[Company Logo]

Application Security Policy

To ensure the security of company data by establishing requirements for the proper maintenance and oversight of systems and applications used by the company.

Document Owner
Head of IT/Security

Application Security Policy
For

[Company Name].

Version: 1.0
Date: 01/01/0000
Next Review Date :

Note: Verify with the Policy Owner if this is the correct and latest version before use.

Revision History

Rev. #	Date	Modification Details	Page#	Suggested By	Reviewed By	Approved By
1.0		First Draft	NA			

Table of Contents

Purpose

To ensure the security of company data by establishing requirements for the proper maintenance and oversight of systems and applications used by the company.

The main purpose of an application security policy or standard is to reduce the risks posed to the applications used by a company. It prevents these applications from external threats that arrive from several paths to harm your business or organization. The threat agents will evaluate the weaknesses in your security system and attack you where you are most vulnerable. The harm caused by such risks can be both minimal and large-scale as well. Therefore, it is very important to create and maintain an effective application security policy to prevent such mishaps from occurring.

Scope

This Application Security Policy applies to all software applications developed, hosted, acquired, or maintained by [Company Name], including web, mobile, and desktop applications, APIs, and third-party solutions. It covers the entire application lifecycle, from design and development to testing, deployment, maintenance, and decommissioning. The policy ensures that security is embedded at every stage, addressing secure coding practices, authentication, data protection, vulnerability management, and compliance with regulatory standards such as GDPR, HIPAA, and PCI DSS.

The policy applies to all personnel involved in application security, including developers, testers, IT teams, third-party vendors, and business stakeholders. Compliance is mandatory to mitigate risks, safeguard sensitive data, and maintain the integrity of [Company Name]'s systems. By adhering to this policy, the organization ensures a consistent and proactive approach to identifying and addressing security threats across all applications.

Objective

The primary objective of this policy is to establish a robust framework for securing all applications within [Company Name] by integrating security best practices throughout their lifecycle. This includes preventing vulnerabilities, protecting sensitive data, and ensuring compliance with relevant regulations and industry standards.

Additionally, the policy aims to foster a culture of security awareness among developers, testers, and stakeholders, ensuring that security is prioritized from design to decommissioning. By implementing consistent security controls and accountability measures, the organization seeks to minimize risks, safeguard customer trust, and maintain the integrity of its digital assets.

Responsibility & Accountability

All personnel involved in the development, deployment, and maintenance of applications at [Company Name] are responsible for adhering to this Application Security Policy. Development teams must implement secure coding practices and integrate security controls throughout the software development lifecycle (SDLC). QA and testing teams are accountable for identifying and reporting vulnerabilities, while IT and operations teams must ensure secure deployment and ongoing monitoring of applications. Third-party vendors must comply with the policy's security requirements for any applications or services provided to [Company Name].

The Chief Information Security Officer (CISO) holds overall accountability for enforcing this policy and ensuring compliance across the organization. Business owners must prioritize security in application requirements, and management is responsible for allocating necessary resources for security initiatives

Non-Compliance

Failure to comply with this policy may result in disciplinary action, including termination of contracts for third parties or corrective measures for employees. Regular audits will be conducted to verify adherence, and all stakeholders must collaborate to address identified gaps promptly.

Exceptions

Not Applicable.

Policy Statement

1. All software and services used to process company information are subject to an Information Security review and sign-off before their purchase or development. Information Security reviews will evaluate specific risks and controls available and necessary based on the information being processed. The system owner will be responsible for the deployment of the agreed-upon security controls before enabling the production capability of the system or application.
2. Only necessary software should be loaded on systems, and old versions of software removed. The use of web browsers should be limited to the management of the system only.
3. A particular employee is responsible for overseeing that the following controls are appropriately applied and adhered to by the cloud provider.
4. Access to information in the possession of or under the control of the company must be provided on a need-to-know basis. The information must be disclosed only to individuals who have a legitimate and approved business need for information.
5. Information may only be used for its intended purpose, and other uses of company information without the approval of the data owner are not allowed.
6. Any system or application that is no longer supported by the vendor or is replaced by newer technology should be decommissioned as soon as possible. The proper update of systems and applications is critical to protecting the confidentiality, integrity, and availability of the system or application and its data. The decommissioning process must include the proper retirement of any physical hardware or virtual images and the proper destruction of any media (e.g., hard drives, tapes, etc.) that may have data.
7. All individuals, who have taken on or been assigned the responsibility of managing any system or application attached to the company network or any cloud system that holds a relationship to the company must ensure the timely implementation of operating systems and application patches to provide for the confidentiality, integrity, and availability of said systems or data.
8. The ongoing maintenance of applications and the application of software updates is an activity that must be regularly scheduled on a minimum quarterly basis.
9. Systems where individuals have access to a significant amount of the PII of other constituents, including employees, vendors, or significant amounts of regulated data, should leverage multi-factor authentication wherever possible.
10. Third-party or acquired web applications (i.e., commercial applications for which source code is not available) must be scanned when installed or upgraded. The vulnerabilities must be reported to Information Security and Assurance (ISA) and the vendor for correction.
11. Shared accounts are prohibited, except where it is not technically possible to provision accounts individually.
12. All applications must be developed with proper error-handling routines and “exception management” in place. Applications must not wrongly disclose system information.
13. Applications must adequately protect users by keeping session times to the minimum duration necessary and performing proper session management to ensure that user sessions are neither hijacked nor impersonated by unauthorized parties
14. Applications not performing authentication against an enterprise-class directory service must provide features and functions that allow for account expiration and renewal.

Conclusion

This document provides an overview of the Application Security Policy & its deliverables, the project team participants, and their roles and responsibilities. It is intended to assist Application Managers and developers of [Company Name] applications and to ensure a consistent approach to Application Security management

<<< End of Document >>>