QSCert

We cover credibility

QSCert, spol. s r. o.
Certification Body of Management Systems
E. P. Voljanskeho 1, 960 01 Zvolen, Slovak Republic

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

SNAS
Reg. No. 091/R-130

IAF CERTSEARCH
CHECK VALIDITY

týmto udeľuje

CERTIFIKÁT

ktorým potvrdzuje, že spoločnosť

thiss s.r.o.

Mlynské nivy 56, 821 05 Bratislava - mestská časť Ružinov

zaviedla a používa systém manažérstva bezpečnosti informácií podľa normy

ISO/IEC 27001:2022

v oblasti:
Poskytovanie podpory v IT
Poradenské a konzultačné činnosti v oblasti IT
Predaj HW, SW, licencií.

Certifikované lokality: Mlynské nivy 56, 821 05 Bratislava - mestská časť Ružinov

Na základe certifikačného auditu, protokol č. 6261/25 bolo preukázané, že manažérsky systém spĺňa požiadavky vyššie uvedenej normy.

Certifikát č.:	I - 6261/25
Vyhlásenie o aplikovateľnosti :	zo dňa 1.3.2025
Dátum prvotnej certifikácie:	10.05.2013
Dátum vydania certifikátu:	10.05.2025
Dátum platnosti:	09.05.2028

CERTIFICATION BODY QSCert OF MANAGEMENT SYSTEMS

Tento certifikát je platný iba ak je uvedený medzi platnými certifikátmi na www.qscert.com

Ing. Marcel Šlúch
riaditeľ certifikačného orgánu

ROZHODNUTIE ZAMESTNÁVATEĽA
o prijatí Politiky informačnej bezpečnosti

Zamestnávateľ:

Obchodné meno:	**thiss s.r.o.**
Sídlo:	Mlynské nivy 56, 821 05 Bratislava - mestská časť Ružinov
IČO:	47 669 217
Zápis:	Obchodný register Mestského súdu Bratislava III, oddiel: Sro, vložka č.: 122069/B

Číslo rozhodnutia:	**TH-RZ04**
Dátum prijatia rozhodnutia:	**25.03.2025**
Dátum účinnosti rozhodnutia:	**01.04.2025**

Rozhodnutie:
Zamestnávateľ týmto rozhodnutím k vyššie uvedenému dňu účinnosti prijíma nasledovnú Politiku informačnej bezpečnosti:

Politika informačnej bezpečnosti

Táto Politika informačnej bezpečnosti obsahuje ciele, rámec a dôležitosť procesov týkajúcich sa bezpečnosti informácií. Účelom Politiky informačnej bezpečnosti je identifikácia cieľov pre oblasť informačnej bezpečnosti a zabezpečenie nevyhnutnej ochrany firemných aktív Zamestnávateľa.

Špecifické politiky, opatrenia a odporúčania informačnej bezpečnosti dopĺňajú túto politiku pre oblasti:

1. Kontrolu prístupu;
2. Fyzickú bezpečnosť a bezpečnosť prostredia;
3. Správu aktív;
4. Prenos informácií;
5. Bezpečnú manipuláciu s koncovými zariadeniami;
6. Riadenie incidentov;
7. Zálohovanie;
8. Kryptografia, šifrovanie;
9. Riadenie technických zraniteľností;
10. Bezpečný vývoj.

Zamestnávateľ kladie dôraz hlavne na:

1. Dodržiavanie legislatívnych a zmluvných požiadaviek v oblasti informačnej bezpečnosti;
2. Stanovenie požiadaviek na vzdelávanie Zamestnancov v oblasti informačnej bezpečnosti;
3. Určenie požiadaviek na prevenciu, monitoring a profylaktiku;
4. Dodržiavanie zásad riadenia kontinuity činnosti organizácie;
5. Prijímanie nápravy zo skúseností z bezpečnostných incidentov;
6. Uvedomenie si následkov porušení bezpečnostnej politiky;
7. Implementáciu bezpečnostných zásad na služby poskytované Odberateľom;
8. Určenie menovitej zodpovednosti za SMIB v Spoločnosti, pričom Spoločnosť vykonáva pravidelnú analýzu rizík, v rámci ktorej určuje prijateľnú úroveň rizika.

Hlavným cieľom tejto bezpečnostnej Politiky informačnej bezpečnosti je zabezpečiť kontinuitu činností, s ohľadom na minimalizovanie strát, spojených so zlyhaním zariadení a personálu, takisto aj minimalizovanie ekonomických dopadov pri výpadku.

Politika SMIB a dopĺňajúce predpisy informačnej bezpečnosti sú oznámené Zamestnancom. Týmto rozhodnutím Zamestnávateľ súčasne odvoláva predchádzajúcu Politiku informačnej bezpečnosti zo dňa 09.03.2018.

Toto rozhodnutie je prijaté v súlade s internými predpismi Zamestnávateľa a všeobecne záväznými právnymi predpismi Slovenskej republiky.