**Cybersecurity Templates**

**Cybersecurity Bug Tracking Policy & Model**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Cybersecurity Bug Tracking Policy & Model** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** |  | **Approved By:** |  |
| **Last Review Date:** |  | **Next Review Date:** |  |

Contents

[Cybersecurity Bug Tracking Policy & Model 3](#_Toc206631820)

[1.Purpose 3](#_Toc206631821)

[2. Scope 3](#_Toc206631822)

[3. Roles & Responsibilities 3](#_Toc206631823)

[4. Bug Lifecycle Process 3](#_Toc206631824)

[5. Bug Tracking Log 4](#_Toc206631825)

[6. Severity & SLA Matrix 4](#_Toc206631826)

[7. Lessons Learned & Continuous Improvement 4](#_Toc206631827)

[8. Review & Maintenance 4](#_Toc206631828)

# Cybersecurity Bug Tracking Policy & Model

## 1.Purpose

The purpose of this document is to establish a structured framework for tracking cybersecurity-related issues. This ensures that security vulnerabilities, defects, and system weaknesses are systematically identified, logged, prioritized, resolved, and reviewed. This model enables organizations to reduce risks, enhance accountability, and maintain compliance with security standards.

## 2. Scope

This policy applies to all cybersecurity bugs, vulnerabilities, and issues identified within the organization’s IT systems, applications, networks, and infrastructure. It covers employees, contractors, vendors, and third parties responsible for reporting, managing, and resolving issues related to bugs.

## 3. Roles & Responsibilities

* Reporters: All employees or stakeholders who identify bugs must document and report them immediately.
* IT Security Team: Validate reported bugs, assess severity, assign ownership, and track progress.
* Developers/Engineers: Investigate and remediate assigned bugs within defined timelines.
* Managers/Team Leads: Oversee bug resolution progress, enforce SLA compliance, and escalate critical issues.
* Auditors/Compliance: Ensure that bug tracking aligns with regulatory and internal audit requirements.

## 4. Bug Lifecycle Process

* Identification – Bugs are detected through security scans, audits, or user reports.
* Logging – Issues are logged in the Bug Tracking Log with unique IDs and details.
* Classification – Bugs are categorized by severity, priority, and root cause.
* Assignment – Each bug is assigned to an owner for resolution.
* Resolution – The bug is fixed, mitigated, or documented with a workaround.
* Validation – Fixes are tested to confirm effectiveness.
* Closure – The issue is formally closed once validated and approved.
* Post-Mortem – Lessons learned are documented for continuous improvement.

## 5. Bug Tracking Log

The following table should be used to record, track, and monitor cybersecurity bugs:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bug ID | Reported By | Date Reported | Severity | Status | Assigned To | System Affected | Description | Date Closed |
|  |  |  |  |  |  |  |  |  |

## 6. Severity & SLA Matrix

Bugs must be resolved according to severity-based timelines (SLA).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Severity | Impact | Example | Response SLA | Owner |
| Low | Minor issue, no security risk | UI typo | 30 days | Developer |
| Medium | Limited functionality | Non-critical feature bug | 14 days | Team Lead |
| High | Major functionality issue | Login failure | 7 days | DevOps |
| Critical | Severe vulnerability | SQL Injection exploit | 24 hrs | Security Team |

## 7. Lessons Learned & Continuous Improvement

After the closure of high- and critical-bug issues, a post-mortem analysis must be performed. This includes identifying root causes, lessons learned, and preventive measures. The outcomes are documented and fed back into development and security processes.

## 8. Review & Maintenance

This document and the bug tracking model will be reviewed annually, or after a significant incident, to ensure alignment with industry best practices, compliance standards, and organizational needs.