



## **About the Company:**

Deep Surface AI is a startup focused on streamlining the cosmetic surgery consultation process. We are developing software tools to improve facial plastic surgery outcomes. Through rigorous quantification of biological variation in facial form we generate detailed proposals for cosmetic surgery objectives customised to each patient's unique face. Our products will help surgeons ensure they understand patient goals, and empower patients to choose outcomes that match their personal needs.

The beachhead market for our visualization software is gender affirming facial surgery (GFS) for transgender female patients. We aim to improve the clinical workflow of surgeons and the experience of patients by offering a data driven approach to visualising and considering alternative surgical objectives.

## **Our Commitment to Equity, Diversity and Inclusion**

As an equitable and inclusive employer, Deep Surface AI is committed to fostering a diverse work environment where all individuals are treated with respect and dignity. We welcome and encourage applicants from women, Indigenous peoples, persons with disabilities, members of visible/racialized minorities and diverse sexual orientation and gender identities. We believe that diversity in backgrounds, perspectives, and experiences leads to a more innovative and effective workplace.

## **About the Role:**

As an AppSec developer, you will support our product, software development and compliance team in commercializing our software product. Successful candidates have a deep understanding of private data management, application security, managing vulnerabilities throughout the software development cycle, and a working knowledge of relevant privacy legislation. Being comfortable with learning on the fly and collaborating with cross disciplinary teams is a must.

## **Role Specifics**

- Temporary full time position for Summer 2023 (May-August).
- Part-time capacity (~5-10 hours per week) during Winter Semester welcome.
- Wage: \$22.50 - \$27.00 per hour
- Hybrid working model

## **Roles and Responsibilities:**

- Support compliance team in identifying privacy and security requirements, and developing privacy and security policies and procedures
- Integrate with development team by designing and implementing security solutions into software product, and responding to information security incidents
- Aid in identifying, remediating and managing security vulnerabilities found in pen-tests
- Aid in the design of simple, scalable and reliable cloud architectures for AppSec

## **Basic Qualifications:**

- Undergraduate level education in computer science, software engineering or related fields
- Demonstrable experience in software development or application security
  - *Note: Good personal portfolios and community participation (hackathons, datathons) will also be considered alongside previous work experience.*



**Preferred Qualifications:**

- Graduate level education in information security, computer science, or related fields
- 1 - 2 years of experience as an application security developer, or software engineer
- Deep proficiency in Python
- Previous exposure to cloud service providers (AWS, GCP, Azure)
- Working knowledge of continuous integration and continuous deployment (CI/CD)