A logo on a black background

Description automatically generated

***Security Controls Integration in Software Development***

***Introduction***

*This plan for integrating security into the Software Development Life Cycle (SDLC) applies to Tech Tribe's creation of a university sports department mobile application. It details security measures and regulations for every stage of the SDLC, guaranteeing that the application's creation, progression, and launch encompass top-notch techniques for safeguarding confidential information and maintaining safe processes. The scope encompasses risk assessment, secure coding, penetration testing, and adherence to industry regulations. This plan also points out deficiencies in existing methods and offers suggestions to improve security in Tech Tribe's development procedures.*

***Scope***

*The SDLC Security Integration Plan is for Tech Tribe's creation of a mobile app for a college sports department. It details security measures and safeguards for every stage of the SDLC to guarantee that the app's creation, design, and release adhere to the highest standards for safeguarding confidential information and maintaining secure processes. The range encompasses risk evaluation, safe programming, penetration testing, and adherence to industry standards. This plan also points out deficiencies in existing procedures and offers suggestions to improve security in Tech Tribe's development processes.*

***Overview***

*The plan for integrating security into Tech Tribe's software development cycle outlines how security can be incorporated into every phase of the SDLC. This document outlines the required controls and activities for protecting sensitive athletic and player data from planning and design through testing and deployment. The plan starts by identifying important security needs and continues with secure design, development techniques, and post-deployment monitoring. It ends by suggesting ways to fill the gaps and improve security in the organization's current SDLC.*

***SDLC Security Integration Plan***

*The SDLC offers a methodical way to develop software, guaranteeing both quality and efficiency. Yet, if security controls are not incorporated at every stage, applications will still be at risk of various cyber threats. The Tech Tribe's SDLC Security Integration Plan fills this void by incorporating security measures at every step of the development process. This plan guarantees that security is not overlooked but is a crucial element of the app’s design and operation. From initial planning to ongoing maintenance, security measures will be smoothly incorporated to reduce risks and guarantee adherence to data protection laws. By adhering to this thorough method, Tech Tribe will provide a safe, strong app for the college sports athletics department, safeguarding sensitive information and upholding the system's integrity.*

**SDLC Security Integration Plan**

***1. Planning/Requirements Gathering***

*Objective: Lay the foundation for security by identifying key requirements and addressing potential risks early in the process.*

*Security Activities:*

* *Conduct a comprehensive security requirements analysis, considering sensitive data such as player performance, health information, and communication channels.*
* *Perform a risk assessment to identify potential threats, vulnerabilities, and impacts to the app’s security.*
* *Ensure compliance with relevant data privacy laws and regulations related to student-athlete data protection.*
* *Establish security baselines to ensure consistent application of security controls throughout the development lifecycle.*

***2. Design***

*Objective: Establish a secure architectural framework and ensure security is embedded in the design phase.*

*Security Activities:*

* *Conduct threat modeling to assess potential security threats and vulnerabilities, ensuring they are mitigated early.*
* *Apply secure design principles such as least privilege, defense-in-depth, and secure by design, to minimize exposure to risks.*
* *Define and implement a robust data encryption strategy to protect sensitive information both at rest and in transit.*
* *Incorporate multi-factor authentication (MFA) to strengthen user access controls and prevent unauthorized access.*

***3. Implementation/Coding***

*Objective: Follow secure coding practices to prevent the introduction of security vulnerabilities during development.*

*Security Activities:*

* *Implement secure coding standards to mitigate vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).*
* *Use static analysis tools to automatically detect and address security flaws in the codebase during development.*
* *Ensure proper input validation, authentication, and session management are applied consistently across the application.*
* *Conduct peer code reviews to ensure adherence to secure coding practices and detect potential vulnerabilities early.*

***4. Testing***

*Objective: Identify and resolve security vulnerabilities before the production release.*

*Security Activities:*

* *Perform penetration testing to simulate real-world attacks and uncover potential vulnerabilities in the system.*
* *Use dynamic testing tools to identify vulnerabilities that may appear during runtime, ensuring secure operation in live environments.*
* *Conduct security regression testing to ensure previously addressed issues do not reoccur with new updates or code changes.*
* *Ensure that all known security vulnerabilities are remediated before the app is deployed to production.*

***5. Deployment***

*Objective: Ensure a secure production environment by enforcing security controls during deployment.*

*Security Activities:*

* *Ensure secure configuration management for all infrastructure components, including databases, APIs, and servers.*
* *Implement continuous monitoring tools to detect and respond to security incidents in real-time, ensuring swift remediation.*
* *Enable logging and auditing for critical security events to provide visibility into potential security issues and breaches.*
* *Conduct a final security review to verify that all security controls are properly implemented and operational before deployment.*

***6. Maintenance***

*Objective: Maintain security throughout the app’s lifecycle by addressing new vulnerabilities, applying updates, and monitoring for threats.*

*Security Activities:*

* *Implement regular vulnerability scans and patch management to protect against newly discovered threats.*
* *Continuously monitor system activity to detect suspicious behavior and respond to potential security breaches in real-time.*
* *Schedule periodic security audits to review and update security measures, ensuring compliance with the latest security policies and best practices.*
* *Regularly update and practice the incident response plan to ensure the team is well-prepared to handle any security incidents effectively.*
* *Periodically review and adjust security configurations to stay ahead of evolving threats and technological advancements.*
* *Maintain a reliable data backup and recovery strategy to minimize downtime and data loss in case of a security breach.*

***Organizational Analysis***

*At present, Tech Tribe's SDLC includes basic development practices but lacks comprehensive security integration, with key gaps such as incomplete risk assessments, minimal use of threat modeling, and inadequate security testing procedures. Additionally, security configuration management is underdeveloped, and incident response measures are not fully implemented. To address these deficiencies, Tech Tribe should adopt proven security frameworks during the design phase to establish a strong security foundation. Automated security testing tools, both static and dynamic, should be integrated into development and testing stages. The company must also develop thorough incident response plans to quickly manage breaches and ensure effective recovery. Finally, continuous real-time monitoring should be employed to detect anomalies and maintain security post-deployment.*

***Conclusion***

*Integrating security controls throughout Tech Tribe’s SDLC ensures that the development of the college sports app is secure from inception to decommissioning. By embedding security into each phase, Tech Tribe will reduce risks of data breaches, protect sensitive information, and comply with industry regulations. The proposed security controls will enhance the app’s security posture, protecting both the athletes and the department from potential cyber threats.*

*This comprehensive security integration plan not only addresses current gaps but also anticipates evolving threats, ensuring that the software remains resilient and secure in the long term.*

*References*

1. *Cybersecurity framework*. NIST. (2024, August 28). https://www.nist.gov/cyberframework
2. Wikimedia Foundation. (2024a, August 1). *ISO/IEC 27001*. Wikipedia. https://en.wikipedia.org/wiki/ISO/IEC\_27001
3. Wikimedia Foundation. (2024b, September 5). *Owasp*. Wikipedia. https://en.wikipedia.org/wiki/OWASP