

# Bezpečnostní povědomí zaměstnance - vstupní proškolení

Kód kurzu: BPZ-A

Dvoudenní kurz školí běžné zaměstnance a uživatele na podnikovou bezpečnost informací a ochranu osobních údajů (INFOSEC, ISMS, GDPR), její požadavky a zodpovědnost pracovníků samotných. Kurz je zakončen testem, po jehož úspěšném složení získá účastník osvědčení o způsobilosti. Jedná se o prvotní dvoudenní proškolení. Později je již možné opakovaně navštěvovat jen jednodenní osvěžující kurz BPZ-B.

## Pro koho je kurz určen

Kurz je určen všem uživatelům informačních technologií, zejména zaměstnancům organizací, které si hledí bezpečnosti informací (InfoSec, ISMS) a nebo jsou správci, nebo zpracovateli osobních údajů (GDPR)

## Co vás na kurzu naučíme

Porozumět důvodům a důležitosti ochrany informací v organizaci

Pochopit co jsou a co naopak nejsou osobní údaje a jak se k nim chovat

Být schopen přijmout vlastní zodpovědnost za svoje chování při nakládání s citlivými podnikovými a osobními údaji

Vědět jak si správně zvolit a chránit hesla a jiné přihlašovací údaje

Chápat na co je třeba šifrování, k čemu se využívá a jak si zkontrolovat, že se opravdu šifruje

Jaká jsou rizika při přístupu k podnikovým informacím z mobilních zařízení, z internetu obecně a jak to dělat bezpečně

Co znamená fyzická bezpečnost a jak je nebezpečné nechávat počítačové vybavení bez dozoru

Jaké existují technická bezpečnostní opatření a jaká je nebo není jejich schopnost zamezit útokům a ztrátě dat

Vidět některé útoky na vlastní oči a pochopit jak to může být jednoduché, pokud si člověk nedává pozor

## Zkouška způsobilosti

Na konci kurzu probíhá 30 minutový test

Odpovědi na otázky účastníci vyplňují do elektronického testovacího systému, který také výsledek okamžitě vyhodnotí

Odpovědi na otázky se vybírají z několika možných, každá otázka může mít více správných odpovědí, které je v takovém případě potřeba zvolit všechny (multi-select)

K testu nesmí mít účastníci po ruce nic, nejsou dovoleny ani mobilní telefony, tužky ani poznámkové bloky, připojení k internetu je odpojeno, nejsou dovolena ani jiná "chytrá" zařízení jako hodinky apod.

Jakákoliv spolupráce testovaných je zakázána, v průběhu testu není možné opouštět testovací místnost

Úspěšné ukončení zkoušky je při dosažení alespoň 70% správných odpovědí

Při úspěšném složení zkoušky obdrží účastník osvědčení o způsobilosti k práci s informacemi v zabezpečeném prostředí

Osvědčení o způsobilosti se vydává na dobu neurčitou, ale obsahuje výrazně uvedné datum jeho získání a postupem času tedy přirozeně ztrácí na aktuálnosti

## Osnova kurzu

Důležitost informační bezpečnosti pro fungování organizace (ISMS, InfoSec)

Zákonné požadavky na ochranu osobních údajů (GDPR)

Co jsou osobní údaje, jak se k nim chovat a na co nezapomenout

Na co si dát pozor při zveřejňování osobních údajů na sociálních sítích

Uživatelská jména a hesla pro přihlašování do podnikové počítačové sítě

Zásady pro správnou volbu délky a vlastností hesla

### GOPAS Praha

Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved

# Bezpečnostní povědomí zaměstnance - vstupní proškolení

Co je a proč se používá více-faktorové přihlašování do počítačů a mobilních zařízení

Jak chránit přihlašovací údaje proti útokům jako je keylogger

Ukládat nebo raději neukládat hesla na počítačích?

Šifrované komunikace jako například HTTPS a jak se o tom ujistit

Zásady bezpečného připojování k firemní poště a vnitřním webům z mobilních zařízení

Odkud se mohou připojovat a odkud naopak nesmím

Šifrovaná a nešifrovaná WiFi, bezpečné VPN připojení, připojení na vzdálenou plochu

Šifrování disků a mobilních zařízení jako ochrana proti fyzickému útoku na počítače

Opatrnost při ústním a papírovém sdílení informací

Proč fyzická bezpečnost, vstupy s kartou a visačkou, hlášení incidentů a ztráty, nebo krádeže

Jak rozeznat phishing a jak si dávat pozor na spouštění nebezpečných příloh

Co jsou zero-day útoky, ransomware a (ne)schopnost antiviru nákazu odhalit a zablokovat

## **GOPAS Praha**

Kodaňská 1441/46  
101 00 Praha 10  
Tel.: +420 234 064 900-3  
[info@gopas.cz](mailto:info@gopas.cz)

## **GOPAS Brno**

Nové sady 996/25  
602 00 Brno  
Tel.: +420 542 422 111  
[info@gopas.cz](mailto:info@gopas.cz)

## **GOPAS Bratislava**

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 248 282 701-2  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2020 GOPAS, a.s.,  
All rights reserved