ISZK feladata.

(3) Az IBSZ összhangban áll a hatályos törvényekkel és magasabb szintű szabályokkal, azok hatályossági körét nem érinti. Az IBSZ-ben nem szabályozott kérdésekben a hatályos jogszabályok irányadók.

(4) Az ISZK működésének javítása, megbízhatóságának növelése érdekében további ajánlásokat tehet, ill. saját hatáskörében olyan szabályokat írhat elő, amely a felhasználókat nem korlátozza a szolgáltatások igénybevételében, csupán annak formáit határozza meg (pl. kötelező cache, kötelező kliens használat, névkonvenciók betartása, egyes szolgáltatások kötelezően előírt dedikált szerveren keresztüli igénybevétele, tűzfalelőírások).

(5) A biztonsági szabályzat megsértése esetén a szabályzat nem ismerete nem mentesít semmilyen következmény alól!

IV. Az IBSZ biztonsági fokozatai

(1) Az ISZK kezelésében lévő adatokról adatvédelmi szempontból az Adatvédelmi szabályzat rendelkezik. (lásd. IBSZ C melléklet)

(2) Az ISZK által üzemeltetett rendszerek, az ott kezelt adatok, információk nem egyforma minősítésűek fontosság és a biztonsági igények tekintetében. Az alábbiakban felsoroljuk a szabályzat által meghatározott és hivatkozott biztonsági szinteket és jellemzőiket.

4.1 Alapvető biztonsági igény (S1)

(1) Az alapvető biztonsági igényűnek tekintett adatok és rendszerek jellemzői, hogy az adatok felőli kezdeményezője, illetve fogadója, vagy a rendszerek felhasználója csak azonosított vagy utólag beazonosítható az adott hálózathoz hozzáférési jogosultsággal rendelkező személy lehet. Az ide sorolt adatok és rendszerek biztonsága érdekében az ISZK egyetemi szintű, központi megoldásokat alkalmaz: egyetemi spamszűrő, központi tűzfal, VLAN szintű hozzáférés-vezérlés, az egyetem és a külvilág közötti teljes forgalom naplózása stb. A forgalom titkosítását az ISZK nem garantálja.

4.2 Fokozott biztonsági igény (S2)

(1) A fokozott biztonsági igényűnek tekintett adatok és rendszerek számára az S1 szinten jellemző megoldásokon túl további szabályok és biztonsági garanciák vonatkoznak. A fokozott biztonsági igényű adatok és rendszerek az egyetemi közösség számára valamilyen bejelentett szolgáltatást nyújtó rendszerelemek. Az S2 biztonsági igény jelzése a rendszerelem üzemeltetőjének felelőssége. A fokozott biztonság elérése érdekében a rendszer integritását szigorúbb hozzáférési szabályokkal kell biztosítani (pl. a felhasználói kör leszűkítése), a védelmet pedig a rendszerre személyre szabottan kell megvalósítani (pl. egy adott adatfolyam titkosításával). A fokozott védelem gyakorlati megvalósításának felelőssége az ISZK-é. Ennek azonban csak olyan mértékben tud megfelelni, amilyen pontosságú információ és igény a rendszer üzemeltetője részéről rendelkezésére áll, így az információszolgáltatás az üzemeltető kötelessége.

4.3 Kiemelt biztonsági igény (S3)

(1) A kiemelt biztonsági igényű adatok és rendszerek legfőbb ismérve, hogy az egyetemi közösség számára olyan szolgáltatást nyújtanak, amelyeknek az akár időleges kiesése is kritikusnak tekinthető. A kiemelt biztonsági igényű szintbe való besorolás a rendszer üzemeltetőjének, az ISZK-nak, és az igénybe vevők képviselőjének együttes döntése alapján történik. A kiemelt biztonsági igényű rendszerek esetében akár adatmentéssel, akár redundancia biztosításával meg kell valósítani a 99,99%-os rendelkezésre állást, és emellett az alsóbb biztonsági szintek szolgáltatásait is meg kell valósítani.

4.4 Nem kívánt adatok és rendszerek (S0)

(1) Nem kívánt adatoknak és rendszereknek tekintendők azok a rendszerelemek, amelyeket nem lehet besorolni a fenti három kategória egyikébe sem. Úgyszintén ide tartoznak azok a rendszerelemek, amelyekről bebizonyosodik, hogy nem egyetemi célokat szolgálnak, vagy egyéb módon sértik a felhasználói szabályzatot. Az ilyenek adatok és rendszerek biztonsági fenyegetést jelentenek. A biztonságos üzemeltetése érdekében az ISZK felelőssége, hogy az ilyen elemeket (tipikusan illetéktelenül csatlakoztatott eszközöket, vírusok által generált forgalmakat, jogosulatlan felhasználókat) a rendszerből kizárja, illetve a fenti három (S1-S2-S3) kategória valamelyikébe illessze, a kategóriához kapcsolódó kritériumok betartatásával.

4.5 Adatvédelmi szempontok

(1) Adatvédelmi szempontokból is meg kell különböztetni általános és kritikus szinteket. Adatvédelmi szempontból kritikusnak tekintett rendszerek esetében az adatok megbízhatósága, integritása és illetéktelenek számára való hozzáférhetetlensége érdekében a rendszernek további biztonsági garanciákat kell tartalmaznia. Ilyen kritikus rendszernek tekinthetők az alábbiak:

a) Bér- és Munkaügyi rendszer
b) Gazdasági, ügyviteli rendszer
c) Dokumentumkezelési rendszer
d) Tanulmányi és elearning rendszer

e) Központi levelezés
f) Központi tárhely-kiszolgálás
g) Központi felhasználó-kezelői rendszer
h) Iktatási rendszer

4.6 Intézményi authentikációs rendszer

(1) Az egyetem egységes keretben kezeli a felhasználói azonosítást. Ez a rendszer a saját fejlesztésű CUSMAN rendszer. A rendszer az egyetem nagyszámú felhasználójának központi kezelésére szolgál, az adminisztratív funkciók delegálásának lehetőségével. Jelenleg a következő rendszerek kezelhetőek vele:

a) Központi levelezés
b) Központi bejelentkezés az egyetemi tartományba
c) Központi háttértár
d) Egyetemi VPN bejelentkezés
e) Saját weboldal
f) Bejelentkezés a központi UNIX szerverre
g) Tartalomtár
h) Gazdasági rendszer
i) Office 365
j) Egyetemi portál

(2) Az IBSZ szempontjából ennek jelentősége abban áll, hogy a felhasználói azonosítás követelményeinek minden rendszernek meg kell felelnie, és ez csak egységes keretben biztosítható. Ebből következően minden bevezetésre kerülő rendszernek illeszkednie kell a központi felhasználó kezelő rendszerhez.

B rész – Biztonsági szabályozás

V. Az IBSZ által szabályozott gépek körei

(1) Az egyetemi hálózatba tartozó és azon kívüli eszközök eltérő biztonsági igényeik mellett különböző biztonsági fenyegetettséggel rendelkeznek. A potenciális biztonsági fenyegetés szerinti csoportosítást eszközök szerint érdemes elvégezni. Az alábbi kategóriákra hivatkozunk ebben a Biztonsági Szabályzatban.

5.1 Központi szerverek

(1) Meghatározott feladatra, ismert, jól védhető protokollokkal rendelkező gép. Sok potenciális felhasználója van, de jellemzően nincs tetszőleges futtatási lehetősége a felhasználóknak. Logikailag a számítógép-hálózat központi eszközei (switchek, router, tűzfal) is ide tartoznak. A központi szerverek tipikusan fokozott vagy kiemelt biztonsági igényű eszközök (S2-S3), amelyek ezért megfelelő védelemmel rendelkeznek, és a felhasználók részére is csak meghatározott szolgáltatást nyújtanak. Ezért innen érkező támadásokra

kevésbé kell számítani. Feladat viszont a védett állapot fenntartása, és az ismerté váló biztonsági résekre való reagálás, mivel ezen eszközök kiesése potenciálisan sok felhasználót érint.

5.2 Alkalmazásszerverek

(1) Alkalmazásszerverek azok a kiszolgálók, amelyek nem egy-egy jól ismert, jól védhető protokollt használnak, nem az informatikai standard alkalmazásokat (mint pl. web, levelezés stb.) szolgálják ki, hanem valamilyen egyedi alkalmazás fut rajtuk. Ezáltal biztonsági szempontból speciális védelmet igényelnek. Az üzemeltetővel, aki ilyen esetben néha külső személy, sokkal szélesebb körű kommunikáció szükséges, a sajátos igények miatt.

5.3 ISZK dolgozók gépei

(1) Használói jellemzően rendszergazdák az adott gépeken, illetve az egyetem rendszereihez könnyebben hozzáférnek. Ezért különösen fontos a felelősségi viszonyok, illetve az egyes rendszerekhez való hozzáférési szabályok ismerete és betartása. A visszaélések elkerülése érdekében az ISZK alkalmazottainak a CORNET szabályzatát, jelen Biztonsági Szabályzat ajánlásait, a munkahelyi szabályokat és etikai normákat el kell fogadniuk és azokkal azonosulniuk kell. Az ilyen számítógépeken található anyagok jobban védendők.

5.4 Megbízható gépek

(1) Ezeket a gépeket az ISZK tartja karban. Az ISZK általi karbantartás magával vonja, hogy a gép felhasználója, illetve felelőse nem rendszergazda az adott eszközön, így a gép által jelentett fenyegetés a központi irányelvek alapján jól megítélhető. Kívánatos, hogy az egyetem területén használt számítógépek túlnyomó többsége ebbe a kategóriába essen.

(2) A megbízható gépek otthoni használata esetén a megfelelő azonosítás és VPN kapcsolat után válik lehetővé az egyetemi szolgáltatások egy részének elérése.

5.5 Nem megbízható gép

(1) Az egyetemi alkalmazottak és hallgatók saját eszközeikről távolról is elérhetik az egyetemi szolgáltatások egy részét VPN segítségével. Az említett gépek karbantartása kizárólag a tulajdonosok feladata, így az ilyen gépeket alapvetően biztonsági fenyegetésnek kell tekinteni külön csoportként kell kezelni, a hálózat védelmét tőlük biztosítani kell (pl. a VPN segítségével csatlakozott gépekre szigorúbb hozzáférés-vezérlő szűrőlisták alkalmazásával).

(2) Az egyetem alkalmazottainak lehetősége van a saját tulajdonában lévő laptopját vezetékesen is a hálózatra csatlakoztatni.

5.6 Laborgépek

(1) ISZK által karbantartott, de sok felhasználó által használt gépek. Megvalósul ugyan a felhasználói azonosítás, de az emberi tényező miatt nem zárható ki, hogy az azonosítást nem az összes, vagy nem a legfőbb felelős végzi el (tipikusan ilyen helyzet valaki más azonosítójával való visszaélés). A nagyszámú felhasználói kör, illetve a laborok magas kihasználtsága miatt itt kell a leginkább egyéb fenyegetésekre (szándékos vagy véletlen rongálások, lopások stb.) felkészülni. A számítógépek kiemelt gyakoriságú és alaposságú karbantartása fontos biztonsági szempont.

5.7 Rendezvények

(1) Az ide sorolt eszközök specialitását az adja, hogy használójuk külső felhasználók, akik az ISZK publikus szolgáltatásai mellett határozott időre szóló engedélyt kapnak nem publikus szolgáltatások (pl.: internethozzáférés, számítógép használat) igénybevételére. A rendezvényes gépek minden esetben azonosított felelőst, ám sok esetben azonosítatlan, nagyszámú felhasználót jelentenek. Bár a gépek maguk fizikailag hozzáférhetők, az ISZK ezeken a gépeken karbantartást csak nagyon korlátozottan tud végezni. A rendezvényes gépeket a fenti okokból komoly biztonsági kockázatnak kell tekinteni, mindig külön csoportként kell őket kezelni, és központi eszközökkel kell gondoskodni arról, hogy csakis az engedélyezett erőforrásokhoz férjenek hozzá. A Campus a rendezvényekkel kapcsolatban önálló szabályzattal rendelkezik. (lásd. IBSZ C melléklet)

5.8 Kollégiumok

(1) A kollégiumok hálózatát az ISZK üzemelteti, illetve hálózatüzemeltetésének felügyeletét, koordinálását végzi. A kollégiumokat ebből a szempontból részben külső, részben belső rendszernek kell tekinteni.
Külső rendszernek tekintendők az egyetemi hálózat szempontjából, így ugyanazokhoz a publikus szolgáltatásokhoz férhetnek hozzá, mint a külvilág bármely része. Belső rendszernek tekintendők a külvilág szempontjából, hiszen a kollégiumokból induló forgalom a külvilág szempontjából az egyetem felől érkezik.

Mindezekből következően:

a) A kollégiumok számára semmilyen olyan szolgáltatás elérése nem engedélyezett, amit a külvilág sem ér el. Ez alól egyedi esetekben adhat az ISZK kivételt, ha az adott kérelmező ellenőrizhetően biztosítani tudja, hogy megfelel a szükséges biztonsági követelményeknek.

b) A kollégiumok a megbízott rendszergazdáikon keresztül tartják a kapcsolatot az ISZK-val, amely esetükben szakmai felügyeletet lát el. Az ISZK saját hatáskörében kezdeményezhet bármely szankciót a kollégiumok ill. kollégiumi gépek hozzáférési jogosultságainak megvonásával, illetve fegyelmi eljárás kezdeményezésével, amennyiben ezt szükségesnek látja.

5.9 Külvilág

(1) Külvilágnak tekintünk minden olyan eszközt, amelyik nem része az egyetemi hálózatnak. Az egyetemi hálózat a külvilággal jól meghatározott pontokon érintkezik (az egyetemi hálózat internetösszeköttetése éppúgy ide tartozik, mint a pendrive használat), és csak az így definiált pontokon keresztüli adatcserét tekinthetjük megengedettnek. Minden más ponton megvalósuló adatcserét, vagy más kapcsolódási pontot (ilyen pl. egy be nem jelentett Access Point csatlakoztatása a hálózatra) súlyos biztonsági kockázatnak kell tekinteni. Az ISZK jogosult a rendelkezésére álló eszközökkel az ilyen típusú kockázatok megszűntetésére.

VI. Felelősségi körök, szabálysértések

6.1 Felhasználói kör

(1) Az egyetem felhasználóit - jogosultságok, igények és felelősség alapján - az alábbi csoportokba soroljuk:

a) Egyetemi dolgozók, tanszékcsoportok, intézmények
b) Hallgatók (kollégiumok, HÖK, egyéb diákszervezetek)
c) Központi kiszolgáló szerverek
d) Adminisztrációs kiszolgálók
e) Infrastruktúra (adathálózat, telefon)
f) ISZK dolgozói
g) Gazdasági Igazgatóság
h) Regionális központ voltunk miatt kapcsolódó intézmények

(2) A csoportok egymás közötti, illetve az ISZK által üzemeltetett szerverekkel és a külvilággal való engedélyezett forgalmát meg kell határozni. Minden más nem engedélyezett forgalmat tiltani kell. A forgalom engedélyezéséről a hálózati rendszergazda dönt. Ezt az adott felhasználók, vagy az őket képviselő személyek akkor kérhetik módosítani, ha az nem okoz sem fokozott biztonsági kockázatot, sem túlzott mértékű adminisztrációs vagy üzemeltetési terhet az ISZK felé. A hálózati rendszergazda döntését, illetve a módosítási kéréseket dokumentálni kell. A dokumentáció meglétéért a hálózati rendszergazda felel.

6.2 A felhasználók számára létező tilalmak

(1) A felhasználók számára érvényes, biztonsági okokból szükséges tilalmak:

a) Olyan szoftverelem telepítése, melyet nem jogosult használni (a telepíteni kívánt új szoftverelemről szakmai véleményt kell kérni az ISZK munkatársaitól)

b) Az ISZK írásbeli engedélye nélkül bármilyen hálózati vagy hardver eszközt telepíteni,
c) Olyan tevékenységet folytatni, melynek célja vagy előrelátható következménye az egyetemi informatikai infrastruktúra szoftver- vagy hardverintegritásának bármilyen sérülése
d) Hálózati eszközök, szerverek telepítése (WiFi Access Point, router stb.)
e) Az esetlegesen előforduló biztonsági réseket, hiányosságokat kihasználni
f) Olyan eszközök használata, melyek az egyetem által telepített rádiófrekvenciákat használó eszközöket (pl.: wifi, hangosítás) zavarja.
g) Nem engedélyezett erőforrásokat illetéktelenül megszerezni, használni
h) A szolgáltatásokat és informatikai eszközöket felhasználni egyetemen kívüli munkavégzésre
i) Tilos más felhasználók tevékenységének zavarása, illetéktelen jogosultságok és adatok megszerzése, jogosultságok (felhasználói azonosító stb.) átadása, a szoftverek és a hardver elemek megrongálása, működőképességük veszélyeztetése, eszközök jogosulatlan megbontása vagy önkényes átkonfigurálása, szegmensek tartós megszakítása vagy átépítése, a szoftver licensz, illetve szerzői jogok megsértése (szerzői joggal védett szoftverek másolása).
j) A felhasználó nem kísérelheti meg a számára, ill. a besorolása szerinti felhasználói csoport számára nem engedélyezett erőforrások, szolgáltatások, jogosultságok, kvóták megszerzését. Minden szolgáltatás csak arra a célra vehető igénybe, amelyre azt létrehozták.

6.3 Az üzemeltetők felelőségei és jogai

(1) Az Üzemeltetési Szabályzat szintén tartalmazza az ISZK dolgozóira, azaz üzemeltetőkre vonatkozó előírásokat, amelyek alapján a következő felelőségek állapíthatók meg:

a) Az ISZK felelősségi körébe tartoznak az alábbi eszközök:
- minden, az ISZK által üzemeltetett hálózati eszköz, felelőse a hálózati csoport
- minden, az ISZK által üzemeltetett szerver, felelősei a rendszergazdái
- minden, az ISZK által üzemeltetett számítógép, felelős a Felhasználótámogatási Osztály munkatársai
- minden, a hálózatra rácsatlakozott számítógép, felelős a tulajdonosa

b) A BCE ISZK munkatársai felelősek az informatikai rendszerek optimális működtetéséért, feladatuk az informatikai rendszereket használó oktatóknak és munkatársaknak segítség nyújtása.
c) Felelősségük csak a szolgáltatási körökben leírt és részletezett működési paraméterű, szabványos informatikai alrendszerekre vonatkozik.
d) Az ISZK munkatársai nem felelnek az Egyetem tulajdonában lévő, de nem az Egyetem épületében működtetett informatikai rendszerekért.
e) Amennyiben a BCE oktató vagy munkatárs nem a szabványos informatikai alrendszereket használja (pl.: más operációs rendszerrel, vagy valamilyen speciális alkalmazással dolgozik, mint az ajánlott), abban az esetben az ISZK munkatársai

segítséget adhatnak, de az ilyen alrendszerek üzemeltetése nem az ISZK feladata és felelőssége.

f) Ha egy ilyen nem szabványos alrendszer olyan jelenségeket produkál, ami a hálózat, vagy más, központi rendszerek működtetését veszélyezteti, az ISZK szakembereinek a felelőssége, hogy ezt a rendszert megtalálják, és a normális működést akár az eszköz rendszerből való kiiktatása árán is visszaállítsák
g) A biztonságos üzemeltetéshez az ISZK meghatározhatja a szolgáltatások körét, visszautasíthatja az igényeket.
h) Az ISZK munkatársainak felelőssége továbbá monitorozni a hálózat forgalmát, naplózni a szolgáltatások használatát,
i) Az egyetem területére érkező, és innen induló elektronikus leveleket vírus irtóval
    a. és SPAM szűrővel ellenőrizni, és figyelmeztetés nélkül eldobni a vírusos és a nyilvánvaló SPAM leveleket
j) Kizárni a hálózati erőforrások eléréséből azokat a felhasználókat, akik nem rendeltetésszerűen használják azokat, kizárni a hálózat működéséből azokat a számítógépeket, amelyek veszélyt jelentenek a hálózat működésére, biztonságára (például vírusos és fertőző gépeket),
k) Kizárni a hálózat működéséből azokat a számítógépeket, amelyek nem jogszerű tevékenységet folytatnak
l) Amennyiben nem állapítható meg a hibás gép csak a hálózati szegmens, akkor az üzemeltetők a hiba pontos helyének meghatározásáig kizárhatnak részhálózatokat is a szolgáltatásból.

VII. A műszaki-technikai, szakmai védelmi intézkedések

(1) Az infrastruktúra különböző karbantartási mértéke, és az adatok különböző fontossága miatt a felhasználókat és az infrastruktúra elkülöníthető részeit eltérő módokon kell kezelni. Ott, ahol műszaki korlátok miatt nem elkülöníthetők egymástól biztonsággal a gépek, a legkisebb megbízhatóságú géppel egyező szinten kell az adott csoportot kezelni.

8.1 A bejövő, illetve kimenő forgalom megkülönböztetése

(1) A belső támadásokon túl a legfontosabb a hálózat határán áthaladó forgalom. A befelé jövő forgalom tartalmazhat vírust, kéretlen reklámlevelet, valamilyen biztonsági rés elleni támadást, amely az informatikai infrastruktúrát károsíthatja, vagy adatvesztést okozhat, bizalmas adatok kiszivárgását teszi lehetővé. Ugyanez a fajta forgalom tőlünk eredeztetve aláásható az egyetem jó hírét, illetve azt okozhatja, hogy internetszolgáltatónk korlátozást léptet érvénybe az internetkapcsolatunkon. Általánosan elmondható, hogy a befelé jövő támadásoknál az egyik potenciális veszélyt a nem megfelelően karbantartott számítógépek jelentik. Ez az által védhető ki, ha csak az a számítógép nyújthat a külvilág számára szolgáltatást, amelyhez egyértelműen rendelhető felelős személy, aki azt karbantartja, rajta a szoftvereket rendszeresen frissíti. Az egyetemről kifelé irányuló incidensek kezelése érdekében pedig a kifelé menő forgalom csak olyan személytől, számítógéptől eredhet, amelynek a forrása egyértelműen azonosítható, a felelős visszakereshető.

8.2 Infrastruktúrához kapcsolódó védelmi intézkedések

(1) Az egyetemi infrastruktúrát jelentő nyilvános hozzáférésű gépekre vonatkozó védelmi előírások
   a. Az informatikai laborokban, open laborokban lévő gépek, illetve a projektoros és tantermi, tanári gépek felhasználási házirendjét az ISZK határozza meg és teszi közzé. A termet használó egyetemi szervezet tovább szigoríthat ezen szabályokon, azonban kivételt nem tehet alóluk.

(2) A szerverterem védelme: a szerverterembe való belépés csak szabályozott és ellenőrzött módon történhet. Jelenleg erre a következő szabályok vonatkoznak:

   a. A szerverterembe a belépés csak ujjlenyomatleolvasással lehetséges. A leolvasó rendszer naplózza a belépést.
   b. Egy biztonsági kamera rendszer tárolja a helyiségbe belépőkről készült felvételt.
   c. A szerverteremben csak az ISZK meghatározott munkatársai tartózkodhatnak. Amennyiben külső munkavégzőnek kell a helyiségben dolgoznia, ez csak az ISZK dolgozója felügyeletével és jelenlétében történhet.
   d. A helyiség klimatizált, a klíma megfelelő működéséről az épület karbantartója köteles gondoskodni.

(3) Az áramszolgáltatással, szereléssel kapcsolatos intézkedések
   a. A szerverterem tápellátása egy nagyteljesítményű, távmenedzselhető szünetmentes tápról (UPS-ről) megoldott. Ezzel kapcsolatos fontos biztonsági irányelv, hogy az erre kijelölt személy köteles rendszeresen meggyőződni az UPS állapotáról, fázisainak egyenletes terheléséről. Új eszközt csak az ő felügyeletével szabad csatlakoztatni, még ideiglenes jelleggel is. Minden S3 rendszert az UPS-re kell csatlakoztatni. S2 esetén ez akkor kötelező, ha van rá lehetőség.

   b. Az ISZK üzemeltetésében lévő minden aktív hálózati eszközének áramtalanítása, illetve minden aktív és passzív elemének szerelése kizárólag az ISZK vagy megbízottjainak joga. Ez alól csak a baleset, katasztrófahelyzet, vagy egyéb vis major adhat kivételt. A szakszerűtlen vagy illetéktelen beavatkozás által okozott kárt az azt szándékosan vagy felelőtlenül okozó, illetve lehetővé tevő személy köteles megtéríteni. Az okozott kár nem csak a hardverelemek sérülését jelenti, hanem a helyreállítás, kiszállás stb. költségeit, beleértve az adatok sérüléséből és a szolgáltatás kimaradásából adódó költségeket, illetve közvetlenül vagy közvetve okozott károkat.

(4) Az aktív hálózati eszközök, rendezők védelme
   a. A kábelrendezők minden lehetséges esetben zárható, csak az ISZK által használt helyiségben, vagy önállóan zárható szekrényben kerülhetnek csak elhelyezésre. A rendezőszekrényekhez az ISZK dolgozóin kívül másnak csak indokolt esetben lehet kulcsa. Ilyen esetben a további kulccsal rendelkező személy felelős a kábelrendező hozzáférhetetlenségének biztosításról. Meg kell vizsgálni az adott eszközök bekötését az adott épületben rendszeresített eszközvédelmi rendszerbe.
   b. Az esetleges illetéktelen hozzáférés esetén az előző pontban leírtaknak megfelelően kell eljárni.

VIII. Jogosultságok

(1) A felhasználói kör jogosultság- és jelszónyilvántartása egységes keretek között, a CUSMAN-on belül oldódik meg. A CUSMAN rendszer üzemeltetése, karbantartása az ISZK felelőssége. A CUSMAN rendszer használatára külön leírás érhető el, illetve lásd korábban.

8.1 Az egyetem informatikai rendszereihez történő hozzáférések

(1) Jogosultság igénylés folyamata

a. Egyetemi alkalmazottak, és szerződéses partnerek
   A HR terület rögzíti az adatokat az SAP HR moduljába. A CUSMAN az SAP rendszerből veszi át és tartja karban a felhasználói adatokat.
   A felhasználói fiók az ISZK Ügyfélszolgálaton történő személyes igénybejelentést követően kerül aktiválásra.
   Az egyetemi közös tárterület szolgáltatáshoz való hozzáférést a tárterület gazdája kezdeményezheti elektronikusan az eÜgyfélszolgálat felületén, melyet az ISZK Ügyfélszolgálata állít be.

b. Hallgatók
   A hallgatói adatokat a CUSMAN a Neptun rendszerből automatikusan veszi át és tartja karban. A CUSMAN ezen adatok alapján ad hozzáférést szolgáltatásokhoz, a tanulmányaik elvégzéséhez. (Belépés az egyetemi tartományos számítógépekre, egyetemi levelezés, saját meghajtó (tárterület), VPN használat lehetősége.)

   A fentiektől eltérő esetekben a jogosultság igénylést az ISZK vezetőjének kell elküldeni e-mailben. Az ISZK vezetője elbírálja az igény jogosságát és intézkedik a további teendőkről.

8.2 Csatlakozás az egyetemi informatikai rendszerhez

(1) Megbízható eszköz segítségével, megfelelő felhasználói jogosultság birtokában a jogosult egyetemi szolgáltatások teljes köréhez hozzá lehet férni, felhasználói azonosítás után.

(2) Nem megbízható eszközökkel felhasználói azonosítás után lehet a hálózatra csatlakozni. Így a publikus szolgáltatások és az internet elérése válik lehetővé, azon egyetemi polgárok számára, akiknek VPN jogosultsága van.

(3) A VPN-ről elérhető szolgáltatások listáját az ISZK saját hatáskörben, az igényeknek és az informatikai biztonsági szempontoknak megfelelően határozza meg.

8.3 A hálózatra csatlakoztatott eszközökkel kapcsolatos irányelvek

(1) A hálózatra csak az ISZK felelős munkatársai csatlakoztathatnak aktív hálózati eszközt. A felhasználók nem jogosultak semmilyen eszköz hálózatra csatlakoztatására, kivéve saját

használatú, az ISZK által regisztrált laptopjukat vagy a publikus WLAN-szolgáltatáshoz való csatlakozást, ám ez sem láthat el semmilyen asztali gép funkciókon túlmutató funkciót: így nem routolhat, nem NAT-olhat, nem lehet szerver szolgáltatás rajta, nem lehet WLAN hozzáférési pont stb.

(2) A hálózatra csatlakoztatott bármilyen eszköz esetében figyelembe kell venni az ISZK kiadott ajánlásait, esetleges tiltásait.

(3) Az ISZK joga és kötelessége, hogy a nem általa csatlakoztatott eszközöket eltávolítsa, kikapcsolja, a további szabályzatsértést megakadályozza.

8.4 Központi tűzfal

(1) A hálózatot a külső csatlakozási pontjánál védő tűzfalat a következő elvek szerint kell konfigurálni:

a. Minden külsőnek minősített forgalom ezen keresztül érkezhet be.
b. Minden ismeretlen forgalom tiltott, csak ismert forgalom jöhet be.

(2) Az ismert forgalmakról az üzemeltető adatbázist tart nyilván, amelynek alapapján minden tűzfalnyitásról visszakereshető, hogy melyik gépre, melyik portra ki kérte. Kérést csak az adott gép üzembentartójától lehet elfogadni, és csak indokolt esetben. Indoklás nélkül, vagy magáncélra port nem nyitható meg.

(3) Indokolt kivételektől eltekintve elkerülendő a nem portonkénti "teljes" tűzfalnyitás egy gépre.

8.5 Vírusellenőrzési mechanizmus

(1) Egyetemünk a vírusok, férgek, trójaiak, rootkitek, kémprogramok és egyéb digitális kártevők ellen modern antivírus és antimalware megoldásokat alkalmaz. A Felhasználótámogatási osztály munkatársai minden végpontra telepítenek vírusvédelmet.

(2) Az antivírus szoftver konzol részével lehetővé válik:

a. a kliensek menedzselése
b. ripotok készítése
c. szükség esetén távoli beavatkozás pl.: egy gép teljes vizsgálata
d. a kliensek frissítése
e. teljes körű képet kapni a kliensek aktuális állapotáról
f. feladatok automatizált végrehajtására, szükség esetén a felelős értesítésére

(3) Amennyiben az adott gép nincs megfelelően karbantartva (pl. vírusokat, spam-et terjeszt), a rendszergazdáknak joga van az adott gépet a hálózatról leválasztani, a gép számára a hálózati szolgáltatást szüneteltetni egészen a hiba elhárításáig. A leválasztás tényéről az üzemeltető a felhasználót egy munkanapon belül köteles értesíteni.

8.6 Hibakövetés

(1) Az ISZK üzemeltetői kötelesek az általuk észlelt biztonsági hibákat az ISZK által üzemeltetett ticketing rendszerbe (OTRS) rögzíteni. Az ide rögzített hibák, javítási lépések

alapján lehetséges a kapcsolódó biztonsági hiányosságok feltárása, az eljárások, szabályzatok pontosítása. A ticketing felügyelése a Biztonsági Felelős kötelessége.

8.7 Szoftverjogtisztaság

(1) A szoftverek jogtisztaságának kérdése kiterjed a beszerzés, az üzemeltetés, a licenszelés kérdéseire és egyszerre kell megfelelnie a jogi, a pénzügyi és technikai követelményeknek. Ennek érdekében több rendszerelem összhangja szükséges.

(2) Az egyetemek, oktatási intézmények számára elérhető úgynevezett Campus licensz keretében számos alapvető jelentőségű szoftver jogtisztasága megoldott.

(3) A felhasználói gépekre feltelepített szoftverek nyilvántartására automatizált és manuális módon is van lehetőség.

(4) Az ISZK a rajta keresztül beszerzett és/vagy általa üzemeltetett szoftverekről nyilvántartást vezet. Ez a nyilvántartás független a gazdasági terület által vezetett leltártól. A leltározási feladatokat is végző Gazdasági Igazgatóság a szoftvereket az SAP rendszer keretein belül. leltározza.

8.8 Szoftverek telepítése, frissítése

(1) Az egyetemi szintű licenszmegfelelőségi, jogtisztasági kérdések elengedhetetlen feltétele, hogy egyes felhasználók, szervezeti egységek ne tudjanak az ISZK tudta és jóváhagyása nélkül szoftvert telepíteni. Ennek érdekében a gépek úgy vannak konfigurálva, hogy az egyes gépekre csak az ISZK munkatársai rendelkeznek rendszergazdai jogokat biztosító hozzáféréssel, így csak ők tudnak szoftvert telepíteni (illetve eltávolítani).

(2) A munkaállomások Microsoftos szoftvereinek (Windows, Office) frissítése, a javítások a teljes tartományra kiterjedően automatikusan történnek

8.9 Dokumentáltság, naplók, jelentések, jegyzőkönyvek

(1) A biztonság elengedhetetlen feltétele, hogy a biztonsági kérdésekkel kapcsolatos dokumentumok naprakészen és elérhetően megtalálhatóak legyenek.

(2) A biztonsággal összefüggő összes nyilvános dokumentum elérhető az egyetemi weben. A hálózati eszközök és szerverek naplóznak, a naplók biztonsági okokból a nyilvánosság számára nem elérhetőek. Az ISZK dolgozói a saját felelősségi körükben elérik és feldolgozzák a naplókimeneteket.

(3) A mindennapi történések dokumentálása mellett kiemelten fontos a biztonsági kockázatot, kritikus üzemeltetési nehézséget okozó rendszerek monitorozása, azokon előzetes kritikus helyzeteket szimuláló méréseket végezni.

(4) Az egyes erőforrásokhoz való hozzáférést naplózni kell, ahol lehetséges, alkalmazásszinten. Az egyes szolgáltatásokhoz meg kell határozni a naplófájlok megőrzésének idejét, a mentésének, vagy archiválásának rendjét. Hogy a bejegyzések ideje szinkronban legyen, ahol lehetséges, az NTP protokollt kell használni. Minden naplózásra képes hálózati eszközt be kell állítani úgy, hogy egy adott szerverre tegye azt.

(5) Az ISZK a hálózaton belüli vagy a hálózat és a külvilág közötti kommunikáció esetén jogosult és köteles az adott forgalmat a potenciális fenyegetéseknek megfelelően arányosan, és az Adatkezelési Szabályzatot mindenkor szem előtt tartva figyelni vagy ellenőrizni. Ez különösen az internetes forgalmánál a forgalom naplózását és archiválását (illetve utólagos célvezérelt és szabályos ellenőrzését) jelenti. A Biztonsági Szabályzat alapvető irányelve, hogy a hálózatot meg kell védeni minden, a külvilágból érkező támadástól, és úgyszintén védeni kell az egyetemi felhasználók jó hírnevét.

8.10 Reagálás a belső hálózatról induló incidensre

(1) A felhasználók jelentős száma miatt szükségszerűen nemcsak a BCE informatikai infrastruktúráját érheti a külvilág felől támadás, hanem belülről is eredhet ilyen jellegű forgalom. Ezek az incidensek egymástól eltérő fontosságúak, lehetnek egyszerű vírustovábbfertőzések, egy kísérletező kedvű felhasználó próbálkozásai, vagy akár valódi betörési kísérletek. Ezekben az esetekben a legfontosabb dolog az incidens forrásának kiderítése, ami után következhet csak az elhárító intézkedés. Mivel sok esetben az elhárító intézkedés megtétele után már nem lehetséges a forrás kiderítése, ettől a sorrendtől eltérni csak indokolt esetben lehetséges. Az egyetem jó hírének megőrzése érdekében az incidens megszűnte után a külső bejelentő számára az esettel kapcsolatban beszámolót kell küldeni arról, hogy:
    a. Kik voltak az elkövetők és milyen incidens történt?
    b. Milyen ellenlépéseket tettünk a megszüntetéshez?
    c. Milyen lépéseket tervezünk megtenni, hogy ne ismétlődjék az eset?

(2) Amennyiben egy incidens valamely szervezet rendszeréből indult ki, a gyors reagálást elősegíti az adott szervezet informatikusával való szorosabb együttműködés. Annak érdekében, hogy adott esetben ne egy egész részhálózattal szemben kelljen eljárni, szükséges, hogy a szervezetekben lévő számítógépek és felhasználók megkülönböztethetően látszódjanak az ISZK felé is.

8.11 Eszközök kivitele telephelyről

(1) Az eszközöknek az épületekből ki- illetve beszállítását szállítólevéllel kell kísérni, amin többek között az eszközök egyedi azonosítóit is fel kell tüntetni.

8.12 Jelszavakkal kapcsolatos irányelvek

(1) A hálózat üzemeltetője a felhasználók biztonságának érdekében a jelszavakkal kapcsolatban az alábbi irányelveket hirdeti meg és teszi kötelezővé:
    a. Tilos a LOGIN nevet jelszóként használni!
    b. Tilos a vezetéknevet és a keresztnevet jelszóként használni!
    c. Tilos azonos számokból, vagy betűkből álló jelszót használni!
    d. Tilos a jelszót nyilvános helyen kiírva tartani (monitorra ragasztva)!
    e. Elvárható, hogy a felhasználó ne könnyen kitalálható jelszavakat válasszon.
    f. Ajánlott a számok és betűk keverése jelszavak használatakor.
    g. Ajánlott a kis és nagybetűk keverése jelszavak használatakor.
    h. Ajánlott legalább nyolc karakterből álló jelszót választani.

i. Fontos, hogy a felhasználó egyedi jelszót hozzon létre más, általa használt rendszerek jelszavaitól eltérjen.
j. Az egyetemi felhasználói jelszavakat az ISZK által meghatározott időközönként cserélni szükséges.

(2) Amennyiben a felhasználók eltérnek ezektől az irányelvektől, akkor az ebből adódó károkért – akár őket éri kár, akár az egyetemi hálózat valamelyik elemét, akár a külvilágot – felelősséggel tartoznak.

IX. Szabálysértések

9.1 A meg nem engedett tevékenységek szankciói

(1) Az IBSZ megsértése a felhasználó felelősségi körétől, illetve a szabálysértés természetétől, szándékosságától függően különböző súlyú szankciókat von maga után. Jelen Biztonsági Szabályzat az alábbi szankciók alkalmazásáról rendelkezik:

a. Amennyiben a felhasználó a hozzáférési jogosultságát másoknak átadja, vagy azt másokkal megosztja, az ISZK üzemeltetője határozatlan ideig azt felfüggesztheti. Ha a hozzáférési jogosultság illetéktelen felhasználásra kerül, és az illetéktelenül használó súlyos vétséget követ el, akkor annak felelőssége a jogosultság átadóját is terheli, amennyiben az átadás szándékos volt.

b. Amennyiben a felhasználó (akár sikeres, akár sikertelen) kísérletet tesz arra, hogy a számára (besorolása számára) nem engedélyezett erőforrásokhoz hozzáférjen, akkor cselekménye vétségnek minősül, ami a hálózatából való végleges kizárást vonhatja maga után.

c. Amennyiben a felhasználó szándékos, vagy az elvárható gondosságot be nem tartó tevékenysége anyagi kárt okoz, akkor az ily módon előidézett károkért anyagi felelősséggel is tartozik.

d. Amennyiben a felhasználó tevékenysége zavarja, veszélyezteti vagy bármilyen módon akadályozza a hálózat normális és biztonságos működését, akkor az ISZK üzemeltetője a felhasználó hozzáférési jogosultságát határozatlan időre felfüggesztheti. Ha a felhasználó ilyen tevékenysége szándékosan volt ilyen, akkor a tevékenysége vétségnek minősül, ami a hálózatából való végleges kizárást vonhatja maga után.

e. Meg nem engedett tevékenység esetén, vagyis, ha a hálózatot annak céljával össze nem egyeztethető módon használják (pl. nem oktatási célú használat, szerzői jogok sérelmével járó fájlcsere, játékok futtatása stb.), akkor a szankció figyelmeztetés és a tevékenység felfüggesztésére való felszólítás, súlyosabb esetben a felhasználó hozzáférési jogosultságának határozatlan idejű felfüggesztése, fegyelmi vétség esetén pedig akár a felhasználó hálózatából való végleges kizárása.
f. Az ISZK illetékese köteles a felhasználót értesíteni, ha vele szemben bármilyen szankciót foganatosít, de ez nem hátráltathatja a szankció foganatosítását.

g. Amennyiben a felhasználó tevékenysége bármilyen más egyetemi szabályzatot sért, akkor vele szemben az adott szabály szerinti fegyelmi eljárás is lefolytatandó. Ilyen esetben az ISZK munkatársának kötelessége az illetékes egyetemi szerv tudomására hozni az esetet, és erről a tényről köteles értesíteni a felhasználót.

h. Amennyiben a felhasználó tevékenysége bármilyen hatályos jogszabályt sért, akkor az ISZK munkatársának üzemeltetőjének kötelessége az illetékes hatóság tudomására hozni az esetet, és erről a tényről köteles értesíteni a felhasználót.

9.2 Katasztrófakezelés, mentés, visszaállítás, szolgáltatásfolytonosság

(1) Az IBSZ megsértéséből vagy külső okból (meghibásodás, elem kár stb.) adódó meghibásodások adatvesztések utáni helyreállításról rendszereként külön akciótervek léteznek, melyek karbantartása az adott rendszer felelősének feladata. Az akciótervek a jellegükből adódóan nem nyilvánosak, bizalmasan kezelendők.

C rész - Mellékletek

(1) Jelen Informatikai Biztonsági Szabályzat az alább felsorolásra kerülő dokumentumokra hivatkozik, akár mögöttes szabályként, akár egy részterület már létező szabályzataként, akár egyéb iránymutatásként. A felsorolt dokumentumok nyilvánosságáról nem az IBSZ

nyilvánosságára hozójának kell gondoskodnia. A dokumentumok az IBSZ részeiként az (A) és (B) részekben kifejtettek pontos megértését és alkalmazását teszik lehetővé.

a. **Kormányzati Informatikai Fejlesztési Ügynökség**
   A szabályzat elérhető az alábbi URL-en: http://www.KIFÜ.hu/KIFÜ_intezet/aup

b. **Az Informatikai Szolgáltató Központ szervezete**
   A szervezet leírása elérhető az alábbi URL-en: http://www.uni-corvinus.hu/iszk-szervezet
   A szervezeti ábra elérhető az alábbi URL-en: : http://www.uni-corvinus.hu/iszk-sz-ábra

c. **A Budapesti Corvinus Egyetem adatvédelmi szabályzata**
   A szabályzat elérhető az alábbi URL-en: : http://www.uni-corvinus.hu/iszkszab-adatvedelem

d. **Az ISZK Üzemeltetési Szabályzata**
   A szabályzat elérhető az alábbi URL-en: http://www.uni-corvinus.hu/iszkszab-uzemeltetes
   Az open laborok, a projektoros és tanári gépek felhasználási házirendje A házirend elérhető az alábbi URL-en: http:// www.uni-corvinus.hu/iszkszab-hazirend

e. **Az ISZK adatvédelmi szabályzata**
   http://iszk.uni-corvinus.hu/fileadmin/user_upload/cornet/hu/kozponti_szervezeti_egysegek/informatikai_szolgaltato_kozpont/files/iszk/szabalyozottsag/szabalyzatok_2011/BCE-ISZK_Adatvedelmi_szabalyzat.pdf

f. **A Campus rendezvényszabályzata**
   http://kozgazcampus.uni-corvinus.hu/fileadmin/user_upload/hu/kozponti_szervezeti_egysegek/campusok/kozgaz/campus/Szabalyzatok/HGR_Szabalyzat_Kancellari_utasitas_2015.08.05..pdf

Felhívjuk a felhasználóink figyelmét, hogy az IBSZ rendelkezésein túl mindenkor szem előtt kell tartani az egyéb egyetemi szabályokat és a hatályos jogszabályokat is!