Information Security (ISO 27001)

TPradeepIT was awarded ISO 27001 certification — an International Standard for Information Security Management System issued by external auditors — by IAS Otabu. We are ISO27001:2013 certified. This certification verifies the compliance of PradeepIT's practices for Secure Software Development Lifecycle (SDLC), Secure Coding Practices, Incident Response Planning, Secure API, design, development and testing of Applications, Documentation and Training, and IOT Software Products and Services as per the latest Statement of Applicability.

Having the ISO 27001 logo on our company literature is a continual reminder to potential and existing customers that we are a professionally run organization that takes the confidentiality, integrity and availability of their information and our information seriously.

This helps us enhance customer confidence, ensure a secure operating environment, minimize business damage by reducing the impact of security incidents and eliminating the possibilities of reoccurrences of identified security incidents, and to maximize business investments and opportunities.

PradeepIT's ISMS Policy:

The Information Security Management System (ISMS) Policy of PradeepIT is to design, implement and maintain an Information security program that protects the PradeepIT Application development support systems, services and data against unauthorized use, disclosure, modification, damage and loss, Scope and Applicability, Legal and Regulatory Compliance, Risk Management, Security Awareness and Training, Incident Response, Monitoring and Audit and Review and Revision. Management is committed to establish an appropriate information security governance structure based on International Standards that enables collaboration and support for information security in business initiatives.

- **Confidentiality:** Safeguard sensitive and confidential information from unauthorized access, disclosure, or leakage.
- **Integrity:** Ensure the accuracy and integrity of software code, data, and information throughout its lifecycle.
- **Availability:** Maintain the availability of software systems and services, minimizing downtime and disruptions.

- **Authentication and Access Control:** Implement strong authentication mechanisms and access controls to prevent unauthorized access to software systems and repositories.
- **Secure Software Development:** Integrate security practices into the software development lifecycle to identify and mitigate vulnerabilities during the design, coding, testing, and deployment phases.
- **Data Protection:** Protect customer data and other sensitive information from unauthorized access, processing, or storage.
- **Patch Management:** Regularly apply security patches and updates to software components to address vulnerabilities and reduce exposure to known threats.
- **Incident Response:** Establish a clear incident response plan to detect, manage, and mitigate security incidents affecting software systems.
- **Secure Coding:** Implement secure coding practices to prevent common vulnerabilities such as SQL injection, cross-site scripting (XSS), and buffer overflows.
- **Vulnerability Management:** Continuously assess and manage vulnerabilities in software applications, libraries, and dependencies.
- **Data Encryption:** Encrypt sensitive data at rest and in transit to prevent unauthorized access or interception.
- **User Awareness Training:** Provide ongoing security awareness training to software developers and employees to educate them about security best practices.
- **Change Management:** Implement a structured change management process to ensure that software changes are controlled, tested, and documented.
- **Regular Security Audits:** Conduct regular security audits and assessments of software systems and development processes to identify and address security gaps.
- **Secure APIs:** Design and develop secure application programming interfaces (APIs) that follow best practices for authentication, authorization, and data validation.
- **Secure Development Tools:** Utilize secure development tools, static analysis, and code reviews to identify and remediate security vulnerabilities.
- **Secure Deployment:** Implement secure deployment practices to ensure that software is securely configured and deployed in production environments.
- **Privacy Compliance:** Ensure that software systems and processes comply with applicable data protection and privacy regulations.

- **Supplier Security:** Assess the security practices of third-party software components, libraries, and services used in development.
- **Regular Security Testing:** Conduct regular security testing, including vulnerability scanning and penetration testing, to identify and remediate weaknesses.
- **Business Continuity:** Develop and test business continuity and disaster recovery plans to ensure software systems can be restored in case of disruptions.
- **Continuous Improvement:** Continuously monitor and improve the security posture of software systems based on feedback, incidents, and emerging threats.

Leveraging the ISO 27001 standards leads to the implementation of the following measures, aimed at upholding the security of the information we manage on behalf of our customers, ensuring its Confidentiality, Integrity, and Availability.