SMĚRNICE: POLITIKA BEZPEČNOSTI INFORMACÍ- VEŘEJNOST

Date Issued 22.11.2022
Revised: 1.12.2023
Authorization: Board of Directors
Next Review: 09.2023

Verze dokumentu

Verze	Autor	Změna	Popis změny
1.0		15.09.2022	Vytvoření dokumentu
1.1		22.11.2022	Revize dokumentu
1.2	Kment	19.10.2023	Revize dokumentu
1.3	Kment	1.12.2023	Revize dokumentu

Politika bezpečnosti informací

Cílem je zajistit důvěrnost, dostupnost a integritu všech vlastních i zákaznických dat informací pro úspěšné zajištění našich podnikatelských aktivit.

1. K prosazení této politiky jsou ve společnosti Palasino Group, a.s., jako neoddělitelná součást řízení, zavedeny bezpečnostní předpisy dle standardu ISMS - systém řízení bezpečnosti informací podle ČSN ISO/IEC 27001.

2. Dostupnost a integritu informací (informace nepoškozené, nepozměněné, úplné atd.) v čase a místě dle podnikatelských potřeb společnosti, pouze těm, kteří je potřebují pro svoji pracovní činnost, čímž je zachovávána důvěrnost informací dle stanovené klasifikace informací (veřejné, interní, chráněné).

3. Řízení celého životního cyklu informací, tzn. jejich zpracování od okamžiku získání nebo vytvoření až po jejich likvidaci.

4. Přijímání bezpečnostních opatření přímo úměrných aktuální míře rizik spojených s ohrožením bezpečnosti informací.

5. Pravidelným monitorováním, hodnocením rizik, řízením bezpečnostních incidentů, nápravnými a preventivními opatřeními budeme zvyšovat účinnost řízení bezpečnosti informací.

6. Politika bezpečnosti informací je závazná pro všechny zaměstnance a zainteresované subjekty.

7. Zaměstnanci jsou soustavně vzděláváni a školeni v oblasti bezpečnosti informací.

Tato politika je platná od 19.10.2023

8. Externí subjekty jsou smluvně zavázány k dodržování interních předpisů společnosti Palasino Group, a.s. .

9. Porušení pravidel bezpečnosti informací je považováno za závažné porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci a je předmětem disciplinárního řízení.

10. Každý zaměstnanec a externí pracovník má možnost ohlásit jakékoliv nesrovnalosti s touto politikou přímo svému vedoucímu nebo prostřednictvím emailu na adresu ISO@palasino.eu

Desatero informační bezpečnosti nastavené ve společnosti:

1. Mám bezpečné heslo a chráním si jej a nikdy nesděluji.
2. Dodržuji zásady fyzické ochrany svého počítače (notebooku) a dalších zařízení.
3. Chráněná data neposílám bez použití nastavených pravidel v Uživatelské příručce
4. Neporušuji autorská práva, nepoužívám nelegální software.
5. Nenavštěvuji zakázané a potenciálně nebezpečné weby.
6. Oprávnění pro přístup k datům ve sdílené složce na SharePoint či OneDrive určuje zodpovědný uživatel, který je tam nahrál.
7. Neotvírat přílohy v emailech od neznámých odesílatelů, použít email-alert@palasino.eu.
8. Kontrolovat hypertextové odkazy v emailech před otevřením.
9. Papírové dokumenty chráním s ohledem na jejich klasifikaci (chráněné).
10. V případě nestandardní události použiji Helpdesk případně hlásím incident na ISO@palasino.eu.

Revizi této politiky provádí vedení společnosti každoročně, poslední revize ze dne 19.10.2023.

11. Závazek vedení a managementu

Vedení a management společnosti deklaruje závazek za podporu finančních a lidských zdrojů pro plnění nastaveného systému ISMS ve společnosti Palasino Group, a.s.. Pro následující roky bude podporovat krytí finančních a lidských zdrojů pro plnění nastavené politiky.

Revizi této politiky provádí vedení společnosti každoročně, poslední revize ze dne 19.10.2023.

Ing.Tomáš Kment
IT Security Manager, member of BoD

Tato politika je platná od 19.10.2023