# Application Security Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The quality and integrity of [Company Name’s] applications will be designed and implemented in as secure a manner as possible using pre-defined application development principles and procedures. Without secure application development, the potential exists that the application component of an information system could be constructed with flaws or other weaknesses that could allow for the subversion of the application and the contravening of [Company Name]’s other security controls.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This Application Security Policy applies to all information systems and information system components of [Company Name]. Specifically, it includes:

* Mainframes, servers, and other devices that provide centralized computing capabilities.
* SAN, NAS, and other devices that provide centralized storage capabilities.
* Desktops, laptops, smart phones, tablets, and other devices that provide distributed computing capabilities.
* Routers, switches, and other devices that provide network capabilities.
* Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.
* Cloud services, including but not limited to, infrastructure as a service, platform as a service, and/or software as a service.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. The application component of all information systems, whether it is developed in house or purchased from a third party, will be designed using security engineering principles. These security engineering principles will be applied to the entire lifecycle of the application element via a systems development life cycle methodology that includes security considerations at all stages of the life cycle. Further, development of the application element of an information system must include the creation and execution of a security test and evaluation plan. The results of this test and evaluation must be documented and shared with key stakeholders.
2. The application element of all information systems will logically separate user functionality from administrative functionality such that the interface for the one cannot be used to operate the other.
3. This policy applies to any application programming interface (API) that exposes application functionality to external consumers, written in the native application language or exposed in an open standard such as SOAP or Restful Web Services.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

Applications will be developed according to set methodologies that enforce security:

* + - * + Development processes should make use of documented and repeatable standards and processes.
        + Security training should be provided for the development team.
        + Quality management should be performed throughout the development process.
        + Code should be developed in a dedicated and secured environment.
        + Code should be stored in securely maintained repositories.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |