Advisor.AI - Information Security

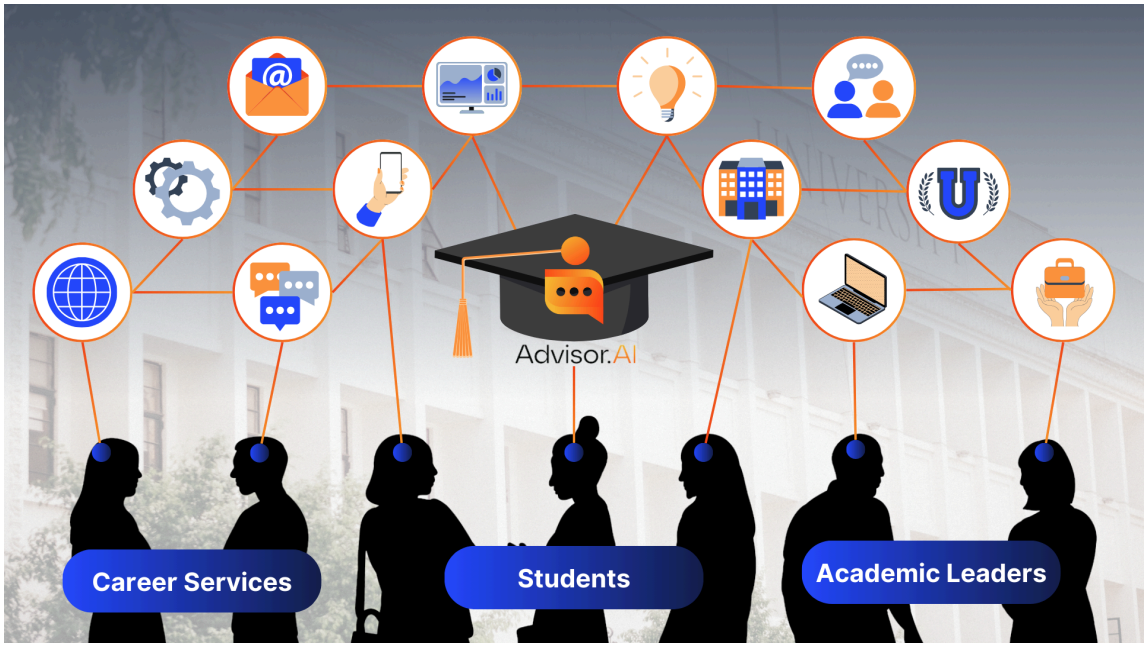
At Advisor.AI, data privacy, integrity, and security are of the utmost importance. This document provides a detailed overview of the measures we have in place to ensure the security of the Advisor.AI platform and to safeguard our users' information.

As a pioneering AI-powered advising platform, Advisor.AI is committed to supporting students, educators, and institutions with personalized and data-driven tools to enhance student success. With this commitment comes a responsibility to protect sensitive user data, and we have implemented various security measures, including advanced encryption protocols and strict access controls, to keep all user information safe.

Advisor.AI conducts regular security audits and assessments to identify potential risks or vulnerabilities, allowing us to take proactive steps to secure our system and services. With these robust measures in place, Advisor.AI provides peace of mind to its partners, ensuring that sensitive data is handled with care and remains fully protected.

Our dedicated security and ethical AI team consists of senior engineering experts, ethical AI practitioners from Fortune 500 tech companies, legal professionals specializing in data privacy, and leaders of various public and private universities, all working together to ensure robust security and ethical AI best practices are followed and implemented.

All of our industry-leading security and responsible AI services are included as part of the Advisor.AI platform at no additional cost. This sets us apart as the only comprehensive AI advising solution with no hidden fees related to security, AI model training, and implementation.



Platform Security

Access Control Policy

Access to data within the Advisor.AI platform is strictly managed through robust access controls, ensuring that all users—whether students, advisors, or administrators—have the appropriate permissions based on their roles. Advisor.AI implements a closed-system approach to data entry and access, limiting exposure to and entry of sensitive information into the system. Our predefined roles and permissions adhere to the least-privilege principle, making it easy for administrators to assign the correct access levels for each user while safeguarding data privacy and system integrity.

Secure Authentication

Advisor.AI supports the modern Google Sign-On option to provide secure and seamless access. Access to administration interfaces is encrypted using industry-leading protocols like HTTPS and TLS 1.3, with AI models and data privacy safeguarded through end-to-end security measures. Advisor.AI administrators handle university registration and de-registration.

Data in Transit

Advisor.AI uses industry-leading best practice encryption schemes (HTTPS and TLS1.3) to encrypt data in transit and communications between the platform users (students, advisors, and administrators). Advisor.AI supports TLS 1.3 and 1.2

Data at Rest

The Amazon Web Services (AWS) infrastructure ensures encryption at rest of all data-stores containing non-public information using an industry-standard AES-256 encryption algorithm.

Availability

AWS has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable us to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, our customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

Operations Security

Change Management

Advisor AI's development cycle is based on the scrum framework, specifically Agile. Agile is a project management approach that breaks projects into short, iterative cycles called "sprints". At its core, Agile is based on the assumption that circumstances change as a project develops. That's why, in an Agile project, the planning, design, development, and testing cycles are never done. They continue to change as the project takes form. Change management is directly integrated within the process.

Development Process

Advisor AI maintains an industry-leading secure software development lifecycle program. All code is subject to review and approval via the change management process, which includes separation of duties and approvals. Code security and dependency checks are performed before every deployment. Furthermore, access to source code is heavily restricted, and a Version Control tracks all changes to source code.

Compliance

Advisor.AI leverages Amazon Web Services (AWS) to host its application, manage data storage, system backups, server management, and cloud infrastructure. AWS is an industry leader in data security and provides comprehensive security features that meet stringent industry and FERPA standards.

AWS's infrastructure has been thoroughly vetted and certified for compliance against global security standards, ensuring the highest level of protection for Advisor.AI's platform. AWS is compliant with the following certifications:

- BIO Thema-uitwerking Clouddiensten
- DoD SRG
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- MTCS Tier 3
- OSPAR
- PCI DSS Level 1
- SOC 1
- SOC 2
- SOC 3

By hosting Advisor.AI on AWS, the platform benefits from these industry-leading certifications, ensuring the security and privacy of all data within the system.

Responsible & Ethical AI

Responsible AI is the practice of developing, using, and deploying artificial intelligence (AI) systems in a way that is ethical, transparent, and accountable. The goal of responsible AI is to ensure that AI technologies are aligned with human values and promote the well-being of society and individuals. Our team of legal experts, AI practitioners, and university leaders meet regularly to assess our processes in relation to industry-leading frameworks such as SAFE.

SAFETY

At Advisor.AI, we prioritize data security through robust encryption practices. All training data and model outputs are encrypted both in transit and at rest, ensuring the highest levels of protection throughout the entire data lifecycle. We employ industry-standard encryption protocols to prevent unauthorized access and safeguard sensitive information. Additionally, role-based access controls are implemented, allowing only authorized personnel to interact with model training and inference APIs. These security measures ensure that the platform remains resilient against potential threats, maintaining the confidentiality of our AI-driven insights.

ACCOUNTABILITY

We foster accountability through a system that ensures active collaboration between students and advisors. Our platform is designed to prevent over-reliance on AI by empowering human oversight. Advisors can engage with students directly through the platform, while students have access to advisors and mentors via the app, ensuring that human feedback remains integral to academic and career decisions. This collaborative approach ensures both our AI systems and users are accountable for driving meaningful outcomes.

FAIRNESS AND TRANSPARENCY

Fairness and transparency are foundational to our AI development process. We proactively mitigate bias by rigorously testing our proprietary models before deployment, ensuring that they deliver equitable results across diverse student profiles. Continuous monitoring and weekly model audits, help us maintain fairness and ethical standards. Transparency is also key: we make our AI-driven recommendations clear and understandable to users, supplemented by comprehensive FAQs that explain how decisions are made. This openness fosters trust and confidence in the recommendations powered by the platform.

EFFICACY

Advisor.AI is built to achieve measurable success outcomes, guiding students from pre-enrollment to career readiness. Our AI-driven insights work alongside human support systems to enhance, not replace, personal advisor-student interactions. The platform's reliability ensures that students receive timely, accurate, and personalized support throughout their academic journey, helping them stay on track and succeed in their educational goals.

Technical Operational Measures

Environment Separation

Development, testing and pre-production environments are divided logically from the production environment via a distinct ECS cluster. Production data is never used in lower environments.

Backup

Our backup policy guarantees that platform data on Advisor AI is replicated in several geographical locations. The replication instances are configured and reliant. Our production databases are backed up and versioned every day. Those backups are kept for seven days. Backups are encrypted at the whole disk level.

Logging and Monitoring

Advisor AI uses application server logs which contain all user actions that prompt an HTTP request to the application (e.g. loading a page, submitting a form, triggering background HTTP requests etc.), as well as some associated data. These logs include actions performed by administrative accounts.

Logical Access

Access to the Advisor AI's production infrastructure is restricted to specific members of the Advisor AI's technical team, following the least-privilege principle. By default, members of the technical team do not have access and have to request access during a certain time frame.

Physical Perimeters and Location

Our platform is hosted in Amazon Web Services (AWS) facilities in the US Data Region. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. The AWS physical access points to server rooms are recorded by Closed-Circuit Television Cameras (CCTV). Images are retained according to legal and compliance needs.

Protecting Against External and Environmental Threats

Power
Our data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. AWS ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

Climate and Temperature
AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Fire Detection and Suppression
AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

Leakage Detection
In order to detect the presence of water leaks, AWS equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

Equipment Maintenance
AWS monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within AWS data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

Other Key Resources

1. Terms of Service
2. Privacy Policy