Sample Vulnerability Management Policy

Establishment date, effective date, and revision procedure

This policy is established on mm/dd/yyyy and is based on our Information Security Policy and policy and shall become effective on the same date. Corporate Security shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the head of Corporate Security shall prepare a draft and apply for authorization, and with the prior confirmation of the Corporate Executive Officer(s) in charge of the area(s) that will be affected by amendment or repeal, the theorganization C-Level executive will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Introduction

Purpose

The purpose of this policy is to establish security requirements to be observed by [*Organization Name's*] IT Departments.

Scope

The scope of this standard shall be the same as the scope of [*Organization Name's*] Security Policy.

Applicability

This policy applies to the organization's Information Systems personnel and if the applicable organization does not have an IT department, this policy shall apply to the organization that has the equivalent function of the organization's IT department.

Definitions

The definitions shall be the same as those set out in the organization's Information Security Policy and the Glossary for the organization's Information Security Policy.

Managing Information Security Vulnerabilities

Contractors/Third Parties Vulnerability Management

[*Organization Name*] shall ensure that contracts with Contractors/Third Parties who manage the organization data systems, networks and applications include the necessary language to require that Contractor/ Third Party vulnerability management practices meet or exceed this Vulnerability Policy where applicable.

Collecting Vulnerability Information

[*Organization Name's*] IT Department shall establish and maintain an Information Security Vulnerability Management Framework to clearly define how vulnerability information regarding important information system devices will be collected and provided to the respective system administrator(s). The framework will include risk assessment procedures to define the level of system importance. System administrators shall promptly check the impact of vulnerabilities, and then implement the appropriate measures in a timely manner.

Vulnerability Prevention Training

The Information Security Vulnerability Management Framework will include awareness and training, as outlined in Information Security Policy and the Human Resources Policy, to ensure that all employees as well as contractors and third party users, if applicable, are familiar with best practices to minimize computer vulnerabilities. The program should include technical and non-technical training.

Handling Vulnerabilities

System Administrators will promptly implement appropriate measures to remediate any vulnerabilities on information system devices.

Vulnerability type and standard schedule for implementing solutions

System administrators, in conjunction with the person in charge of Information Security at the organization shall prioritize vulnerabilities by Risk Level Based on Risk Assessment as set out in the

Vulnerability Risk Level Chart below. Once prioritized, the system administrator will then promptly implement the appropriate measures to minimize or eliminate the vulnerability according to the respective "Standard Required Correction Time". All patches and service packs shall first be tested before being widely deployed to ensure they do not negatively impact business processes. System Administrators will ensure that the appropriate patches and service packs are installed on all designated computers and systems.

Automated Patch Management System

System Administrators are to implement automated patch management systems where applicable and appropriate and record corrective actions in a change control process.

Security Patch Application Record

Details of vulnerability mitigation actions taken, such as implementation of latest security patches, shall be recorded and kept for a minimum of 3 months. Retention time frames should be adjusted to meet all applicable legal and regulatory requirements.

Vulnerability Inspections

Vulnerability inspections such as penetration tests shall be performed on a periodic basis on information system devices (excluding client PCs) in accordance with industry best practices. The inspector, inspection schedule, results format, and tools shall comply with the vulnerability framework of theorganization.

Vulnerability assessments must be designed and implemented in such a way as to not adversely impact production systems.

Vulnerability Information shall be classified based on an evaluation of the sensitivity of the Vulnerability Information.

Vulnerability Risk Level Chart

Impact	Risk Level Based on Risk Assessment *	Standard Required Correction Time
Very High Impact The vulnerability could allow broad exposure/compromise of Secret Information or massive denial or disruption of service	Risk Level 1	Within 1 business day
	Risk Level 2	Within 7 business Days
	Risk Level 3	Within 30 business days
High Impact The vulnerability could allow broad exposure/compromise of Confidential Information (and/or limited exposure of Secret Information) or significant denial or disruption of service	Risk Level 2	Within 7 business Days
	Risk Level 3	Within 30 business days
Medium Impact The vulnerability could allow a more limited exposure/compromise of Confidential Information (or a broad exposure of Internal Use Only	Risk Level 3	Within 30 business Days
	Risk Level 4	Within 60 business days

Information) or limited denial or disruption of service		
Low Impact The vulnerability could allow a limited exposure/compromise of Internal Use Only Information or a very limited denial or disruption of service	Risk Level 4	Within 60 business days

* Risk Assessment based on a qualitative evaluation incorporating factors such as:

- Applicability to theorganization
- Vendor's evaluation of risk
- Ease of exploitation
- System importance
- Type of data on system
- Susceptibility to the vulnerability

Categories of Risk Level Based on Risk Assessment:

- Risk Level 1 = very high risk
- Risk Level 2 = high risk
- Risk Level 3 = medium risk
- Risk Level 4 = low risk