Security and Compliance at Visor.ai

Effective Date: 23/08/2024

Protecting personal and customer confidential information is our unwavering commitment. To ensure the highest possible level of security, we adhere to strict data protection standards and continuously update our practices. Transparency is a cornerstone of our approach. The following overview provides a high-level look at the continuous evolving security practices we have in place.

General Information Security Policy

Protect Visor.ai's informational and IT assets (including but not limited to all computers, mobile devices, networking equipment, software and sensitive data) against all internal, external, deliberate or accidental threats and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems;

Ensure information will be protected against any unauthorized access. Users shall only have access to resources that they have been specifically authorized to access. The allocation of privileges shall be strictly controlled and reviewed regularly.

Protect CONFIDENTIALITY of information. When we talk about confidentiality of information, we are talking about protecting the information from disclosure to unauthorized parties;

Ensure INTEGRITY of information. Integrity of information refers to protecting information from being modified by unauthorized parties;

Maintain AVAILABILITY of information for business processes. Availability of information refers to ensuring that authorized parties can access the information when needed.
Comply with and, wherever possible, exceed, national legislative and regulatory requirements, standards and best practices;

Develop, **Maintain** and **Test** business continuity plans to ensure we stay on course despite all obstacles that we may come across. It is about “keeping calm and carrying on!”;

Raise awareness of information security by making information security training available for all Employees. Security awareness and targeted training shall be conducted consistently, security responsibilities reflected in job descriptions, and compliance with security requirements shall be expected and accepted as a part of our culture;

Ensure that no action will be taken against any employee who discloses an information security concern through reporting or in direct contact with Information Security Management Leader, unless such disclosure indicates, beyond any reasonable doubt, an illegal act, gross negligence, or a repetitive deliberate or willful disregard for regulations or procedures;

Report all actual or suspected information security breaches to **securityoffice@visor.ai.**