Vulnerability Management and Virus Protection Policy

Document Control

Document Title:	Vulnerability Management and Virus Protection Policy
Version:	1.0
Version Date:	June 23, 2022
Created By:	Pivot Point Security (PPS)
Approved By:	TJ McCauley
Document Owner:	Information Security Management Committee
Confidentiality Level:	Confidential

Revision History

Version	Date	Author	Comments
0.1	March 19, 2020	PPS	1st Draft for Review
0.2	August 1, 2020	PPS	Control language updates
1.0	September 15, 2020	TJ McCauley	Approved
1.0	July 1, 2021	TJ McCauley	Annual Review & Approval
1.0	June 23, 2022	TJ McCauley	Annual Review & Approval

References

Standard / Guideline	Control Area(s)
ISO 27001:2013 ISO 27108:2014	A.5.1.1 Policies for information security A.12.2 Protection from malware A.12.6 Technical vulnerability management

Table of Contents

1. Purpose

The purpose of Accommodations Plus International's (API) Vulnerability Management & Virus Protection Policy is to define the requirements for notification, testing, and installation of security-related patches and to define the requirements for the implementation of antivirus and other forms of protection from malicious software on all corporate systems.

2. Scope

The Vulnerability Management & Virus Protection Policy applies equally to all individuals with authorized access to any information assets.

3. Vulnerability Management

3.1 Vulnerability Management Responsibilities

Information Technology and Information Security responsibilities for ensuring effective vulnerability management include, but are not limited to the following:

- Annual external penetration test by an independent third party for an independent review of API's security configuration.
- Annual external vulnerability scans by an independent third party for an independent review of API's security configuration.
- Monthly external port scanning.
- Review and approval of exception requests.
- Tracking the status of each vulnerability from discovery to final remediation.
- Providing updated reports for management review regarding current security posture and any open/unresolved vulnerabilities or exceptions.
- Ensuring that vulnerabilities on systems are remediated according to the requirements in this policy.
- Assessment of the impact of remediation or patch installation on systems under their management.
- Responsible for performing patch installation or other remediation.

3.2 Vulnerability Remediation

- Information Security will classify identified vulnerabilities according to the following severity levels:

SEVERITY	DESCRIPTION	SERVICE LEVEL
Critical	Critical vulnerabilities have a score of 5. They can be readily compromised with publicly available malware or exploits.	7 Days

High	High-severity vulnerabilities have a score of4. There is no known public malware or exploit available.	30 Days
Medium	Medium-severity vulnerabilities have a score of 3 and can be mitigated within an extended timeframe.	90 Days
Low	Low-severity vulnerabilities are defined with a 2 or lower score of . Not all low vulnerabilities can be mitigated easily due to the potential impact on applications and normal operating processes. These should be documented for exclusion if they cannot be remediated.	180 Days (Can be accepted)

- System administrators must apply required patches on all corporate-owned or managed devices or complete other remediation actions within the timeframe associated with the vulnerability's severity level.
- In a situation where a patch cannot be installed due to incompatibility with a system or other application, the application or system owner must request an exception within the same timeframe.
- Additional Recommendations.
    - System administrators should test patches or remediation actions on a non-production system, if available, to verify that it will not adversely impact system functionality or availability.
    - If a non-production system is not available, system administrators must take appropriate measures to verify the patch's correct functionality after being installed into production.
    - When available, it is recommended that system administrators utilize tools to automate the consistent installation of security patches.

4. Virus Protection

4.1 Virus Protection Responsibilities

Information Technology and Information Security responsibilities for ensuring effective virus protection include, but are not limited to the following:

- Manage and support antivirus software on corporate-owned and managed devices.
- Monitor and remediate infection events on corporate-owned and managed devices.
- Employees are responsible for reporting any notifications of possible infection on their assigned devices or attempted security breaches.

4.2 Virus Protection Administration

- Manage and support antivirus software on corporate-owned and managed devices.
- All computers and devices connected to the network or networked resources, whether physical or virtual, must have antivirus software installed and actively running on these devices if supported.
- Antivirus software programs must be configured to update their virus definitions daily (automatically). Monitoring processes will be used to ensure successful updates and compliance with this requirement.
- Antivirus software programs must be configured to scan all files on a computer device for signs of infection weekly at a minimum.
- All files downloaded from the Internet must be scanned for viruses at the point of download.
- If deemed necessary to prevent malware propagation or reduce detrimental effects to other networked devices, an infected computer device may be disconnected from the corporate network or platform until the infection has been removed.