

WEDOS Group SA



TLP: CLEAR

Verze: 1

POLITIKA BEZPEČNOSTI INFORMACÍ

Nabývá účinnosti dne

02. ledna 2026

	Zpracoval	Schválil
Jméno	Ing. Petr Říha	Mgr. Josef Grill
Podpis		 WEDOS Internet, s.r.o. Návrykova 1225 373 61 Huboká nad Vltavou IČ: 28115798, DIČ: CZ28115798 www.WEDOS.com
Datum	2. ledna 2026	2. ledna 2026

1. ÚVOD

1.1 Účel dokumentu

Tato **Politika bezpečnosti informací** stanovuje základní principy a požadavky pro zajištění důvěrnosti, integrity a dostupnosti informačních aktiv společnosti.

1.2 Kontext organizace

Skupina společností WEDOS (dále jen „skupina“), zastřešená firmou WEDOS Group SA, se zabývá registrací internetových domén, webhostingem, pronájmem virtuálních a dedikovaných serverů, serverhostingem, poskytováním cloudových služeb a provozem vlastních datacenter v Hluboké nad Vltavou a obchodním oddělením v Sezimově Ústí.

Skupina působí na domácím i mezinárodním trhu a poskytuje služby s vysokými nároky na dostupnost, integritu a bezpečnost zpracovávaných informací.

Provoz vlastních datacenter představuje klíčový prvek kontroly nad fyzickou a technickou bezpečností infrastruktury.

ISMS je aplikován rovněž na poskytování cloudových služeb, včetně ochrany osobních údajů zákazníků a dat uložených v cloudové infrastruktuře.

1.3 Rozsah

Tato politika se vztahuje na všechny zaměstnance, externí spolupracovníky, dodavatele a třetí strany, které mají přístup k informacím nebo informačním systémům společnosti, a na všechny informace v digitální i fyzické podobě.

1.4. Prohlášení vedení

Vedení společnosti považuje informace za klíčová aktiva a zavazuje se k jejich ochraně prostřednictvím implementace, udržování a neustálého zlepšování systému řízení bezpečnosti informací v souladu s normou ISO/IEC 27001.

Bezpečnost informací je současně vnímána jako strategická konkurenční výhoda skupiny WEDOS, zejména při poskytování mezinárodních služeb, jako jsou WEDOS Global Protection a Anycast DNS. Ochrana informací a vysoká dostupnost služeb jsou klíčovými faktory důvěry zákazníků a dlouhodobé stability skupiny.

Vedení skupiny vnímá systém integrovaného managementu jako základní nástroj řízení organizace a zavazuje se podporovat tuto politiku, zajišťovat optimální plánování a využívání potřebných zdrojů a vytvářet podmínky pro trvalé udržování a zlepšování systému integrovaného managementu v souladu s požadavky norem ČSN EN ISO/IEC 27001, ČSN ISO/IEC 27017, ČSN EN ISO/IEC 27018, ČSN EN ISO 9001 a ČSN EN ISO 14001.

2. ZÁKLADNÍ PRINCIPY A CÍLE

2.1 Hlavní principy

- Bezpečnost informací je odpovědností každého jednotlivce v organizaci
- Ochrana informací musí být zajištěna v celém jejich životním cyklu
- Opatření bezpečnosti informací musí být přiměřená zjištěným rizikům
- Bezpečnost informací je nedílnou součástí všech činností, projektů a služeb

- Přístup k informacím je založen na principu "need-to-know"
- Bezpečnost informací podporuje důvěru zákazníků, stabilitu poskytovaných služeb a dlouhodobou prosperitu skupiny.

2.2. Vlastníci aktiv

- Zajistit soulad s právními, regulatorními a smluvními požadavky
- Chránit důvěrné informace společnosti a osobní údaje klientů před neoprávněným přístupem
- Zajistit kontinuitu kritických procesů a služeb v případě bezpečnostních incidentů
- Minimalizovat bezpečnostní rizika při vývoji a poskytování IT služeb
- Zvyšovat povědomí o bezpečnosti mezi zaměstnanci a relevantními třetími stranami

3. ORGANIZACE BEZPEČNOSTI INFORMACÍ

3.1 Role a odpovědnosti

- Představenstvo schvaluje politiku bezpečnosti informací a poskytuje strategické vedení
- Výkonný ředitel nese celkovou odpovědnost za bezpečnost informací ve společnosti
- Bezpečnostní manažer koordinuje implementaci a správu ISMS, dohlíží na dodržování politik
- Vedoucí oddělení jsou odpovědní za implementaci bezpečnostních opatření ve svých útvarech
- Zaměstnanci a externí spolupracovníci jsou povinni dodržovat stanovené bezpečnostní politiky a postupy
- Vedení skupiny jde osobním příkladem při dodržování bezpečnostních pravidel a aktivně podporuje rozvoj bezpečnostní kultury v celé organizaci.

3.2 Oddělení povinností

Ve společnosti bude uplatňován princip oddělení povinností, aby se snížilo riziko neoprávněné nebo neúmyslné modifikace nebo zneužití informačních aktiv.

4. KLASIFIKACE A SPRÁVA INFORMAČNÍCH AKTIV

4.1 Klasifikace informací

Informace jsou klasifikovány podle své důvěrnosti do následujících kategorií:

- **Veřejné** - informace určené ke zveřejnění bez omezení
- **Interní** - informace určené pouze pro zaměstnance a případně také s dalšími partnerskými subjekty.
- **Důvěrné** - informace určené pouze pro omezenou skupinu osob a jejím partnerům, a to pouze osobám, které splňují zásady need-to-know.
- **Přísně důvěrné** – informace přísně důvěrně pouze pro osoby(skupiny) na principu „need-to-know

4.2 Označování a nakládání s informacemi

Všechny informace musí být označeny podle své klasifikace a musí být s nimi nakládáno v souladu s příslušnými směrnicemi.

5. ŘÍZENÍ PŘÍSTUPU

5.1 Základní principy

- Přístupy k informacím jsou udělovány na základě pracovní role
- Uplatňuje se princip nejnižších privilegií
- Přístupy podléhají pravidelné revizi
- Přístupová práva jsou ukončena nebo změněna při změně pracovní role nebo ukončení spolupráce

5.2 Správa identit a přístupů

Společnost implementuje a udržuje procesy pro správu identit a přístupových práv uživatelů.

6. FYZICKÁ BEZPEČNOST

6.1. Zabezpečené oblasti

Kritické informační systémy a zařízení musí být umístěny v zabezpečených oblastech chráněných vhodnými bezpečnostními bariérami a kontrolami vstupu.

6.2. Bezpečnost zařízení

Zařízení musí být chráněna před fyzickými a environmentálními hrozbami a před neoprávněným přístupem.

7. PROVOZNÍ BEZPEČNOST

7.1 Provozní postupy

Provozní postupy musí být dokumentovány, udržovány a dostupné všem uživatelům, kteří je potřebují.

7.2 Ochrana před malwarem

Musí být implementována vhodná opatření pro detekci, prevenci a obnovu po útoku malwarem.

7.3 Zálohování

Zálohy informací, softwaru a systémových obrazů musí být prováděny a pravidelně testovány v souladu se schválenou politikou zálohování.

7.4 Správa zranitelností

Společnost pravidelně vyhodnocuje a řeší zranitelnosti technických systémů a aplikací.

7.5 Zajištění zdrojů

Vedení skupiny zajišťuje plánování a alokaci dostatečných finančních, personálních a technických zdrojů nezbytných pro udržování, provoz a neustálé zlepšování systému managementu bezpečnosti informací.

8. BEZPEČNOST KOMUNIKACÍ

8.1 Správa sítě

Sítě a síťová zařízení musí být adekvátně spravována a kontrolována, aby byla chráněna před hrozbami a byla zajištěna bezpečnost systémů a aplikací využívajících síť.

8.2 Přenos informací

Musí existovat formální politiky, postupy a kontrolní mechanismy pro ochranu přenosu informací prostřednictvím všech typů komunikačních zařízení.

9. AKVIZICE, VÝVOJ A ÚDRŽBA SYSTÉMŮ

9.1 Bezpečnostní požadavky

Bezpečnostní požadavky musí být zahrnuty do požadavků na nové informační systémy nebo rozšíření stávajících systémů.

9.2 Bezpečný vývoj

Společnost stanovuje a aplikuje pravidla pro bezpečný vývoj softwaru a systémů.

10. VZTAHY S DODAVATELI

10.1 Bezpečnost v dodavatelských vztazích

Požadavky na bezpečnost informací musí být dohodnuty s dodavateli a formálně dokumentovány.

10.2 Monitorování a přezkoumávání služeb dodavatelů

Společnost pravidelně monitoruje, přezkoumává a audituje poskytování služeb dodavateli.

11. ŘÍZENÍ INCIDENTŮ BEZPEČNOSTI INFORMACÍ

11.1 Hlášení událostí a incidentů

Všichni zaměstnanci a smluvní partneři jsou povinni hlásit události a slabá místa bezpečnosti informací.

11.2 Reakce na incidenty

Společnost má stanoveny postupy pro rychlou, účinnou a řádnou reakci na incidenty bezpečnosti informací.

12. SOULAD S POŽADAVKY

12.1 Soulad s právními a smluvními požadavky

Společnost identifikuje, dokumentuje a dodržuje všechny relevantní legislativní, regulační a smluvní požadavky.

12.2 Přezkoumání bezpečnosti informací

Přístup organizace k řízení bezpečnosti informací a jeho implementace musí být nezávisle přezkoumávány v plánovaných intervalech nebo při významných změnách.

13. ZÁVĚREČNÁ USTANOVENÍ

13.1 Platnost a aktualizace

Tato politika je platná ode dne schválení a bude přezkoumávána nejméně jednou ročně nebo při významných změnách.

Politika bezpečnosti informací je veřejně dostupným dokumentem a je závazná pro všechny zaměstnance, externí spolupracovníky a další relevantní zainteresované strany.

13.2 Důsledky nedodržení

Nedodržení této politiky může vést k disciplinárnímu řízení v souladu s interními předpisy společnosti a může mít právní důsledky.