Árajánlat

e-Learning platform szolgáltatáshoz és tananyagokhoz

I. LMS PLATFORM

A Moodle LMS (Learning Management System) a világ legnépszerűbb e-learning platformja, mely elsősorban nagyvállalati és felsőoktatási intézmények számára készült oktatásmenedzsment rendszer. A Moodle egyszerre alkalmas a tananyagok tárolására, szerkesztésére, összeállítására, vizsgáztatásra, az egyes hallgatók tevékenységének nyomon követésére, értékelésére az oktatók és hallgatók közötti online digitális együttműködésre.

1. MEGFELELŐSSÉG FENNTARTÁSA A BIZTONSÁG ÉRDEKÉBEN

Problémamentes, költséghatékony e-learning tanfolyamaink ráébresztenek a szabályozói megfelelés és a biztonság fontosságára, segítenek munkatársainak a megfelelő munkamódszerek kialakításában, és támogatást nyújtanak abban, hogy cége megfeleljen az adatvédelmi előírásoknak (GDPR), elérje és fenntartsa az olyan akkreditációit, mint például az ISO szabvány, vagy a 2013. L. tv. szerinti megfelelés.

- Az e-learning költséghatékony, rugalmas és hatékony eszköz arra, hogy nagyszámú résztvevő számára biztosítsa a dolgozói tudatosság erősítését a napi munkavégzésben.
- Az összetett fogalmakat gyakorlati és nem technikai terminológiával magyarázza, megkönnyítve ezáltal a cég minden munkavállalója számára azok megértését.
- A résztvevők a saját tempójukban tanulhatnak, és a tanfolyamok elvégzését rugalmasan igazíthatják napi feladataikhoz.
- E-learning megoldásaink márkajelzéssel és bizonyos tartalmakkal testre szabhatók a szervezet igényeinek megfelelően.
- A felhasználóbarát irányítópult minimális adminisztrációt igényel.
- A tanfolyam tartalmát az iparág szakértői készítik, a kiberbiztonság, az adatvédelem és az informatika területén.

2. E-LEARNING TANFOLYAMAINK

- Csatlakozzon ahhoz a több ezer szervezethez, amelyek már használják az online e-learning tanfolyamokat.
- Gondoskodjon róla, hogy cége munkavállalói felismerjék a kiberbiztonsági és adatvédelmi kockázatokat, és időben tudjanak reagálni azokra.
- Tesztelje a munkavállalók tudását, hogy az auditok során cége igazolni tudja a kötelező oktatások elvégzését.
- Az iparági szakértők által kifejlesztett oktatási anyagainkat három havonta frissítjük annak érdekében, hogy a tartalom továbbra is hatályos és releváns maradjon.
- Szabja testre a tanfolyamokat a vállalati dokumentumokra, irányelvekre és eljárásokra mutató hivatkozások hozzáadásával.
- Gyors üzembe helyezés azonnali hozzáféréssel az összes tanfolyamhoz.

2.1. NIS2 Oktatási csomag

Mit tartalmaz az anyag?

Témák minden alkalmazott számára (beleértve a középszintű és a felső vezetést is)

- A NIS 2 irányelv alapjai (az összes vonatkozó cikkre kiterjed)
- Alapvető kiber higiéniai gyakorlatok
- Biztonsági események kezelése
- Biztonsági mentés
- Üzletmenet-folytonosság
- A többtényezős hitelesítés és a folyamatos hitelesítési megoldások használata
- Integrált kockázatelemzés szerepe

Témakörök informatikai alkalmazottak és biztonsági vezetők számára

- Az információs rendszerek biztonságára vonatkozó politika
- Katasztrófa utáni helyreállítás
- A hálózati és információs rendszerek beszerzésének, fejlesztésének és karbantartásának biztonsága
- A kriptográfia és titkosítás használatára vonatkozó politikák és eljárások
- Hozzáférés-szabályozás
- Vagyonkezelés
- Biztonságos hang-, video- és szöveges kommunikáció
- Biztonságos segélyhívási célú kommunikációs rendszerek
- Kockázatmenedzsment keretrendszer szerepe, feladat és felelősségi körök

Biztonsági menedzserekre vonatkozó témakörök

- A NIS 2 megfelelőség lépései
- Hogyan kapcsolódik a NIS 2 az ISO 27001-hez
- Hogyan kapcsolódik a NIS 2 a DORA-hoz?
- Hogyan kapcsolódik a NIS 2 a CER-hez?
- Hogyan kapcsolódik a NIS 2 az EU GDPR-hez?
- Az informatikai termékek és szolgáltatások tanúsítása
- A NIS 2-ben meghatározott kormányzati szervek
- Rendszeres kiberbiztonsági képzések szervezése a vállalat különböző szintű alkalmazottai számára
- A NIS 2 szerinti kockázatértékelés és kezelés elvégzése
- A beszállítók sebezhetőségének és minőségének értékelése
- Az emberi erőforrások biztonsága
- A kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelése
- Korrekciós intézkedések meghozatala

Témakörök felsővezetők és biztonsági vezetők számára

- Melyek azok az alapvető és fontos entitások, amelyeknek meg kell felelniük a NIS 2 előírásainak?
- A NIS 2 fő kiberbiztonsági követelményei
- kiberbiztonsági kockázatkezelési intézkedések jóváhagyása és felügyelete
- Válságkezelés
- A beszállítói lánc védelme
- Működésbiztonság
- Üzemeltetési kockázatok a mindennapokban
- Jelentéstételi kötelezettségek
- NIS 2 bírságok és kötelezettségek
- Az uniós országok kiberbiztonsági jogszabályai

2.2. Információbiztonsági és kiberbiztonsági tudatossági e-learning tanfolyam

A tanácsadás és képzés terén szerzett jelentős tapasztalataink felhasználásával ez a tanfolyam úgy van kialakítva, hogy megfeleljen az ISO 27001:2022 követelményeinek, amely előírja, hogy a biztonsági kérdéseket feltétlenül munkavállalói szinten kell kezelni.

A szabványnak való megfelelés fenntartása nem lehet az egyetlen oka annak, hogy a vállalatok információbiztonsági tudatossági képzéseket vezessenek be. A számítógépes támadásokkal kapcsolatos ismeretek és az ilyen fenyegetések megelőzésére vagy elkerülésére vonatkozó bevált gyakorlatok megosztása minden információbiztonsági és kiberbiztonsági stratégia szempontjából a leg fontosabb.

Mit tartalmaz az anyag?

- Bevezetés az információbiztonságba
- Bevezetés a kiberbiztonságba
- A kibertámadás lehetséges következményei
- Információbiztonsági kockázatok
    - Az információbiztonságot fenyegető veszélyek
    - Szervezeteken belüli sebezhetőségek
    - Veszélyeztetett területek

    - Felhasználói fiókok és jogosultságok
- Kiberbiztonsági kockázatok
    - Rosszindulatú programok
    - Adathalászat
    - Biztonságos webböngészés
    - Közösségi média kockázatok
- A kiber és információbiztonsági fenyegetések kezelése
- Hogyan védheti meg saját és a vállalata vagyonát
    - Rosszindulatú tevékenység észlelése
    - Mit tegyek?
    - Fontos dokumentumok, amelyekkel tisztában kell lennie

2.3. Otthoni munkavégzés (Home Office) kiberbiztonsági tanfolyam

Ez a rövid tanfolyam lehetővé teszi alkalmazottai számára, hogy biztonságban maradjanak a távoli munkavégzés során. A következőkre terjed ki:

- Hogyan maradhat biztonságban, ha otthonról dolgozik egy megosztott Wi-Fi hálózat használatával;
- Mi a megosztott Wi-Fi hálózat;
- Milyen intézkedéseket kell tenniük az alkalmazottaknak annak elkerülése érdekében, hogy kibertámadás áldozatává váljanak;
- Családtagok és az otthoni hálózat más felhasználói;
- A távmunka élményének javítása;
- A csalások típusai;
- Hogyan lehet elkerülni az adathalász és phishing csalásokat;
- Hogyan lehet elkerülni egy kiber átverést;
- A sötét weben terjedő koronavírus témájú rosszindulatú programok;
- Hogyan lehet biztonságosan böngészni;
- Mit kell tenniük az alkalmazottaknak, ha rosszindulatú mellékletet töltenek le, vagy gyanús hivatkozásra kattintanak

2.4. Védekezés Ransomware támadások ellen

Mire terjed ki a csomag?

- Példák ransomware támadásokra és azok következményeire.
- Példák arra, hogyan sérülhetnek egyének és szervezetek, ha ransomware támadás áldozatává válnak.
- A ransomware támadás megelőzésének előnyei.
- A ransomware támadás fő formái és azonosításuk módja.
- Az adathalászat és az incidensek bejelentésével kapcsolatos képzés fontossága.
- A kártevőirtó szoftverek helyes használata, a szervezet irányelveinek és eljárásainak követése, valamint a zsarolóvírus-támadásokra való reagálás.
- A személyes eszközök biztonságos használata munka közben.

Minden tanuló automatikusan megkapja exkluzív személyzeti tudatossági havi hírlevelünket, amely információkat tartalmaz a legújabb adathalász támadásokról és létfontosságú biztonsági tippekről, segítve munkatársait abban, hogy éberek maradjanak a legújabb fenyegetésekkel szemben.

2.5. Adathalász támadások veszélyei

Nem számít, hány technológiai védelem van érvényben, egyetlen e-mail szűrési módszer sem 100% -ban sikeres, ezért gyakran a címzettre bízzák annak eldöntését, hogy megnyit-e egy adathalász e-mailt, vagy rákattint-e egy rosszindulatú hivatkozásra. Itt lehet az adathalászattal kapcsolatos tudatossági képzés létfontosságú különbséget tenni.

Ez a tanfolyam segít Önnek és csapatának megérteni az adathalász támadások működését, a számítógépes bűnözők által alkalmazott taktikákat, valamint az adathalász kampányok észlelését és elkerülését.

Mire terjed ki a csomag?

- Mi az adathalászat?
- Az e-mailek és az adathalász támadások típusai
- Mi az a social engineering?
- Milyen következményekkel jár az adathalász támadás?
- Milyen könnyű adathalász támadás áldozatává válni
- Mi történik, ha rosszindulatú hivatkozásra kattint?
- Hogyan tervezik meg és hajtják végre a számítógépes bűnözők az adathalász támadásokat?
- Az adathalász csalások azonosítása
- Az adathalász csalások elkerülésének alapvető szabályai
- Adathalászat és közösségi média

2.6. Adatvédelmi tudatosság (GDPR, 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról) növelése e-learning tanfolyam

Mire terjed ki a csomag?

- Bevezetés az adatvédelembe és a GDPR-ba
- Mit jelent az adatok bizalmas kezelése, integritása és rendelkezésre állása, és hogyan lehet azokat fenntartani?
- Példák a személyes adatokra és a védelmük bevált gyakorlataira
- Hogyan segítenek a szervezeten belüli funkciók az adatok védelmében?
- Hogyan teljesíti a szervezet a kötelezettségeit, és ki kérhet további információkat?
- A legfontosabb adatvédelmi elvek és azok betartása

2.7. GDPR és Információbiztonság a HR számára

Mire terjed ki a csomag?

- A HR műveleteivel kapcsolatos legfontosabb GDPR-szempontok, beleértve az érintettek jogait és a személyes adatok feldolgozását.
- Milyen adatokra van szükség, és hogyan kell azokat biztonságosan tárolni a toborzási folyamat során, beleértve a hozzáférési jogokat is.
- A bevezetési folyamat, beleértve a referenciák megszerzését és a szűrést, valamint a szerződéses feltételek kezelésének módját.
- A bérszámfejtési folyamat és az, hogy kinek kell hozzáférnie ezekhez az információkhoz.
- Milyen HR-adatokat lehet és nem lehet megosztani.
- Az értékelési és fegyelmi eljárás, valamint a munkavállalókkal való kommunikáció.
- A munkavállalók betegszabadságával kapcsolatos titoktartás.
- Mit kell kérdezni/megválaszolni a kilépési interjúk során, és hogyan kell bizalmasan kezelni.
- Tudja meg, hogy milyen információkat kell megosztania, mikor oszthatók meg, kivel oszthatja meg az információkat, és mennyi ideig kell megőrizni a személyes adatokat.

2.8. GDPR és Információbiztonság a Marketing terület számára

Mire terjed ki a csomag?

- Mit kell figyelembe venni a személyes adatok gyűjtésekor?
- Az érintettek GDPR szerinti jogai.
- A jogalap különböző típusai és használatuk időpontja.
- Hogyan és mikor kell használni a beleegyezést.
- Mi a jogos érdek és mikor nem megfelelő használni.
- A szerződéses és a marketing e-mail közötti különbség.
- Az adatvédelmi nyilatkozat ellenőrzése.

3. MINŐSÉGBIZTOSÍTÁSHOZ KÖTHETŐ ÉVES KÖTELEZŐ KÉPZÉSEK

3.1. Minőségbiztosítás ISO 9001 alapokon

Mire terjed ki a csomag?

- Hogyan javíthatja a minőség a szervezet teljesítményét?
- Mi az ISO 9001, milyen fontos és milyen hatással van a szervezetre?
- Hogyan alkalmazzák a kockázatalapú gondolkodást egy szervezet kontextusában.
- Hogyan alkalmazható a folyamatfejlesztés a megfelelőség biztosítása érdekében?

3.2. ISO 27001:2022 Információbiztonság Irányítási Rendszer

Mire terjed ki a csomag?

- Bevezetés – Tudjon meg többet az információbiztonságról és arról, hogyan illeszkedik be
- Mi az ISO 27001? – Az ISO 27001 szabvány és annak jelentősége az Ön szervezete számára
- Információbiztonság a munkahelyen – Fedezze fel az információbiztonsági kockázatokat a munkakörnyezetben
- Fontos dokumentáció – Ismerje meg szervezete információbiztonsági irányelveit

3.3. Üzletmenet folytonosság a szervezetben az ISO 22301 szabvány alapján

Mire terjed ki a csomag?

- A szervezet működését befolyásoló zavaró események különböző típusai, a példák a széles körben elterjedttől a kisebb, valószínűbb eseményekig terjednek.
- Hogyan sérül egy szervezet, ha nem tudja tovább kínálni termékeit és szolgáltatásait?
- Példák arra, hogy a szervezetek hogyan profitálhatnak abból, ha hatékonyan reagálnak egy zavaró eseményre.
- Hogyan néz ki egy jó gyakorlatú üzletmenet-folytonossági program?
- Hogyan illeszkedik az üzletmenet-folytonosság nemzetközi szabványa (ISO 22301) a programba?
- Mit tehetnek az alkalmazottak a szervezet védelme érdekében a zavaró események előtt, alatt és után?

3.4. Kockázatmanagement rendszer kialakítása és bevezetése a szervezeti kultúrába ISO 31000 alapon

Mire terjed ki a csomag?

- A kockázatkezelés újra értelmezése a szervezetirányítás hatékonyabbá tételére
- A kockázatkezelés integrálása a szervezetirányítás rendszerébe
- Megfelelés-irányítási forgatókönyvek az integrált kockázatkezelés megvalósítására
- Kockázatkezelés irányítása forgatókönyv alkalmazása
- A kockázatkezelésre vonatkozó államháztartási belső kontroll standardok és az iso 31000 szabvány összefüggései
- A folyamatfelmérési szabvány alkalmazása a belső kontrollrendszer folyamatainak kockázatértékelésére

3.5. Munkavédelem és Tűzvédelem az ISO 45001 alapján

Az ISO 45001 azokra a szervezetekre vonatkozik, amelynek célja egy nemzetközileg elismert munkahelyi egészségvédelem és biztonság irányítási rendszer (MEBIR) létrehozása és bevezetése annak érdekében, hogy a legkisebbre csökkentsék a munkatársakat és más érdekelt feleket érő kockázatokat, továbbá, hogy fenntartsák és folyamatosan fejlesszék egészségvédelmi és biztonsági teljesítményüket.

3.6. Környezetirányítási rendszer működtetése a szervezeten belül ISO 14001 alapokon

A fogyasztói életstílusok környezetre gyakorolt hatásával kapcsolatos növekvő globális tudatosság hatására a gyártók és szolgáltatók nyomás alá kerültek, hogy ellátási láncukat környezetbarátabbá tegyék. Azok a szervezetek, amelyek kereskedelmi céljaikat összehangolják a globális ökológiai problémákkal, alapvető

versenyelőnyre tesznek szert. Ez továbbá csökkenti az energia -és anyag fogyasztás, újrafeldolgozás, levegő- és víz kibocsátások költségeit, valamit a jogszabályi nemmegfelelőségekből adódó bírságokat.

A fenntartható gazdálkodás és működés fontos része a jelenért és a jövőnkért való felelősségünk. Az ISO 14001 szabvány 1996 óta képezi környezetközpontú irányítási rendszerek felépítésének, bevezetésének, felügyeletének és továbbfejlesztésének az alapját. A szabvány megfelelő követelményeket határoz meg, amelyek bármilyen jellegű és méretű szervezetre, valamint különböző földrajzi, kulturális és társadalmi feltételek mellett is alkalmazhatóak. A szabványkövetelmények alapvető célja, hogy a környezetvédelmet és a környezetszennyezések megelőzését összhangba hozza a gazdasági, szociális és jogszabályi követelményekkel.

4. ÁRAZÁS

Oktatés neve	Oktatási anyag hossza	Ár / felhasználó / Év	Felhasználó független LMS-SCROM Package
2.1 NIS2 Oktatási csomag	45-50 perc	54 EUR / felhasználó / Év	9700 EUR
2.2. Információbiztonsági és kiberbiztonsági tudatossági e-learning tanfolyam	45 -55 perc	28 EUR / felhasználó / Év	5000 EUR
2.3. Otthoni munkavégzés (Home Office) kiberbiztonsági tanfolyam	45 -55 perc	21 EUR / felhasználó / Év	3700 EUR
2.4. Védekezés Ransomware támadások ellen	45 -55 perc	23 EUR / felhasználó / Év	4100 EUR
2.5. Adathalász támadások veszélyei	45 -55 perc	23 EUR / felhasználó / Év	4100 EUR
2.6. Adatvédelmi tudatosság (GDPR, 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról) növelése e-learning tanfolyam	45 -55 perc	28 EUR / felhasználó / Év	5000 EUR
2.7. GDPR és Információbiztonság a HR számára	45 -55 perc	25 EUR / felhasználó / Év	4500 EUR
2.8. GDPR és Információbiztonság a Marketing terület számára	45 -55 perc	25 EUR / felhasználó / Év	4500 EUR
3.1. Minőségbiztosítás ISO 9001 alapokon	120-130 perc	40 EUR / felhasználó / Év	7200 EUR

3.2. ISO 27001:2022 Információbiztonság Irányítási Rendszer	120-130 perc	40 EUR / felhasználó / Év	7200 EUR
3.3. Üzletmenet folytonosság a szervezetben az ISO 22301 szabvány alapján	120-130 perc	40 EUR / felhasználó / Év	7200 EUR
3.4. Kockázatmanagement rendszer kialakítása és bevezetése a szervezeti kultúrába ISO 31000 alapon	120-130 perc	40 EUR / felhasználó / Év	7200 EUR
3.5. Munkavédelem és Tűzvédelem az ISO 45001 alapján	120-130 perc	40 EUR / felhasználó / Év	7200 EUR
3.6. Környezetirányítási rendszer működtetése a szervezeten belül ISO 14001 alapokon	120-130 perc	35 EUR / felhasználó / Év	6300 EUR

Áraink nettó árak. Nem tartalmazzák az Általános Forgalmi Adót!

Felhasználó független LMS-SCROM Csomagjaink felhasználói szám függetlenek. Ezeket a Csomagokat 180 fő feletti szervezeteknek ajánljuk.

Felhasználói éves előfizetői csomagjaink 50-180 fő közötti szervezeteknek javasolt, ezek az árak MINIMUM 50 fő esetén érvényesek.

Egyedi oktatási tematika és e-learning anyag (45-55 perc) kidolgozása 10 munkanap. Ezt a csomagot minden esetben egyénre szabottan készítjük el 4600 EUR értékben, LMS SCROM csomagban.

Meglévő oktatási csomag cégre szabása +20% / felhasználó / Fő, vagy SCROM csomag esetén: Csomagár +10%

5. FIZETÉSI FELTÉTELEK

Fizetési kötelezettségeinek a Megrendelő a Szolgáltató OTP Bank NYRT BPR. IBAN: HU56 1176 3134 4474 9880 0000 0000 EUR folyószámlájára, a kiküldött számla dátumától számított 30 napon belül történő átutalással tesz eleget.

Megrendelés esetén lehetőség van HUF alapú számlázásra is, ez esetben a mindenkori MNB középárfolyamon kerül kiszámlázásra az összeg.

Amennyiben az Ajánlatkérő fizetési kötelezettségét ezen határidőn túl teljesíti, a Ptk. 6:155. § (1) szerinti késedelmi kamatot köteles megfizetni.

Kérdése esetén keressen minket bizalommal.

2024.03.28 Budapest

Megrendelési adatok				
Oktatás neve	*Ár / Felhasználó / év (minimum 50 felhasználó)*	*Ár / Felhasználó / év*	*Felhasználó független LMS-SCROM Csomag*	*Megrendelt csomag mennyiség*
2.1. NIS2 Magyar oktatási csomag (Tartalmazza a kötelező elemeken felül az Üzletmenet folytonossági és kockázatkezelési keretrendszerek oktatásait is cégre szabva)		54 EUR / felhasználó / Év	9700 EUR	
2.2. Információbiztonsági és kiberbiztonsági tudatossági e-learning tanfolyam		28 EUR / felhasználó / Év	5000 EUR	
2.3. Otthoni munkavégzés (Home Office) kiberbiztonsági tanfolyam		21 EUR / felhasználó / Év	3700 EUR	
2.4. Védekezés Ransomware támadások ellen		23 EUR / felhasználó / Év	4100 EUR	
2.5. Adathalász támadások veszélyei		23 EUR / felhasználó / Év	4100 EUR	
2.6. Adatvédelmi tudatosság (GDPR, 2011. évi CXII. törvény) növelése e-learning tanfolyam		28 EUR / felhasználó / Év	5000 EUR	
2.7. GDPR és Információbiztonság a HR számára		25 EUR / felhasználó / Év	4500 EUR	
2.8. GDPR és Információbiztonság a Marketing terület számára		25 EUR / felhasználó / Év	4500 EUR	
3.1. Minőségbiztosítás ISO 9001 alapokon		40 EUR / felhasználó / Év	7200 EUR	
3.2. ISO 27001:2022 Információbiztonság Irányítási Rendszer		40 EUR / felhasználó / Év	7200 EUR	
3.3. Üzletmenet folytonosság a szervezetben az ISO 22301 szabvány alapján		40 EUR / felhasználó / Év	7200 EUR	
3.4. Kockázatmanagement rendszer kialakítása és bevezetése a szervezeti kultúrába ISO 31000 alapon		40 EUR / felhasználó / Év	7200 EUR	
3.5. Munkavédelem és Tűzvédelem az ISO 45001 alapján		40 EUR / felhasználó / Év	7200 EUR	
3.6. Környezetirányítási rendszer működtetése a szervezeten belül ISO 14001 alapokon		35 EUR / felhasználó / Év	6300 EUR	
Összesen felhasználó		*Összesen SCROM Csomag*		

Kapcsolattartási adatok	
Vezeték és keresztnév név*:	
Telefonszám (mobil):	
E-mail cím*:	

Számlázási adatok	
Számlázási név (kérjük pontosan kitölteni) *:	
Számlázási cím*:	
Számlázási e-mail cím *:	
Adószám (cég esetén) *:	
Dátum:	**Cégszerű aláírás:**
	Megrendelő neve: