Životní cyklus zaměstnance

a role IT správce

Digital Security
Progress. Protected.

Cesta každého zaměstnance v organizaci zahrnuje různé fáze, od nástupu přes každodenní práci až po případný odchod, přičemž každá z nich má své jedinečné požadavky na IT. Pro zajištění bezproblémového a bezpečného chodu společnosti je nezbytné, aby byl IT tým dobře připraven na každý krok této cesty.

Máte pro každou fázi jasný plán? Jste si jisti, že vaše IT procesy odpovídají osvědčeným postupům? Tento checklist byl vytvořen s cílem provést IT specialisty různými fázemi pracovního života zaměstnanců, pomoci jim efektivně plnit jejich povinnosti a chránit digitální prostředí organizace.

Jak tento checklist používat?

Checklist činností při nástupu a odchodu zaměstnance je výchozím bodem pro udržení bezpečnosti a efektivity digitální infrastruktury vaší organizace.

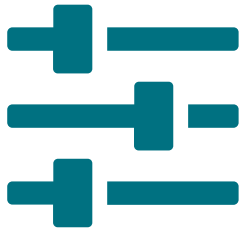
Pro snadné použití si ho můžete vytisknout nebo uložit a používat v digitální podobě.

Seznam vám pomůže zvážit všechny nezbytné kroky pro každou fázi životního cyklu zaměstnance. Můžete se k němu pravidelně vracet a ověřovat si, jestli jste nezapomněli na něco podstatného.

Při nástupu

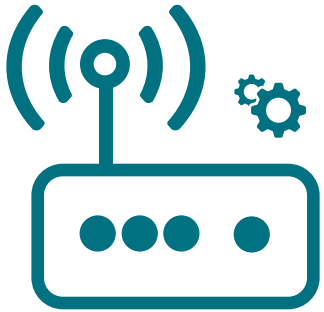
Digital Security
Progress. Protected.

1. Příprava zařízení pro nové zaměstnance:



- Přiřaďte zaměstnancům odpovídající hardware a důkladně ho označte.
- Připravte veškeré potřebné příslušenství, včetně monitorů, dokovacích stanic, klávesnic a myší.
- Nastavte daná zařízení pro nové zaměstnance. To může zahrnovat:
  - ☐ Instalaci a zajištění veškerého potřebného hardwaru a softwaru.
  - ☐ Konfiguraci e-mailových účtů a přístupových oprávnění.
  - ☐ Nastavení bezpečnostních opatření a uživatelských profilů.
  - ☐ Přizpůsobení zařízení tak, aby odpovídalo roli a požadavkům uživatele.

2. Předání zařízení:



- Pomozte novým zaměstnancům s prvním přihlášením.
- Pomozte zaměstnancům nastavit jejich hesla.
- Proveďte s uživatelem kontrolu zařízení, abyste se ujistili, že vše funguje správně.
- Poskytněte uživatelům základní instrukce týkající se zabezpečení, nastavení Wi-Fi apod.
- Zajistěte, aby nový zaměstnanec podepsal předávací protokol.

3. Směrnice a postupy:

- Sdílejte s novými zaměstnanci seznam směrnic a postupů pro práci se softwarem, který budou používat.
- Seznamte zaměstnance s různými firemními předpisy, mezi které mohou patřit:
  - ☐ IT/bezpečnostní směrnice
  - ☐ Zásady ochrany dat
  - ☐ Zásady práce na dálku
  - ☐ Zásady pro práci se sociálními médii
  - ☐ Pravidla pro BYOD (Bring Your Own Device)

Pravidla pro BYOD (Bring Your Own Device)

BYOD neboli práce na soukromém zařízení je v dnešní době poměrně populární, což znamená, že je nutné poučit zaměstnance o používání jejich zařízení pro osobní i pracovní účely, aniž by byla ohrožena bezpečnost vaší společnosti. Co by měly obsahovat zásady pro BYOD?

- ☐ **Kdo je oprávněný využívat své soukromé zařízení pro práci**
- ☐ **Seznam zařízení, operačních systémů a platforem, které jsou v rámci pravidel povoleny a podporovány**
- ☐ **Požadavky na hesla**
- ☐ **Požadavky na šifrování dat**
- ☐ **Vysvětlení procesu vzdáleného výmazu**
- ☐ **Omezení přístupu k datům a jejich používání**
- ☐ **Objasnění úrovně IT podpory poskytované pro osobní zařízení**
- ☐ **Specifika monitorování a auditu**
- ☐ **Odpovědnosti zaměstnanců z hlediska bezpečnosti a dodržování předpisů**
- ☐ **Co dělat při ukončení pracovního poměru**

V průběhu zaměstnání

Digital Security
Progress. Protected.

1. Vzdělávání v oblasti kybernetické bezpečnosti:

- Průběžně vzdělávejte zaměstnance v oblasti kybernetických hrozeb a bezpečnostních best practices.

Jak tvořit kyberbezpečnostní kulturu a vyhnout se únavě z bezpečnosti?

- ☐ Spolupracujte s personálním oddělením, aby bylo vzdělávání interaktivní a užitečné.
- ☐ Realizujte kratší a častější školení, která jsou často účinnější než jedno roční školení.
- ☐ Sdílejte reálné příběhy a příklady ze své praxe, aby byl obsah srozumitelný.
- ☐ Využívejte zábavné formáty - například hry, kvízy a simulace.
- ☐ Nestrašte zaměstnance. Jinak se budou spíše bát nahlásit jakékoli chyby nebo potenciální kybernetické hrozby.
- ☐ Buďte otevření otázkám a ujistěte zaměstnance, že jste jim k dispozici, pokud vás budou potřebovat.

2. Dodržování principu nejnižších privilegií:

- Zajistěte dodržování principu nejnižších privilegií.
- Pravidelně kontrolujte a odpovídajícím způsobem upravujte přístupová oprávnění.
- Vytvořte a vynucujte pravidla pro sdílení souborů a přeposílání e-mailů na externí adresy, abyste zabránili úniku dat.

3. Údržba zařízení:

- Pravidelně ověřujte, zda zařízení zaměstnanců obsahují nejnovější bezpečnostní záplaty a aktualizace softwaru. To se týká jak firemních, tak osobních zařízení používaných k práci.

4. Pravidla pro vzdálenou práci:

- Pokud se vaše společnost neřídí systémem BYOD, zakažte používání osobních zařízení k pracovním úkolům.
- Vynucujte používání virtuální privátní sítě (VPN) pro bezpečné připojení.
- Vyžadujte používání šifrování pro citlivá data.
- Zdůrazněte význam silných hesel pro Wi-Fi, která zabrání neoprávněnému přístupu.
- Zajistěte, aby ochrana koncových bodů byla aktivní a aktuální na všech vzdálených zařízeních.

Při odchodu

Digital Security
Progress. Protected.

1. Správa účtů a přístupů:

- Zrušte oprávnění pro všechny aplikace a služby, ke kterým měl odcházející zaměstnanec přístup.
- Resetujte hesla na všech firemních zařízeních, která zaměstnanec používal.

2. Fyzický přístup a hardware:

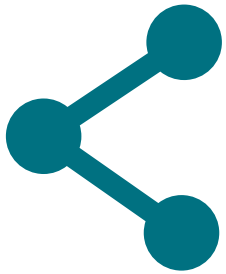
- Odeberte přístup do budovy, včetně přístupových karet a klíčů.
- Shromažděte a převeďte zpět všechna firemní zařízení vydaná odcházejícímu zaměstnanci, včetně notebooků, chytrých telefonů a dalšího hardwaru.

3. Sledování a ochrana dat:

- Udržujte pravidelnou komunikaci s odcházejícím zaměstnancem a sledujte jeho chování během procesu odchodu.
- Proveďte závěrečnou kontrolu monitorovacích a logovacích nástrojů, abyste zjistili, zda nedošlo k neobvyklým nebo neoprávněným aktivitám spojeným s účty a systémy odcházejícího zaměstnancem.
- Zvažte nasazení řešení prevence ztráty dat (DLP), abyste odhalili neoprávněný přístup k zařízením nebo datům během nástupu nebo po něm.

4. Poslední den zaměstnance:

- Ujistěte se, že bylo dokončeno předání hardwaru.
- Zablokujte účty zaměstnance, abyste zabránili neoprávněnému přístupu.
- Proveďte bezpečné vymazání zařízení zaměstnance, abyste odstranili firemní data.



O společnosti ESET

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky připravuje podcast True Positive.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Digital Security
Progress. Protected.