INTEGER WEALTH GLOBAL

Policy on Software Development Life Cycle (SDLC)

Date: 14 March 2023

Policy Statement

This policy outlines the Software Development Lifecycle (SDLC) used at Integer Wealth Global for the development and maintenance of the Accelero Platform. The Accelero Platform, developed by Accelero Tech Ltd, is an artificial intelligence-based system that facilitates online applications for funding and investment management. This policy ensures that all software development activities are conducted in a structured, efficient, and compliant manner.

1. Scope

This policy applies to all software development activities related to the Accelero Platform, including design, development, testing, deployment, and maintenance.

2. SDLC Phases

2.1 Planning

- 2.1.1 **Requirements Gathering**: Collect and document business requirements from stakeholders.
- 2.1.2 **Feasibility Study**: Assess the technical, operational, and financial feasibility of the project.
- 2.1.3 **Project Planning**: Develop a project plan outlining timelines, resources, and milestones.

2.2 Analysis

- 2.2.1 **Requirement Analysis**: Analyse and refine requirements to ensure clarity and completeness.
- 2.2.2 **Risk Assessment**: Identify potential risks and develop mitigation strategies.

2.3 Design

- 2.3.1 **System Design**: Create detailed system architecture and design specifications.
- 2.3.2 **User Interface Design**: Develop user interface prototypes and gather feedback from stakeholders.
- 2.3.3 **Security Design**: Incorporate security measures to protect sensitive client and investor information.

2.4 **Development**

2.4.1 **Coding**: Write and review code according to design specifications and coding standards.
2.4.2 **Version Control**: Use version control systems to manage code changes and collaboration.
2.4.3 **Integration**: Integrate various system components and ensure compatibility.

2.5 **Testing**

2.5.1 **Unit Testing**: Test individual components for functionality and performance.
2.5.2 **Integration Testing**: Test the interaction between integrated components.
2.5.3 **System Testing**: Conduct end-to-end testing to ensure the system meets requirements.
2.5.4 **User Acceptance Testing (UAT)**: Validate the system with end-users to ensure it meets their needs.

2.6 **Deployment**

2.6.1 **Deployment Planning**: Develop a deployment plan, including rollback procedures.
2.6.2 **Environment Setup**: Prepare the production environment for deployment.
2.6.3 **Release Management**: Deploy the system to the production environment and monitor for issues.

2.7 **Maintenance**

2.7.1 **Monitoring**: Continuously monitor the system for performance and security issues.
2.7.2 **Bug Fixing**: Address any defects or issues identified post-deployment.
2.7.3 **Updates and Enhancements**: Implement updates and enhancements based on user feedback and changing requirements.

3. Compliance and Security

3.1 **GDPR Compliance**: Ensure all development activities comply with GDPR and other relevant data protection regulations.
3.2 **Security Measures**: Implement robust security measures, including encryption, access controls, and regular security audits.
3.3 **Data Protection**: Protect client and investor information from unauthorized access and disclosure.

4. Roles and Responsibilities

4.1 **Project Manager**: Oversees the project, ensuring it stays on schedule and within budget.
4.2 **Business Analyst**: Gathers and analyses requirements from stakeholders.
4.3 **Software Developers**: Write and review code and integrate system components.
4.4 **Quality Assurance (QA) Team**: Conducts testing to ensure the system meets quality standards.

4.5 **Data Protection Officer (DPO)**: Ensures compliance with data protection regulations and oversees security measures.
4.6 **Chief Liaison Officer**: Coordinates between departments and ensures alignment with business objectives.

5. Data Breach Response

5.1 **Immediate Action**: Take immediate steps to contain and mitigate any data breaches.
5.2 **Assessment**: Assess the scope and impact of the breach.
5.3 **Notification**: Notify relevant authorities and affected parties within 72 hours.
5.4 **Investigation**: Conduct a thorough investigation to determine the cause and prevent future incidents.
5.5 **Documentation**: Document all breaches and responses for future reference.

6. Continuous Improvement

6.1 **Feedback Loop**: Collect feedback from users and stakeholders to identify areas for improvement.
6.2 **Regular Reviews**: Conduct regular reviews of the SDLC process to ensure it remains effective and efficient.
6.3 **Training**: Provide ongoing training for all team members on best practices and new technologies.

7. Contact Information

For further inquiries or detailed explanations regarding this policy, clients are encouraged to contact our Chief Liaison Officer at info@integerwealth.global or the legal officer at legal@integerwealth.global.