NÁZEV:	SMĚRNICE POLITIKA INFORMAČNÍ BEZPEČNOSTI

	Jméno, pracovní pozice:	Podpis:
Zpracoval:	Mgr. et Mgr. Radek Holub, manažer pro ochranu majetku a osob	
Schválil:	Petr Rybníček, MBA, generální ředitel	

Úložiště dokumentu v elektronické podobě: ownCloud SHERLOG Technology, a.s.
Úložiště dokumentu v originální podobě: sekretariát společnosti, bezpečnostní úsek

1. Účel a působnost:

Tato směrnice stanovuje zásady, organizační rámec a bezpečnostní opatření v oblasti kybernetické bezpečnosti ve společnosti SHERLOG Technology, a.s., IČO: 471 15 467, se sídlem Praha 1, Staré Město, Revoluční 767/25, PSČ 110 00, sp. zn.: B 1753 vedená u Městského soudu v Praze a jejích dceřiných společnostech (dále Společnost) s cílem chránit informační aktiva Společnosti, zajistit kontinuitu podnikání, plnit legislativní požadavky, přičemž Společnost, v souladu s výstupy externě zpracované analýzy a vlastní analýzy, prohlašuje, že se nezabývá dlouhodobou správou technických aktiv zákazníků, jejím provozem, monitoringem, údržbou nebo samotnou podporou.

Cílem Směrnice je:

- Zajistit důvěrnost, integritu a dostupnost informací.
- Minimalizovat rizika ztráty dat, zneužití, neoprávněného přístupu a výpadků.
- Naplnit zákonné požadavky dle zákona č. 264/2025 Sb., Zákon o kybernetické bezpečnosti ve znění pozdějších změn.
- Reagovat na aktuální změny v rámci regulace, dle prováděcí směrnice NIS2.

Právní rámec:

- Zákon č. 264/2025 Sb., Zákon o kybernetické bezpečnosti.
- Vyhlášky č. 208/2025 Sb., 409/2025 Sb. a 410/2025 Sb. 82/2018 Sb. o regulovaných službách
- Směrnice Evropského parlamentu a Rady o kybernetické bezpečnosti (NIS2).
- Nařízení (EU) 2016/679 (GDPR).
- Interní předpisy společnosti SHERLOG Technology, a.s.

Směrnice se vztahuje na všechny zaměstnance, externí spolupracovníky i dodavatele využívající nebo spravující informační systémy.

2. Definice a vymezení pojmů:

- Informační systém (IS) – systém pro zpracování informací, který obsahuje software, hardware, data a procesy;
- ISMS – systém řízení bezpečnosti informací;
- Aktivum – jakýkoli prvek (hardware, software, data), který má pro Společnost hodnotu;
- Hrozba – potenciální příčina nežádoucí události, schopná poškodit IS;
- Zranitelnost – slabina systému, kterou může hrozba zneužít;

- Kybernetický bezpečnostní incident:
  – událost, která ohrožuje dostupnost, důvěrnost, integritu nebo autenticitu informací nebo systémů.
- Bezpečnostní opatření:
  – soubor organizačních a technických prostředků sloužících k ochraně aktiv.

3. Minimální požadavky na ochranu IS a odpovědnost:

Představenstvo:
- Zajišťuje strategické řízení bezpečnosti informací.
- Schvaluje Směrnici a její aktualizace.
- Přijímá rozhodnutí na základě výstupů z auditů, analýz rizik a hlášení incidentů.

Manažer kybernetické bezpečnosti:
- Zavádí a spravuje ISMS.
- Koordinuje klasifikaci aktiv a analýzu rizik.
- Zajišťuje školení a testování zaměstnanců.
- Vyšetřuje incidenty, navrhuje nápravná opatření.
- Komunikuje s externími autoritami.

IT oddělení / Správce systémů:
- Realizuje technická bezpečnostní opatření.
- Správa přístupových práv, logování, obnova dat, aktualizace a zálohování systémů.

Zaměstnanci:
- Používají jen přidělené účty, hlásí incidenty.
- Dodržují směrnici, účastní se školení.

Dodavatelé:
- Dodržují bezpečnostní pravidla, podepisují doložky smluv o bezpečnostních opatřeních uvedených v této Směrnici, jakožto i dalších interních předpisech vztahujících se ke kybernetické bezpečnosti, popř. GDPR

4. Klasifikace a ochrana aktiv:

Třídy informací - aktiv:

Klasifikace přístupu	Aktiva	Režim přístupu
Veřejná	webová prezentace	volně přístupná
Interní	vnitropodniková směrnice	Ochrana před neoprávněným zveřejněním
Důvěrná	klientská data	šifrování, omezený přístup
Přísně důvěrná	vývojová data, kniha jízd, registr smluv, uživatelská data, systém PLAZ, přístupové klíče, hesla, kvalifikované certifikáty aj. vysoce důvěrná data.	silná ochrana, vybraný přístup

Každé aktivum je klasifikováno dle důvěrnosti, integrity a dostupnosti. Rizika jsou vyhodnocována nejméně 1× ročně a po každé zásadní změně v infrastruktuře. Přijatá opatření jsou dokumentována a přezkoumávána. Každé aktivum má stanoveného vlastníka a způsob ochrany.

5. Řízení přístupů:

- Více faktorová autentizace pro kritické systémy.
- Hesla: min. 8 znaků, změna každých 180 dní.
- Uzamykání obrazovky při nepřítomnosti.
- Kontrola oprávnění 1× ročně nebo při změně pozice.
- viz Směrnice pro využívání IT.

6. Řízení rizik:

Postup řízení rizik:

1) Identifikace aktiv.
2) Vyhodnocení hrozeb a zranitelností.
3) Stanovení rizik (dopad × pravděpodobnost).
4) Výběr a zavedení opatření.
5) Revize 1× ročně.

7. Fyzická a provozní bezpečnost:

- Serverovny – vícestupňová elektromechanická ochrana kombinovaná s fyzickou ostrahou 24/7.
- Zálohování: stanoveno podle klasifikace, nejméně na denní bázi + týdenní.
- Ochrana: klimatizace, UPS.
- Roční inventura HW/SW.
- Další podrobnosti jsou upraveny v dalších interních předpisech pro IT, management a zaměstnance.

8. Řízení incidentů:

- Evidence incidentů (do 30 minut)
- Reakce IT: do 4 hodin
- Kategorizace (nízký – střední – kritický)
- Hlášení NÚKIB (podle kategorie incidentu)
  - prvotní hlášení do 24 hodin
  - oznámení o incidentu do 72 hodin

9. Školení a osvěta:

- Noví zaměstnanci: školení do 5 dnů od nástupu.
- Opakovací školení: 1× ročně.
- Obsah: phishing, hesla, home office, BYOD (tj. užívání soukromých zařízení v práci).
- Roční test znalostí specialistů IT.

10. Audit a revize:

- Interní audit každé 2 roky.
- Samohodnocení 1× ročně.
- Nápravná opatření s odpovědnostmi.
- Vedení elektronické knihy incidentů.
- Archivace dokumentace min. 5 let.

11. Soulad s legislativou:

- Sledování právních změn.
- V případě, že osoby regulované, tedy povinné z hlediska nové legislativní úpravy, budou požadovat po dodavatelích nebo spolupracujících osobách další ochranná opatření z hlediska zajištění zvýšené kybernetické bezpečnosti IS bude na toto reagováno.

12. Závěr:

Směrnice je závazná pro všechny zaměstnance a spolupracující osoby. Nedílnou součástí této směrnice jsou přílohy, které jsou neveřejné a upravují konkrétní postupy při realizaci kybernetické bezpečnosti. Na tuto Směrnici navazují další interní Směrnice, kde jsou konkrétně rozvedeny mechanismy ochrany IS (Minimální bezpečnostní požadavky) a další speciální směrnice v rámci kybernetické bezpečnosti Společnosti. Porušení Směrnic na ochranu IS může být a bude Společností vnímáno jako porušení vnitřních směrnic a Etického kodexu s možností konkrétní sankce.

Směrnice nabývá účinnosti dne 1.3.2026

Petr Rybníček MBA

Předseda představenstva

Ing. Martin Hofman

Člen představenstva