NOVARTIS

# Associate Director, AI Security Architecture

Job ID
REQ-10091829
Nov 10, 2026
LOC_CZ

### About the Role

### Key Responsibilities

- Lead AI architectural activities and develop secure solution architectures across business and technology domains.
- Define AI security standards and best practices for protecting AI pipelines, datasets, models, and infrastructure.
- Develop logical architecture designs and strategies to secure the organization’s AI domain and infrastructure.
- Establish and evolve AI architecture governance frameworks, including methods, practices, standards, and reusable architecture patterns.
- Assess the AI landscape, identifying and mitigating security risks across model training, deployment, and operations.
- Evaluate AI security technologies and integrate appropriate security controls across AI platforms and Large Language Models.
- Secure AI and agentic systems against model poisoning, adversarial inputs, prompt injection, jailbreaking, and emerging threats.
- Design Model Context Protocol servers, AI agent workflows, secure deployment architectures, and AI gateway integrations.
- Build Python services, developer tools, integrations, and AI security harnesses supporting secure software development.
- Collaborate with data scientists, engineers, and DevOps teams to embed security throughout the AI development lifecycle.

### Essential Requirements

- 12+ years of overall professional experience, including substantial experience across security, architecture, software development, and AI security engineering.
- At least 5 years of security experience, 5 years in architecture, 5 years in development, and 2+ years in AI security and engineering.
- Proven AI security architecture expertise covering training data, models, pipelines, deployed AI solutions, security policies, standards, and architecture patterns.
- Strong knowledge of AI threats, risk identification, threat modeling, data privacy, and defenses against adversarial and AI-based attacks.
- Hands-on experience securing Artificial Intelligence and Machine Learning applications across cloud platforms, with strong Amazon Web Services engineering and architecture expertise.
- Production experience with AI coding agents, Model Context Protocol servers, agent workflows, Python development, automated testing, and AI gateway integrations.

### Desirable Requirements

- Security engineering or application security background, with experience evaluating and working with specialized AI security technologies.

- Experience building developer-facing command-line tools and working effectively in multi-vendor, global technology environments.

The base salary offered is determined based on gender-neutral objectives, such as relevant skills, competencies and experience in accordance with the Novartis pay setting policy and upon joining Novartis will be reviewed periodically.

In addition to your base salary, you may be eligible for a performance-based bonus depending on certain performance parameters.

The rewards of being part of our team go far beyond base pay and incentives. We also offer a variety of competitive benefits in kind to help you thrive personally and professionally, such as insurance plans, retirement plans, wellbeing resources and global recognition programs. In addition, we provide flexible and hybrid working options, where possible, and minimum 14 weeks paid parental leave.

You'll receive (CZ only):
Monthly pension contribution matching your individual contribution up to 3% of your gross monthly base salary; Risk Life Insurance (full cost covered by Novartis); 5-week holiday per year; (1 week above the Labour Law requirement) ; 4 paid sick days within one calendar year in case of absence due to sickness without a medical sickness report; Cafeteria employee benefit program – choice of benefits from Benefit Plus Cafeteria in the amount of 1,500 CZK per year; Meal vouchers in amount of 105 CZK for each working day (full tax covered by company); Car Allowance; MultiSport Card. Find out more about Novartis Business Services: https://www.novartis.cz/

Pay equity is a fundamental principle of our employment policy and reflects our commitment to create a diverse, equitable and inclusive environment that treats all employees with dignity and respect, as outlined in our Code of Ethics.

Read our brochure to learn more about our global total rewards offering:
https://www.novartis.com/sites/novartis_com/files/novartis-life-handbook.pdf

Note: Benefits and compensation may vary by country and are subject to local legal requirements, including provisions of collective bargaining agreements where applicable. A full overview of your compensation package, including any relevant collective bargaining agreement details applicable to your role based on your employment location and Novartis employer entity, will be communicated separately to you during the application process.

Commitment to Diversity & Inclusion:

Novartis is committed to building an outstanding, inclusive work environment and diverse teams representative of the patients and communities we serve.

Accessibility and accommodation:

Novartis is committed to working with and providing reasonable accommodation to all individuals. If, because of a medical condition or disability, you need a reasonable accommodation for any part of the recruitment process, or in order to receive more detailed information about the essential functions of a position, please send an email to di.cz@novartis.com and let us know the nature of your request and your contact information. Please include the job requisition number in your message.

## Role Requirements

Primary location salary range
Kč1,288,241.50 - Kč2,392,448.50
Division
DIV_TO
Business Unit
Information Technology
Location
LOC_CZ
Site
Prague
Company / Legal Entity
CZ02 (FCRS = CZ002) Novartis s.r.o.
Functional Area
FCT_IT
Job Type
Full time
Employment Type
Regular
Shift Work
No
Apply to Job

Job ID
REQ-10091829

## Associate Director, AI Security Architecture

Apply to Job

---

**Source URL:** *https://jobapi.novartis.com/req-10091829-associate-director-ai-security-architecture*

**List of links present in page**

1. https://jobapi.novartis.com/req-10091829-associate-director-ai-security-architecture
2. https://www.novartis.cz/
3. https://www.novartis.com/sites/novartis_com/files/novartis-life-handbook.pdf
4. mailto:di.cz@novartis.com
5. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Prague/Associate-Director--AI-Security-Architecture_REQ-10091829
6. https://novartis.wd3.myworkdayjobs.com/en-US/Novartis_Careers/job/Prague/Associate-Director--AI-Security-Architecture_REQ-10091829