Bezpečnost informací ve společnostech Zentity

1. Společnosti mají sestaveny bezpečnostní politiky, které definují pravidla pro jednotlivé aspekty systému managementu bezpečnosti informací a jsou platné jak pro zaměstnance, tak i pro externí subjekty. Jsou k dispozici na firemním intranetu a nebo na vyžádání.
2. Podezření na porušení bezpečnosti informací nebo objevení zranitelnosti systému je každý povinen hlásit **bezpečnostnímu týmu** společností a to na emailové adrese **security@zentity.com.**
3. Informace zpracovávané společnostmi jsou označovány dle pravidel stanovených v politice klasifikace a označování informací. Jednotlivé úrovně klasifikačního schématu jsou:

   C1 - Veřejné: Informace, které společnosti sdílí s veřejností

   C2 - Vyhrazené: Informace vyhrazené pracovníkům společností nebo vybrané skupině osob

   C3 - Důvěrné: Citlivé nebo klíčové informace dostupné pouze úzké skupině osob

   C4 - Tajné: Strategické informace určené zejména vedení společností
4. Při nakládání s informacemi je nutné řídit se odpovídajícími politikami, zejména pak politikou manipulace s aktivy. Přístup k informacím v elektronické i fyzické podobě je řízen v souladu s politikou přístupu. Je zakázáno sdílet informace úrovně C3 nebo C4 s neautorizovanými osobami a to včetně přeposílání elektronických zpráv.
5. Hesla přístupových účtů a nakládání s nimi musí být v souladu s politikou hesel. Je zakázáno sdělovat hesla k účtům neautorizovaným osobám nebo je ukládat a sdílet v nezabezpečené podobě.
6. Společnosti dbají na dodržování platných legislativních předpisů v oblasti bezpečnosti informací, včetně ochrany osobních údajů a práv duševního vlastnictví.
7. Vybavení pro zpracování informací je chráněno a pravidelně servisováno, aby odpovídalo bezpečnostním požadavkům. Softwarové vybavení je používáno v souladu s licenčními podmínkami dodavatelů a je pravidelně aktualizováno, včetně aplikace všech dostupných bezpečnostních záplat. Společnosti také pravidelně monitorují veškeré zranitelnosti používaných informačních systémů.
8. Interní síť a síťové služby jsou zabezpečeny před neoprávněným přístupem pomocí vhodných bezpečnostních prvků. Pro přenos informací jsou využívány pouze bezpečné komunikační kanály a jsou využívány kryptografické techniky.
9. Bezpečnost informací je řešena také v rámci dodavatelských vztahů. Požadavky na bezpečnosti informací jsou v potřebné míře přenášeny na dodavatele a komunikovány s nimi.
10. Softwarové produkty ZENTITY splňují vysokou úroveň bezpečnostních standardů a dalších opatření vyžadovaných normou **ISO/IEC 27001**. Jsou také pravidelně kontrolovány a testovány z pohledu bezpečnosti a kvality.