UNIVERSITAS SCIENTIARUM SZEGEDIENSIS
SZEGEDI TUDOMÁNYEGYETEM

Valamennyi Egységvezető részére
e-mail útján

Iktatószám: JIG-SZTE/1071-1/2025.
Tárgy: 6/2025. (XI.18.) sz.
rektori-kancellári együttes körlevél az információbiztonsági tudatosság növeléséről

Tisztelt Egyetemi Vezető!

Az információbiztonságért vállalt felelősség, az adott szervezet vezetése által meghatározott biztonsági szintnek, mint követelménynek az elfogadása, a biztonsági szempontból erkölcsös, etikus magatartási kultúra együttesen jellemzi a biztonságtudatos szervezetet.

A Szegedi Tudományegyetem vezetése kiemelten fontosnak tartja a biztonságtudatos szervezeti kultúra kialakítását, amelyben az Egyetem munkatársai, hallgatói ismerik jogaikat és kötelezettségeiket.

A biztonsági kultúrát az egyének biztonságtudatos magatartása alakítja ki, amelyben a felhasználó képes érzékelni a biztonságot veszélyeztető eseményeket, és képes ennek megfelelően cselekedni.

A tudatosság kialakítása, annak fenntartása informatikai biztonsági oktatások, tájékoztatók keretein belül történik. Az oktatás az informatikai biztonság leggyengébb láncszemét, az embert helyezi középpontjába, annak biztonságtudatos felkészítésével, biztonságtudatos éberségének kialakításával.

Felhívjuk a Tisztelt Egyetemi Vezetők figyelmét, hogy az információbiztonság tudatossági oktatás több okból is kiemelten fontos:

1. **Biztonsági kultúra kialakítása**: a biztonsági kultúra akkor jó, ha a munkatársak ismerik jogaikat és kötelezettségeiket. A biztonságtudatos magatartás kialakítása és fenntartása érdekében az informatikai biztonsági oktatások középpontjában az ember áll, annak biztonságtudatos felkészítésével és éberségének kialakításával.
2. **Prevenció**: Az informatikai biztonsági oktatások célja a nem biztonságtudatos viselkedések minimalizálása. Ez segít megelőzni, hogy a kiberbűnözők csaló módszerekkel megszerzett adatok birtokában jogosulatlanul hozzáférjenek az egyetemi infrastruktúrához, az intézmény információs rendszereihez és adataihoz.
3. **Szabályok betartása**: Az oktatások során a munkatársak megtanulják, hogy milyen viselkedés veszélyezteti a biztonságot, és mit kell tenniük ilyen helyzetekben. Ez

4. magában foglalja a szakképzetlenség, szakszerűtlen üzemeltetés, szándékos károkozás, eltulajdonítás, megvesztegetés és figyelmetlenség kezelését.
5. **Adatvédelem**: Az SZTE kiemelt fontosságúnak tartja az általa kezelt személyes adatok védelmét. Az információbiztonság tudatossági oktatások segítenek abban, hogy a munkatársak és hallgatók a mindennapi gyakorlat során tisztában legyenek az adatvédelmi jogi és adatbiztonsági előírásokkal, ismeretekkel és azok betartásával, illetve a személyes adatok védelmét biztosító egyéb szabályozókkal, köztük a GDPR előírásaival.
6. **Folyamatos fejlődés**: Az információbiztonsági oktatások folyamatos tevékenységek, amelyek célja a biztonságtudatosság erősítése.

Ezek az oktatások növelik a szervezet általános biztonsági és védelmi szintjét, hozzájárulnak a munkatársak tudatosságának és felelősségtudatának erősítéséhez, és jelentős szerepet játszanak a NIS2 irányelv (Network and Information Security Directive 2) kritériumainak teljesítésében, az IT biztonsági kockázatok csökkentésében.

A NIS2 irányelv célja az információs rendszerek és hálózatok biztonságának növelése az Európai Unióban. Az irányelv szigorúbb követelményeket ír elő a kiberbiztonsági események kezelésére, és fokozott koordinációt követel meg a tagállamok között. Az információbiztonság tudatossági oktatás az alábbi módokon segíthet a NIS2 kritériumok teljesítésében:

1. **Tudatosság növelése**: Az oktatások révén a munkatársak jobban megértik a kiberbiztonsági fenyegetéseket és azokat a szabályokat, amelyekkel ezek ellen védekezhetnek. Ez segít abban, hogy a szervezet megfeleljen a NIS2 irányelv által előírt biztonsági követelményeknek.
2. **Képzés és felkészítés**: A NIS2 irányelv előírja, hogy az érintett szervezeteknek megfelelő képzést kell biztosítaniuk a munkatársaik számára. Az információbiztonság tudatossági oktatások biztosítják, hogy a munkatársak naprakész ismeretekkel rendelkezzenek a legújabb kiberbiztonsági gyakorlatokról és szabályozásokról.
3. **Incidensek megelőzése, kezelése**: Az oktatások során a munkatársak megtanulják, hogyan lehet megelőzni a kiberbiztonsági incidenseket, valamint azt, hogyan szükséges reagálniuk a bekövetkezett incidensekre, és milyen lépéseket kell tenniük a károk minimalizálása érdekében. Ez hozzájárul a NIS2 irányelv által előírt incidenskezelési követelmények teljesítéséhez.
4. **Emberi tényező kezelése**: Az oktatások segítenek a munkatársaknak felismerni és elkerülni a kiberbiztonsági fenyegetéseket, mint például a phishing támadásokat és a szociális mérnöki módszereket. Ezáltal csökken az emberi hibákból eredő kockázatok száma.
5. **Biztonsági protokollok betartása**: Az oktatások során a munkatársak megismerik a szervezet biztonsági protokolljait és eljárásait, és megtanulják, hogy hogyan kell ezeket betartani. Ez növeli a szervezet általános biztonsági szintjét.
6. **Folyamatos fejlődés**: Az információbiztonság tudatossági oktatások folyamatosan frissülnek, hogy lépést tartsanak a legújabb kiberbiztonsági fenyegetésekkel és technológiákkal. Ez biztosítja, hogy a szervezet mindig naprakész legyen a legújabb biztonsági kihívásokkal szemben.

Mindezekre tekintettel összességében az információbiztonság tudatossági oktatás elengedhetetlen a NIS2 irányelv kritériumainak teljesítéséhez és az IT biztonsági kockázatok csökkentéséhez, mivel növeli a munkatársak tudatosságát, javítja a biztonsági protokollok betartását, és segít a kiberbiztonsági incidensek megelőzésében és hatékony kezelésében.

A fenti célok érdekében az SZTE Informatikai és Szolgáltatási Igazgatósága az RRF-2.1.2 pályázat keretében elkészítette az egyetemi munkatársak, valamint egyetemi hallgatók számára szóló biztonságtudatossági oktatási anyagokat. Az oktatási anyagok az SZTE Coospace felületén érhetők majd el.

A szervezeti célok elérése, az információbiztonsági kockázatok kezelése és csökkentése, a biztonságtudatos szervezeti kultúra kialakítása érdekében minden egyetemi munkatárstól és hallgatótól elvárt a fenti szabályok betartása, amelyek megismerésében nyújtanak segítséget a kidolgozott oktatási anyagok.

Ennek elérése érdekében kötelező az adatbiztonsági szabályok megismerése, az oktatási anyagok elsajátítása.

Az oktatási anyagok elérhetőségéről és az oktatások lebonyolításának részleteiről külön rektori-kancellári utasítás kerül kiadásra.

Felkérjük a Tisztelt Egységvezetőket, szíveskedjenek gondoskodni arról, hogy jelen körlevél tartalmát valamennyi munkatársuk megismerje és kérjük Önöket, hogy működjenek közre az elrendelt intézkedések végrehajtásában, a szabályok betartásában.

Kelt: Szegeden, 2025. év november hó 17. napján

Tisztelettel:

Dr. Fendler Judit
kancellár

Prof. Dr. Rovó László
rektor