Bezpečnostní povědomí zaměstnance - pravidelné přezkoušení

Kód kurzu: BPZ-B

Jednodenní opakovací kurz a přezkoušení zaměstnanců a běžných uživatelů ze základů a vlastních povinností při práci s informacemi a osobními údaji v zabezpečeném prostředí (InfoSec, ISMS, GDPR). Kurz pouze opakuje problematiku a na jeho konci probíhá přezkoušení, při jehož úspěšném složení obdrží účastník osvědčení o způsobilosti. Kurz není možné navštívit bez předchozí účasti na kurzu BPZ-A, který problematiku plnohodnotně vysvětluje, zatímco zde se jedná jen o bleskové zopakování před následnou zkouškou.

Pro koho je kurz určen

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

Co vás na kurzu naučíme

Zopakujete si všechna témata z kurzu a zkoušky BPZ-A tak, abyste ji dokázali složit znovu

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

Obsah kurzu je stejný, jako BPZ-A s tím rozdílem, že se jedná pouze o zrychlené zopakování s cílem znovu úspěšně složit zkoušku

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

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

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

Bezpečnostní povědomí zaměstnance - pravidelné přezkoušení

Odkud se mohu 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
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved