Pravidla kybernetické a informační bezpečnosti pro externisty

GasNet, s.r.o.

středa, říjen 27, 2021

Verze 1.0

Úvod

Tento dokument „Pravidla kybernetické a informační bezpečnosti pro externisty“ stanovuje 10 pravidel práce ve společnosti GasNet, s.r.o.

I. Fyzická bezpečnost

Identifikační karta slouží k vstupu do prostor společnosti.

II. Pravidlo čistého stolu a čisté obrazovky

Při opuštění pracovního místa odstraňte všechny tištěné dokumenty z pracovního stolu a uzamkněte je do míst k tomu určených tak, aby nebyly volně přístupné dalším osobám. Při ukončení práce s IT zařízením (pracovní stanice, notebook, tablet, mobilní telefon apod.) uzamkněte obrazovku zařízení tak, aby bylo nutné opětovné přihlášení pomocí hesla nebo PINu.

III. Klasifikace informací

Klasifikace informací pomáhá určit, s jak důležitými informacemi externisté pracují. Ve společnosti rozlišujeme čtyři stupně klasifikace informací: veřejné, interní, citlivé a strategické. Uživatel se MUSÍ řídit klasifikací informací ve společnosti.

IV. Hesla

Uživatel MUSÍ chránit hesla k informačním systémům a aplikacím. Hesla jsou nepřenosná a není povoleno je sdílet. Pro pracovní účely uživatelů NESMÍ používat stejná hesla, která používají pro své soukromé účely. Iniciální hesla MUSÍ být změněna při prvním přihlášení. Minimální délka hesla je stanovena na 12 znaků. Doba platnosti hesla je 18 měsíců. Heslo musí obsahovat malá a velká písmena, a k nim buď číslice, nebo speciální znaky. Uživatel MŮŽE používat trezory hesel pro uchovávání svých hesel. Uživatel BY MĚL využívat vícefaktorovou autentizaci všude tam, kde je to možné. Hesla odpovídají klasifikačnímu stupni „strategická“.

V. Bezpečnost dat a informací

Uživatel NESMÍ přistupovat k datům, ke kterým nemá oprávnění. Při neoprávněném přístupu k datům nebo informacím ihned kontaktujte úvar Security. Uživatel MUSÍ dbát zvýšené opatrnosti při nakládání s osobními údaji.

VI. Zálohování dat

Uživatel BY MĚL ukládat svá data na centrální místa nabízená v rámci společnosti (SharePoint, ShareDir atd.). Veškerá uživatelská data mimo centrální úložiště MUSÍ být zálohována uživatelem.

VII. Přenosná média pro přenos dat

Uživatel NESMÍ ponechat média pro přenos dat bez dozoru. Taková zařízení se ukládají výhradně v uzamčených prostorách k tomu určených. Uživatel NESMÍ předávat datová média neoprávněným příjemcům. Informace klasifikované stupněm „citlivé“ a „strategické“ mohou být předávány na přenosných médiích výhradně v zašifrované podobě.

VIII. Ochrana proti škodlivému softwaru

Uživatel MUSÍ mít na svém zařízení nainstalován standardní bezpečnostní software (minimálně antivir a firewall). Uživatel NESMÍ upravovat ani vypínat nastavení bezpečnostních aplikací.

IX. Použití internetu a elektronické pošty

Uživatel BY MĚL využívat internet jen v souvislosti s plněním pracovních povinností. Pouze poskytovatel IT služeb BY MĚL měnit nastavení softwaru pro prohlížení internetu. Uživatel MUSÍ využívat pro plnění pracovních povinností výhradně pracovní email. Informace zasílané emailem klasifikované jako „citlivé“ a „strategické“ MUSÍ být zašifrovány. Pro případ, kdy musí být identita odesílatele nepopiratelná, uživatel MUSÍ zprávu digitálně podepsat.

X. Hlášení bezpečnostních incidentů

Uživatel MUSÍ bezpečnostní incidenty nebo i podezření na bezpečnostní incidenty hlásit neprodleně v aplikaci Service Desk.

Přílohy

Klasifikace informací ve společnosti

Klasifikační stupeň	**Definice**	**Příklady**
Veřejné	Informace určené pro zveřejnění.	• Marketingové materiály • Nabídka a ceník služeb • Tisková prohlášení • Veřejné nabídky zaměstnání
Interní	Informace týkající se společnosti, s velmi malým dopadem při neoprávněném použití.	• Všechny materiály společnosti, které nejsou předmětem jiné klasifikace • Poznámka: S neoznačeným dokumentem vždy zacházejte tak, že patří do kategorie „Interní“
Citlivé	Zásadní dopad na společnost nebo přerušení důležitých činností.	• Informace o produktech před uvedením na trh • Informace o zamýšlených nákupech nebo prodejích společností • Podmínky smluv vysoké hodnoty • Zákaznická data • Zaměstnanecká data • Zápisy z jednání vedení společnosti
Strategické	Největší dopad na společnost nebo přerušení důležitých činností, ztráta konkurenční výhody, ztráta tržního podílu, ztráta dobrého jména.	• Plány akvizic • Strategie top managementu • Výroční zpráva před zveřejněním