DEBRECENI EGYETEM

Informatikai biztonság és kibervédelmi tudatosság oktatási és képzési stratégia

A biztonság az Egyetemi kultúra része, megléte nem érzékelhető,

csak annak hiánya

Tartalom

1. Dokumentum menedzsment

1.1. Dokumentum leíró adatok

Intézmény megnevezése:	Debreceni Egyetem
Dokumentum címe:	Informatikai biztonság és kibervédelem tudatosság oktatási stratégia
Dokumentum adatosztályozási besorolása:	Belső használatra
Dokumentum állapota:	Átdolgozott, Jóváhagyva
Dokumentum leírása:	A Debreceni Egyetem adatai, információi bizalmassága, sértetlensége, rendelkezésre állása, valamint az informatikai biztonság teljeskörű biztosítása, a dolgozóinak magas szintű tudatosság kialakítása, fenntartása és fejlesztése támogatottsága által.
Dokumentum kódja:	DE-IBTS-2025/V1
Jogszabály compliance:	2024. évi LXIX. törvény *Magyarország kiberbiztonságáról (Kiberbiztonsági tv.),* 418/2024. (XII. 23.) Korm. rendelet *Magyarország kiberbiztonságáról szóló törvény végrehajtásáról,* 7/2024. (VI. 24.) MK *rendelet, a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről*
Dokumentum felülvizsgálata:	Legalább évente. Jelentősebb szabályzó változás esetén. Protokoll folyamat hatékonyságát, eredményességét érintő incidenskezelési megállapítás, tapasztalat, okulás esetén.

1.2. Dokumentum változásai

Verzió	Dátum	Készítette	Jóváhagyta	Változat leírás
V. 1.0	2024.09.30.	Tóth Attila Központvezető DE Kancellária Biztonsági Igazgatág Informatikai Biztonsági Központ	Prof. Dr. Bács Zoltán Debreceni Egyetem Kancellár	Első kiadás
V. 2.0	2025.07.31.	Tóth Attila Igazgató DE Kancellária Biztonsági Igazgatág Informatikai Biztonsági Központ	Prof. Dr. Bács Zoltán Debreceni Egyetem Kancellár	Törvényi változás miatt átdolgozva

készítette

jóváhagyta

Felelősség

1.3. Dokumentum elkészítése, felügyelete, felülvizsgálata

Név	Szervezet	Beosztás
Tóth Attila	Informatikai Biztonsági Központ	Igazgató

1.4. Dokumentum szakmai tartalma

Név	Szervezet	Beosztás
Tóth Attila	Informatikai Biztonsági Központ	Igazgató

1.5. Szabályozás szakmai végrehajtása

A stratégia teljeskörű megvalósításában, az elért eredmények magas szintű fenntartásában érintett szervezeti egységek vezetői és a szervezeti egységek munkavállalói.

1.6. Szabályozás végrehajtás ellenőrzése

Kiberbiztonsági audit (SZTFH által akkreditált szervezet)
Informatikai Biztonsági Központ tervezett, célzott ellenőrzése

2. Bevezető

A tudatosság egy olyan állapot, ami a dolgozók napi rutinját, valamint, az ehhez kapcsolódó ismeretanyagát fejezi ki.

A biztonságtudatosság, a biztonság számára kedvező állapotot jelenti, ahol minden érintett ismeri és napi feladatvégzése során rutinszerüen alkalmazza a számára szükséges és elégséges információkat, erőforrásokat, szem előtt tartva a biztonság legfőbb alapelveivel kapcsolatos egyéni teendőit, ami szavatolja a Debreceni Egyetem (továbbiakban: Egyetem) adatkezelésében megjelenő adatok, információk bizalmasságát, sértetlenségét és rendelkezésre állását.

Az információval szemben elvárás, hogy a megfelelő időben, pontosan, és naprakészen álljon rendelkezésre, de csak azok számára, akik jogosultak megismerni azt. Ez az információ minden formájára igaz, azaz a szóban, a papíron, és az elektronikus formában tárolt, kezelt, feldolgozott és továbbított formáira egyaránt.

A biztonságtudatosság kialakítása az Egyetemen belül az a magatartásforma, ami az Egyetem biztonság stratégiájával egybehangzóan, minden egyéni szinthez differenciáltan olyan biztonságtudatos magatartást határoz meg, ahol az Egyetem munkatársai tisztában vannak azzal, hogy;

- a biztonság és az ehhez tartozó adott biztonsági szintek megfelelöek és szükségesek az Egyetem számára,
- a biztonság fontos az Egyetem reputációja érdekében,
- a biztonság hiánya következményekkel jár,
- a biztonság figyelmen kívül hagyásának, be nem tartásának, a felelőtlen magatartásnak súlyos következményeket (anyagi) magában hordozó biztonsági kockázatai vannak,
- az ö felelősségük, hozzáállásuk, tevékenységük kihatással van a biztonság egyes területeire.

A stratégia kialakításának, fenntartásának, fejlesztésének céljai;

a) a jogkövető magatartás és a jó hírnév (reputáció) érdekében védeni az Egyetem információ, adat értékeit,
b) a tudatosság, a szervezettség, a hatékonyság és a technikai megoldások használata segítségével növelni az információbiztonságot, sértetlenséget, a személyes adatok jogszerű kezelését
c) a megelőzés, a tájékoztatás, az oktatás, a felderítés és a szankcionálás eszközeivel hatékonnyá tenni az intézkedések érvényesítését.

Az Egyetem polgárainak informatikai, kiberbiztonsági tudatosság képzése, az állandó változás időszerű, gyors kezelése megalapozzák az Egyetem elektronikus információs rendszereivel kapcsolatba kerülő személyek felé támasztott minimum információbiztonsági követelményeket, ezáltal meghatározva azokat az elvárásokat, kötelezettségeket és a felelősségeket, amelyekre az adatvédelem, a biztonságos- információellátás és üzletmenetfolytonosság érdekében feltétlenül szükség van.

A biztonságtudatos viselkedés a legfontosabb védelmi vonal, ami egy preventív védelmi intézkedés. Minden rendszer annyira sebezhető, sérülékeny, mint ahogy a leggyengébb eleme. A biztonság leggyengébb láncszeme az ember, a „felhasználó", így kiberbiztonság, informatikai biztonság

tekintetében magának az embernek a biztonságtudatosságát kell növelni az elkerülhető incidensek megelőzése érdekében.

A stratégia a kitűzött cél elérésének átfogó terve, a jövőalkotás eszköze.

A stratégia egy hosszú távú terv vagy tervezési folyamat, amely meghatározza az Egyetem céljait és az azok eléréséhez szükséges lépéseket.
A stratégia segít meghatározni, hogy az Egyetem hogyan fogja felhasználni az erőforrásait, hogyan fogja kihasználni a lehetőségeket és kezelni a kihívásokat annak érdekében, hogy elérje a kitűzött célokat.
A stratégiai tervezés során az Egyetem megvizsgálja a belső és a külső környezetét, az erősségeit és gyengeségeit, a lehetőségeket és fenyegetéseket, valamint az elérni kívánt eredményeket. Az eredmények alapján kialakítja a stratégiáját, amely az Egyetem hosszú távú irányvonalát és cselekvési tervét határozza meg.
A stratégia, lehetőséget ad az Egyetemnek a hosszú távú sikerek elérésére és fenntartására, és segít a fókuszáltabb és összehangoltabb cselekvések meghozatalában.
A stratégiai tervezés során fontos figyelembe venni az Egyetem küldetését, értékeit és a környezetet. A stratégiai döntések befolyásolhatják az Egyetem szerkezetét, működését, erőforrásainak felhasználását és az eredmények mérését.

Összességében a stratégia egy átfogó terv, amely segít az Egyetemnek hosszú távú céljai elérésében.

3. Cél

Az Egyetemi közösség, Egyetemi trendnek megfelelően elvárt magas szintű biztonságtudatosságának elérése, ami elkötelezettségben érezhető.
Az elkötelezettség eredményezi a közösség szabályok betartásával kapcsolatos belső motiváció kialakítását. A belső motiváció szabálykövető magatartáshoz vezet, melynek során nem kényszerként és teherként élik meg a dolgozók az információbiztonságot, valamint általa kialakítható egyfajta közösségi szellem is az információbiztonság folyamatos fenntartása és fejlesztése érdekében.

Definíció leírat szerint, *„ A biztonság a rendszer olyan – az érintett számára kielégítő mértékű – állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg.”*

Az „Informatikai biztonság és kibervédelmi tudatosság oktatási és képzési stratégia” keretében megfogalmazott tevékenységeknek, a definícióban megfogalmazott elvárások teljesítése érdekében, nem csak digitális formába öntötten leírt, hanem tevőlegesen megvalósult cselekvéseknek kell lenniük.

A stratégia ne egy dokumentum, a biztonság meglétének látszata legyen, ami eleget tesz jogszabályoknak vagy hatósági elvárásoknak, hanem alkalmazott módszer, kotta, ami az Egyetemi közösség, közösségi és elhivatott hozzáállását célozza meg, az Egyetemi érdekek, Egyetemi értékek védelmében.

4. Hatály

Az Egyetem egészére vonatkozik.
Hatályaira, mint tárgyi, személyi. szervezeti, területi, időbeni mindenkor a szenátus által elfogadott és jóváhagyott az Egyetem IBSZ-ben leírtak az irányadók.

5. Hatáskör és illetékesség

Belső, nyilvános dokumentum, amelyet a „Informatikai biztonság és kibervédelmi tudatosság oktatási stratégia" személyi hatálya alá nem tartozó harmadik természetes-, és jogi személy csak és kizárólag érintettségi minőségben, szolgáltatásnyújtásának mértékéig ismerhet meg.

6. Kapcsolat más szabályzatokkal

Releváns belső szabályzatok;

a) DE IBSZ
b) DE Belső adatvédelmi szabályzata,
c) DE Egészségügyi adatkezelési és adatvédelmi szabályzata.
d) Tesztelési, felügyeleti és képzési eljárásrend (DE IBSZ gyakorlati végrehajtó utasítása)

Rendeletek, törvények;

a) 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.),
b) 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról,
c) 7/2024. (VI. 24.) MK rendelet, a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

7. Kiadás dátuma és érvényessége

A Debreceni Egyetem Kancellárjának jóváhagyása napján lép érvénybe és válik hatályosan alkalmazhatóvá. Érvényessége a felülvizsgálat során kiadott új verzió közreadásáig tart.

8. A dokumentum minősítése

Az „Informatikai biztonság és kibervédelmi tudatosság oktatási és képzési stratégia" dokumentum minősítése, „*Belső nyílvános*"

9. Felülvizsgálat

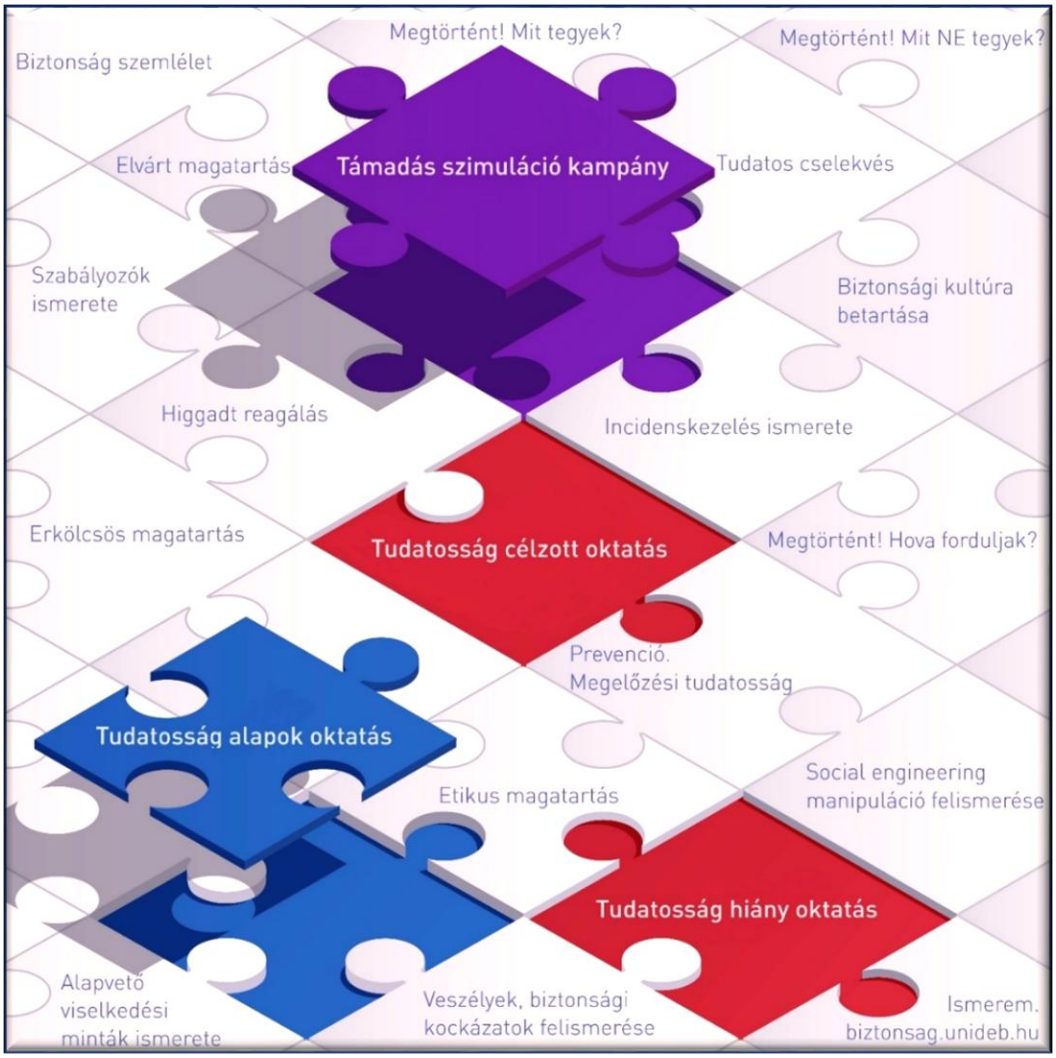
Az Egyetem, jelen stratégiai dokumentumát folyamatosan fejleszti és tökéletesíti, amit érintettség hiányában, legalább évente egy alkalommal felülvizsgál. A megfelelőségi vizsgálat kiterjed a végrehajtás, valamint a felmerülő informatikai, információbiztonsági és adatvédelmi események és az ezekkel összefüggő biztonsági tevékenységek ellenőrzésére.
Módosítani szükséges, ha a benne szereplő adatok, jogi hivatkozások, utalások, tényszerű adatok megváltoznak, ha az Egyetem elektronikus információs rendszereinek működésében vagy az Egyetem elektronikus információs rendszereinek működését meghatározó jogszabályi környezetben változások következnek be. Módosítás indokolt továbbá az elavult informatikai technológiai megoldások kivezetése, és az új technológiai újítások bevezetése során.

A felülvizsgálat és módosítás kezdeményezése, valamint a felülvizsgálat és módosítás elvégzése az Informatika Biztonsági Központ vezetője vagy az általa kijelölt személy feladata. A módosítások engedélyezése és az újabb változat jóváhagyása, a Debreceni Egyetem Kancellárjának a hatásköre.

10. Stratégia tervezés

Hosszabb időtávot átfogó folyamatos tevékenység, ami az Egyetem céljának, céljainak elérését támogatja.

A stratégia tervezés különböző tevékenységek összeillesztéséből (puzzle) áll, aminek teljességét, sikerét azok logikai, célirányos és pontos egymásra, egymáshoz kapcsoládása jelenti, ciklikus valamint külső érintő változás esetén ismétléssel.



A stratégiai folyamat működtetésének célja, hogy az Egyetem minden munkavállalója ismerje meg a;

- digitális biztonságot fenyegető kockázatokat,
- kibertámadási formákat,
- biztonsági események,
  - kezelési módjait,
  - során történő viselkedést,

  - bekövetkezése esetén értesítendő szervezeteket,
- preventiv, megelőző viselkedéseket, tevékenységeket

A stratégia tervezés alapja a képzési terv.
Kidolgozása az Informatikai Biztonsági Központ illetékessége.

A képzési tervnek tartalmaznia kell;

1. Biztonsági tudatosság, éberség felmérése támadás szimulációs tréning végzésével
2. Új munkavállalók tudatosság alapok képzése
3. Célzott tudatosság oktatás (évenként szintentartó)
4. Szimulációs kampány során „áldozatul esett" munkavállalók, célzott tudatosság hiány oktatása

10.1. Biztonsági tudatosság, éberség felmérése támadás szimulációs tréning keretében

Feladat:

Potenciális humán veszélyek feltérképezése, információbiztonsági tudatosságot erősítő oktató és támadás szimulációs keretrendszerben publikált támadás szimulációs kampányon, tréningen keresztül, ezek feldolgozása, elemzése, értékelése.

Cél:

Az Egyetem munkatársainak informatikai biztonsági tudatosság szintjének felmérése.
Évente több, random alkalommal szimulációs teszt, a dolgozók egy kiválasztott csoportján.

Módszer:

„Oktatási és adathalász szimulációs keretrendszer" használata, amely valós szimulációkkal teszi lehetővé az informatikai rendszerek felhasználóinak éberség, felkészültség és ad hoc viselkedés felmérését.

Elemzés, értékelés:

A szimulációs tréning alábbi mutatóinak elemzése választ ad a „hol tartunk", „mi még a feladat" kérdéseinkre

- megnyitott e-mailek száma;
- kattintások száma;
- az e-mailt biztonságtudatosan jelentő felhasználók száma (ibk@unideb.hu, ibk.helpdesk@unideb.hu);
- azon felhasználók, akik kattintottak;
- azon felhasználók, akik belépő (azonosító) adatokat is megadtak;
- azon felhasználók, akik letöltöttek egy fájlt.

A szimulációs tréninget képzés előzi meg, ami szituációs esetek prezentálásával egyértelműen szemlélteti az elvárt cselekvést, biztonságtudatos viselkedést.

A képzés végén informáljuk a munkavállalókat arról, hogy a tudásanyag elsajátítása jelen képzést teszt kérdéseken túl, szimulációs tréning formában is ellenőrzésre kerül, azzal a megjegyzéssel, hogy ezek az ismeretek magánszemélyként is hasznosak számukra!

Mivel a szervezeti vezetők kiemelt fenyegetésnek vannak kitéve, nem maradhatnak ki a kampányból, feltétlen részesei kell, hogy legyenek, mivel a törvényi rendelkezés külön kitér ennek fontosságára.

10.2. Új munkavállalók tudatosság alapok képzése

Feladat:

Az Egyetem új munkavállalóinak informatikai biztonsági alapok képzése, valamint az Egyetem hatályos Információbiztonsági Szabályzat kivonatának és Információbiztonsági politikájának megismertetése és elfogadtatása.

Cél:

Az új munkavállalók Egyetem érdekében elvárt informatikai biztonság tudatosságának, felelősségteljes és szabályzóknak eleget tévő viselkedésének, viselkedési normáinak megismertetése.

A szabályok betartatásával biztosítható a bevezetett biztonsági, védelmi intézkedések által várt magasabb szintű információ-, adat- és informatikai biztonság megteremtése.

Módszer:

eLearning tananyag, teszt

Tananyagok.

- IBSZ és eljárásrend oktatás
- Informatikai biztonsági tudatosság I., II.
- Social Engineering oktatás

Pszichológiai manipuláció (Social engineering) oktatási anyag megtekintése

A pszichológiai manipuláció az informatikában olyan megtévesztő viselkedés, amely arra irányul, hogy a megtévesztett személy az egyébként nem jogosult megtévesztő számára bizalmas adatokat adjon át, vagy lehetőséget biztosítson a rendszerbe történő belépésre (Wikipedia).

Elemzés, értékelés:

A biztonsági tudatosság tananyag megismerése, az abban foglaltak megértése tesztkérdésekre adott válaszok alapján kerül kiértékelésre.

Random 5 kérdésre kell válaszolnia a munkavállalónak. 3 helyes válasz (60 %) a sikeres értékelés kritériuma, melyről tanúsítványt állít ki a rendszer (1. sz. melléklet).

10.3. Célzott tudatosság oktatás

Feladat:

a) Célcsoport tudatosság képzés.

A meghatározott célcsoportok.

- Általános felhasználók
- Kiemelt felhasználói jogokkal rendelkező vezetők, felsővezetők
- Szakértői képzés – „system hardening", sérülékenységmenedzsment üzemeltetők
- Informatikai üzemeltetés
- Biztonsági személyzet
- Szerepkör alapú

b) Témaorientált, tematikus képzés

- Egyetemi specialitás
- Viselkedés minták

Cél:

a) Célcsoport tudatosság képzés

Általános felhasználók

A képzés elsődleges célja az általános felhasználók információ biztonság-tudatossági szintjének emelése, tudatosságának erősítése. Az előadások anyaga a szervezet információ biztonsági igényeinek és elvárásainak megfelelően kerül felépítésre és összeállításra.

Kiemelt felhasználói jogokkal rendelkező vezetők, felsővezetők

Az Egyetem dolgozóinak információ biztonság-tudatossága akkor és úgy növelhető, tartható fenn a leghatékonyabban, ha a biztonsági tudatosság javítására szolgáló intézkedések az Egyetem vezetésének teljes támogatásával valósulnak meg, és a vezetők maguk is szem előtt, fontosnak és támogatandónak tartják az Egyetem adat-, információ-, és informatikai biztonságát.

Szakértői képzés – „system hardening", sérülékenységmenedzsment üzemeltetők

A szakértői képzés koncepciójában különbözik az általános felhasználóknak illetve a kiemelt felhasználói jogokkal rendelkező vezetőknek szánt ismertető jellegű képzésektől.

Az eltérés lényege, hogy a szakértői szintű információbiztonság-tudatosság képzés koncepcionálisan közelíti meg az informatikai rendszer lehetséges sérülékenységeit.

A komplex sérülékenységmenedzsment megközelítést helyezi az eseti sérülékenységek elhárítására törekvő szakmai viselkedés helyett.

A koncepció szereplői azok a munkatársak, akik a prevenció, észlelés, havaria team feladatok, elhárítás és az utólagos elemzés érintettjei, az Egyetem EIR-jeit működtető, üzemeltető, felügyelő és fejlesztő rendszer adminisztrátok, rendszergazdák, rendszerfelügyelők, kiemelt, privilegizált jogú felhasználók, fejlesztők.

Informatikai üzemeltetés

Az Egyetemi informatika üzemeltetői kiemelten fontos szerepet töltenek be az Egyetem működésében, működésfolytonosságának fenntartásában, mivel ők azok, akik birtokolják a tudást, ismeretet az Egyetem hálózatáról, szervereiről, EIR-jeiről, azok működéséről és kapcsolatairól, így, ők képesek megoldani a felmerülő problémákat.

Ennek a komplex, és az Egyetem nagyságát tekintve bonyolult, de összetett rendszerének megbízható müködése csak a biztonsági előírások, szabályzatok betartása, betartatása esetén eredményes.

A betartás az informatikai üzemeltetés oktatásán, a betartatás az Ő közreműködésükkel, mint akik naponta érintkeznek a felhasználókkal, valósítható meg, az Egyetemi magas szintű elvárás érdekében.

Biztonsági személyzet

A biztonsági személyzet részére a fizikai biztonsággal kapcsolatos ismeretek elmélyítése, a területre jellemző kockázatok, fenyegetettségek kezelésére vonatkozó oktatást kell végezni.

A gyakorlati példákon keresztüli megközelítésen (objektumvédelem, védendő adatvagyon elemei, adatvédelmi kérdések, kiemelt infrastruktúra védelem, belépés felügyelet, social engineering) keresztüli szemléltetés módszere alkalmazásával.

b) Témaorientált, tematikus képzés

Egyetemi specialitás

Az Egyetem egészségügyi szolgáltatást nyújtó szervezeti egységeiben dolgozó munkavállalók, bizalmas jellegű egészségügyi adatokat (szenzitív adatok, GDPR besorolás szerint; különleges adatok) kezelnek. Ezek az adatok a kiber térben rendkívül keresettek, így heckerek megszerzési célpontjai lehetnek. Védelmük specialitása, hogy nem csak a medikai rendszer adatbázisaiban lelhetők fel, hanem diagnosztikai eszközök lokális tároló helyein, képi anyagok header részében, interface csatornák (rendszerek közötti kommunikáció) tartalmában. Védelmük összetett biztonsági tudásanyag által támogatható.

Viselkedés minták

Ma már számos hackertámadási formával találkozhatunk, találkozhat a munkavállaló. Kiemelten fontos, hogy ezekre felkészítsük a dolgozókat, ahol tájékoztatást, ismeretanyagot kap;

- mi ez,
- mi a veszély,
- prevenció (megelőzés)
- mit kell tenni, ha bekövetkezik?

részletes ismertetés formájában.

Módszer:

eLearning tananyag, teszt

Tananyagok.

- IBSZ és eljárásrend oktatás
- Informatikai biztonsági tudatosság I.
- Informatikai biztonsági tudatosság II.
- Social engineering
- Szerepkörre készített speciális tananyagok
- Biztonsági esemény bejelentés folyamata

Amennyiben a munkaszervezeti egység vezetője igényli, kiscsoportos képzés keretében, személyi jelenlét mellet, az IBK munkatársai, informatikai biztonsági tudatosság előadást tartanak.

Tananyagok.

- Irányadó jogszabályaink
- IT Biztonság közérthetően
- IT Biztonsági kézikönyv
- IT Biztonsági fogalomtár
- Mesterséges intelligencia
- Kiber biztonság

Kiemelt felhasználói jogokkal rendelkező vezetők, felsővezetők részére;

- biztonságtudatosság, képzés, mások így csinálják, ezeket éltük túl, milyen hibákba futottunk bele és azt hogyan javítottuk terén nagyvállalati tapasztalattal rendelkező külső meghívottak tapasztalatcsere, módszer bemutató konzultációk,
- hatósági szakemberek követelmény, megoldás, tapasztalat előadásának

szervezése, évente legalább egyszer

Elemzés, értékelés:

A biztonsági tudatosság tananyag megismerése, az abban foglaltak megértése teszt kérdésekre adott válaszok alapján kerül kiértékelésre. Random 5 kérdésre kell válaszolnia a munkavállalónak. 3 helyes válasz (60 %) a sikeres értékelés kritériuma, melyről oklevelet állít ki a rendszer (1. sz. melléklet)

10.4. Szimulációs kampány során „áldozatul esett" munkavállalók tudatosság hiány oktatása

Feladat:

Az adathalász (phising) szimulációs kampány során nem biztonságtudatosan viselkedő dolgozó aki;

- megnyitotta a levelet,
- rákattintott a linkre,
- megadta személyes adatait,
- megadta belépési hitelesítő adatait.

célzott újra oktatása.

Cél:

Biztonság tudatos, megfelelő ismerettel rendelkező munkavállaló képzés, hogy az Egyetem dolgozóinak tudatlanságából, ismeret hiányából ne legyen „áldozat".
A munkaválllaló érték és ne kockázat legyen az Egyetem számára.

Módszer:

eLearning tananyag, teszt, szükség esetén személyes jelenlétű

Elemzés, értékelés:

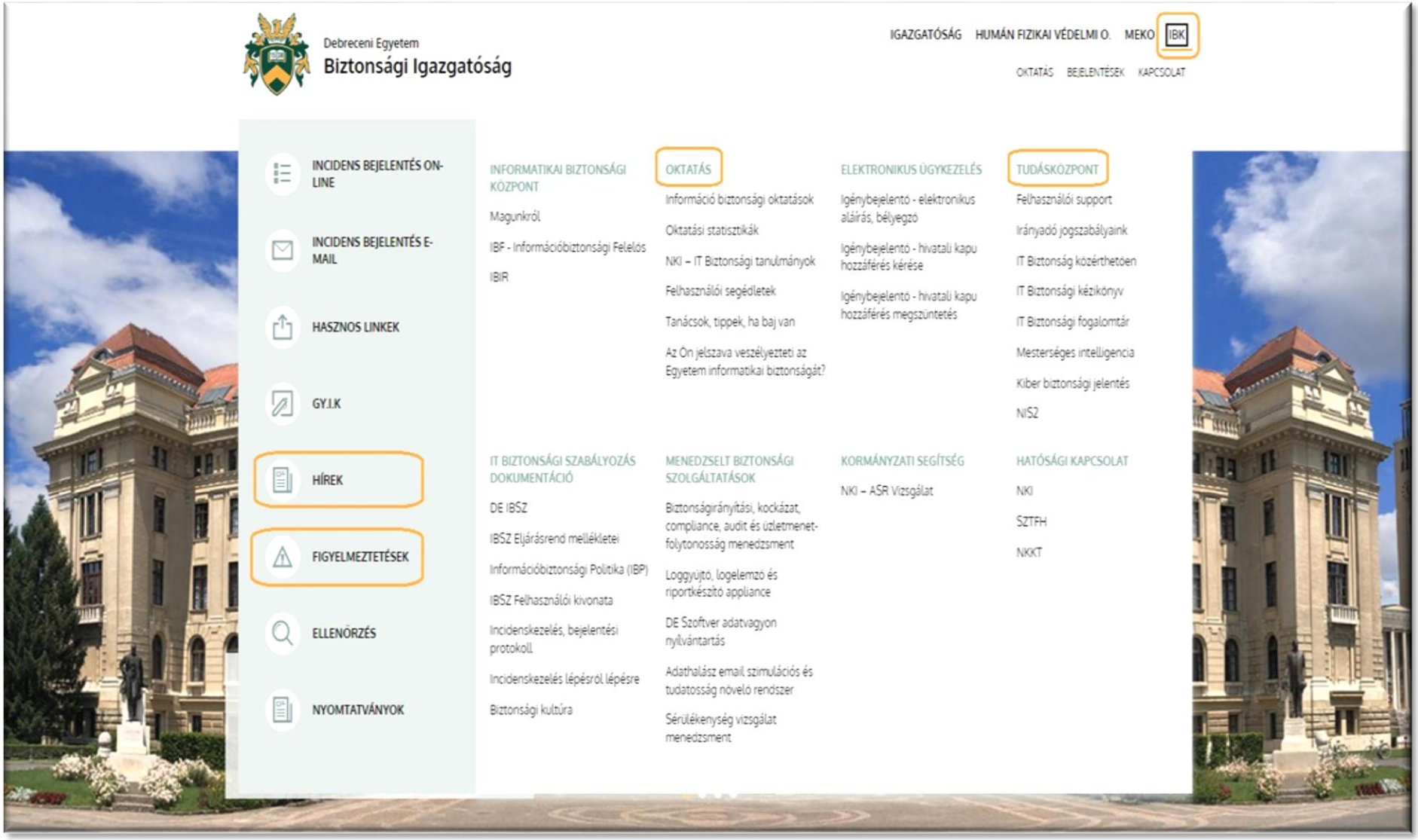
A biztonsági tudatosság tananyag megismerése, az abban foglaltak megértése teszt kérdésekre adott válaszok alapján kerül kiértékelésre.
Random 5 kérdésre kell válaszolnia a munkavállalónak. 3 helyes válasz (60 %) a sikeres értékelés kritériuma, melyről oklevelet állít ki a rendszer (1. sz. melléklet).

11. Biztonsági tudatosság fenntartás (….teljeskörű, folytonos…)

Az oktatásokkal, konzultációkkal, előadásokkal kialakított adat,-, információ-, és informatikai biztonság tudatosság fenntartása, valamint az új fenyegetések, támadások elleni védekezés, preventiv viselkedés, viselkedési norma tudatosításához, az Egyetem Biztonsági Igazgatóságának honlapján létrehozott Informatikai Biztonsági Központ felületének, „Tudásközpont", „Oktatás", „Hírek" és „Figyelmeztetések" szekciói állandó és naprakész információkat biztosít az Egyetemi polgároknak.

Link: https://biztonsag.unideb.hu/

Felület: A következő oldal nézete szerint.


Debreceni Egyetem
Biztonsági Igazgatóság
IGAZGATÓSÁG
HUMÁN FIZIKAI VÉDELMI O.
MEKO
IBK
OKTATÁS
BEJELENTÉSEK
KAPCSOLAT
INCIDENS BEJELENTÉS ON-LINE
INCIDENS BEJELENTÉS E-MAIL
HASZNOS LINKEK
GY.I.K
HÍREK
FIGYELMEZTETÉSEK
ELLENŐRZÉS
NYOMTATVÁNYOK
INFORMATIKAI BIZTONSÁGI KÖZPONT
Magunkról
IBF - Információbiztonsági Felelős
IBIR
OKTATÁS
Információ biztonsági oktatások
Oktatási statisztikák
NKI – IT Biztonsági tanulmányok
Felhasználói segédletek
Tanácsok, tippek, ha baj van
Az Ön jelszava veszélyezteti az Egyetem informatikai biztonságát?
ELEKTRONIKUS ÜGYKEZELÉS
Igénybejelentő - elektronikus aláírás, bélyegző
Igénybejelentő - hivatali kapu hozzáférés kérése
Igénybejelentő - hivatali kapu hozzáférés megszüntetés
TUDÁSKÖZPONT
Felhasználói support
Irányadó jogszabályaink
IT Biztonság közérthetően
IT Biztonsági kézikönyv
IT Biztonsági fogalomtár
Mesterséges intelligencia
Kiber biztonsági jelentés
NIS2
IT BIZTONSÁGI SZABÁLYOZÁS DOKUMENTÁCIÓ
DE IBSZ
IBSZ Eljárásrend mellékletei
Információbiztonsági Politika (IBP)
IBSZ Felhasználói kivonata
Incidenskezelés, bejelentési protokoll
Incidenskezelés lépésről lépésre
Biztonsági kultúra
MENEDZSELT BIZTONSÁGI SZOLGÁLTATÁSOK
Biztonságirányítási, kockázat, compliance, audit és üzletmenet-folytonosság menedzsment
Loggyűjtő, logelemző és riportkészítő appliance
DE Szoftver adatvagyon nyilvántartás
Adathalász email szimulációs és tudatosság növelő rendszer
Sérülékenység vizsgálat menedzsment
KORMÁNYZATI SEGÍTSÉG
NKI – ASR Vizsgálat
HATÓSÁGI KAPCSOLAT
NKI
SZTFH
NKKT

12. Biztonsági tudatosság oktatás kurzusai

Kötelezettek rövídítés magyarázata.

[ÚD] Új dolgozó
[ÁF] Általános felhasználók
[KF] Kiemelt felhasználói jogokkal rendelkező vezetők, felsővezetők
[SZÉ] Szakértői képzés – „system hardening", sérülékenységmenedzsment üzemeltetők
[IÜ] Informatikai üzemeltetés
[BSZ] Biztonsági személyzet

Kurzus megnevezése	Kurzus forma	Kötelezett						Kurzus zárás feltétel
		ÚD	ÁF	KF	SZÉ	IÜ	BSZ	
Adathalász szimuláció	Szimulációs rendszer		√	√		√		Teljesítés
IBSZ és eljárásrend oktatás	eLearning	√	√			√		Sikeres teszt
Social Engineering oktatás	eLearning	√	√	√	√	√	√	Sikeres teszt
Informatikai biztonsági tudatosság I.	eLearning	√	√		√	√		Sikeres teszt
Informatikai biztonsági tudatosság II.	eLearning		√	√	√	√		Sikeres teszt
Informatikai biztonsági kézikönyv	Web felület		√					Megtekintés
Fizikai védelmi eljárásrend	Web felület						√	Megtekintés

1. sz. Melléklet – Sikeresen elvégzett képzések tanusítványai

Tanúsítvány

Tuba Huba

Részére

aki az **Információ Biztonsági Szabályzat felhasználói kivonata és Információbiztonsági Politika**képzés tartalmát megismerte és nyilatkozott az abban foglaltak betartásáról.

Debrecen, 2024

DEBRECENI EGYETEM

Debreceni Egyetem, Kancellária
Biztonsági Igazgatóság
Informatikai Biztonsági Központ

Tanúsítvány

Tuba Huba

Részére

aki sikeresen teljesítette az **Informatikai Biztonsági Központ** által szervezett **Informatikai biztonsági tudatosság I.** képzést.

Debrecen, 2024.

DEBRECENI EGYETEM

Debreceni Egyetem, Kancellária
Biztonsági Igazgatóság
Informatikai Biztonsági Központ

Tanúsítvány

Tuba Huba

Részére

aki sikeresen teljesítette az **Informatikai Biztonsági Központ** által szervezett **Informatikai biztonsági tudatosság II.** képzést.

Debrecen, 2024.

DEBRECENI EGYETEM

Debreceni Egyetem, Kancellária
Biztonsági Igazgatóság
Informatikai Biztonsági Központ

Tanúsítvány

Tuba Huba

részére

aki sikeresen teljesítette az **Informatikai Biztonsági Központ** által szervezett **Social engineering** képzést.

Debrecen, 2024.

DEBRECENI EGYETEM

Debreceni Egyetem, Kancellária
Biztonsági Igazgatóság
Informatikai Biztonsági Központ

2. sz. Melléklet – 7/2024. (VI. 24.) MK rendelethez, Védelmi intézkedések katalógusa, 3. Tudatosság és képzés

Követelménycsoport megnevezése	Követelmény szövege	Teljesülés
3.1. Szabályzat és eljárásrendek	3.1. A szervezet: 3.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti a szervezet által meghatározott személyekkel szerepkörük szerint 3.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó tudatossági és képzési szabályzatot, amely 3.1.1.1.1. meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, a szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat, továbbá 3.1.1.1.2. összhangban van a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal. 3.1.1.2. a tudatossági és képzési eljárásrendet, amely a tudatossági és képzési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő. 3.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a tudatossági és képzési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel. 3.1.3. Felülvizsgálja és frissíti az aktuális tudatossági és képzési szabályzatot és a tudatossági és képzési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.	IGEN
3.2. Biztonságtudatossági képzés	3.2. A szervezet: 3.2.1. Biztonságtudatossági képzést biztosít a rendszer felhasználói számára (beleértve a vezetőket, felsővezetőket és a szerződéses partnereket is): 3.2.1.1. Az új felhasználók kezdeti képzése keretében, majd ezt követően a szervezet által meghatározott gyakorisággal. 3.2.1.2. Amennyiben az EIR-ben bekövetkezett változások ezt indokolttá teszik, vagy a szervezet által meghatározott események ezt megkövetelik. 3.2.2. Meghatározza azokat a technikákat, melyeket a rendszerfelhasználók biztonságtudatosságának növelése érdekében alkalmaz. 3.2.3. Frissíti a képzési és tudatossági tananyagot a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően. 3.2.4. Integrálja a belső és külső biztonsági eseményekből levont tanulságokat a képzési anyagokba, valamint az alkalmazott biztonságtudatossági eszközrendszerébe.	IGEN
3.3. Biztonságtudatossági képzés – Gyakorlati feladatok	3.3. A szervezet a felkészítő képzést olyan gyakorlati feladatokkal egészíti ki, amelyek szimulálják a biztonsági eseményeket.	IGEN
3.4. Biztonságtudatossági képzés – Belső fenyegetés	3.4. A szervezet felkészítő képzést nyújt a belső fenyegetések potenciális jeleinek felismerésére és jelentésére.	IGEN
3.5. Biztonságtudatossági képzés – Pszichológiai befolyásolás és információszerzés	3.5. A szervezet felkészítő képzést nyújt a pszichológiai manipuláció és adatgyűjtés lehetséges és valós jeleinek felismerésére, valamint azok jelentésére.	IGEN
3.6. Biztonságtudatossági képzés – Gyanús kommunikáció és szokatlan rendszerviselkedés	3.6. A szervezet felkészítő képzést nyújt a szervezet rendszereiben felmerülő gyanús kommunikáció és rendellenes viselkedés felismerésére.	IGEN

Követelménycsoport megnevezése	Követelmény szövege	Teljesülés
3.7. Biztonságtudatossági képzés – Tartós fejlett fenyegetések	3.7. A szervezet felkészítő képzést nyújt a tartós fejlett fenyegetések (APT) felismerésére és kezelésére vonatkozóan.	IGEN
3.8. Biztonság-tudatossági képzés – Kiberfenyegetési környezet	3.8.1. A szervezet felkészítő képzést nyújt a kiberfenyegetési környezetről és 3.8.2. alkalmazza az aktuális kiberbiztonsági fenyegetési információkat a rendszerüzemeltetésben.	IGEN
3.9. Szerepkör alapú biztonsági képzés	3.9. A szervezet: 3.9.1. Szerepkör alapú biztonsági képzést nyújt a felhasználóknak: 3.9.1.1. Az EIR-hez vagy az információhoz való hozzáférés engedélyezését vagy a kijelölt feladat végrehajtását megelőzően, továbbá azt követően a szervezet által meghatározott rendszerességgel. 3.9.1.2. Amikor az EIR-ben bekövetkezett változás azt szükségessé teszi. 3.9.2. Frissíti a szerepköralapú képzés tartalmát a szervezet által meghatározott rendszerességgel és a szervezet által meghatározott események bekövetkezését követően. 3.9.3. Beépíti a belső vagy külső biztonsági eseményekből levont tanulságokat a szerepköralapú biztonsági képzésekbe.	IGEN
3.10. Szerepkör alapú biztonsági képzés – Környezeti védelmi intézkedések	3.10. A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyek vagy szerepkörök számára a környezethez kapcsolódó biztonsági követelmények alkalmazásáról és működtetéséről.	IGEN
3.11. Szerepkör alapú biztonsági képzés – Fizikai védelmi intézkedések	3.11. A szervezet kezdeti és időszakos képzést biztosít a szervezet által meghatározott személyeknek vagy szerepköröknek a fizikai biztonsági követelményekből fakadó védelmi intézkedések alkalmazásáról és működtetéséről.	IGEN
3.12. Szerepkör alapú biztonsági képzés – Gyakorlati feladatok	3.12. A szervezet olyan biztonsági gyakorlati feladatokkal egészíti ki a felkészítő képzést, amelyek megerősítik a képzési célokat.	IGEN
3.13. A biztonsági képzésre vonatkozó dokumentációk	3.13. A szervezet: 3.13.1. Dokumentálja és nyomon követi az információbiztonsági képzési tevékenységeket, ideértve az általános információbiztonsági tudatossági képzéseket és a speciális szerepkör alapú információbiztonsági képzéseket. 3.13.2. Meghatározott ideig megőrzi a képzésről készült dokumentumokat.	IGEN
3.14. Képzés eredményeiről való visszajelzés	3.14. A szervezet rendszeresen visszajelzést ad a meghatározott személyeknek a szervezeti képzések eredményeiről.	IGEN