Virus and Malware Prevention Policy

# Template

This is an example policy. Please ensure you update this policy template so that it’s suitable for your organisation.

## Policy statement

To meet our objectives and ensure continuity of its operations, we will adopt and follow well-defined and time-tested plans and procedures. This is to ensure the protection of IT assets from malware and virus attacks. IT assets must be employed in ways that achieve business objectives. Our IT assets will be protected in a way that ensures that they’re resistant to virus and malware attacks. All preventive and protective measures will be used to resist such attacks.

## Purpose

The purpose of this policy is to promote the use of anti-virus and other anti-malware software. The aim is to educate the employees regarding the policies that are widely followed to use anti-malware effectively. This policy provides direction to ensure that legal regulations are followed.

## Scope

### Employees

This policy applies to all who have access to our IT assets:

* employees
* volunteers
* contractors
* third party employees

### IT Assets

This policy applies to all workstations, servers and mobile devices that are under our control, or that are owned or leased by us.

### Documentation

The policy documentation will consist of ‘Anti-Malware Policy’ and related guidelines.

### Records

Records being generated as part of the ‘Anti-Malware Policy’ will be retained for a period of 2 years. Records will be in hard copy or electronic media. The records will be owned by <Role> and will be audited once a year.

### Distribution and Maintenance

The ‘’Anti-Malware Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document will be made available to the persons concerned. The maintenance responsibility of the document will be with the <Role>.

## Responsibility

The <Role> is responsible for the proper implementation of the policy. The ‘Virus/Malware Prevention Policy’ applies equally to all individuals that use our information resources.

## Policy

We will adopt certain practices to prevent malware/virus problems:

1. All workstations whether connected to our network or standalone, must use approved anti-virus and anti-malware software and configuration.
2. The anti-virus and anti-malware software must not be disabled or bypassed.
3. The settings for the anti-virus and anti-malware software must not be altered in a manner that will reduce the effectiveness of the software.
4. The automatic update frequency of the anti-virus and anti-malware software must not be altered to reduce the frequency of updates.
5. Each file server attached to the network must utilise approved anti-virus and anti-malware software, and set up to detect and clean malware that may infect file shares.
6. Every virus/malware that’s not automatically cleaned by the anti-virus and anti-malware software constitutes a security incident and must be reported to the <Role>.
7. The organisation will adopt suitable controls to prevent and detect the introduction of malicious code and unauthorised mobile code.
8. The information system automatically updates malicious code protection mechanisms. For example, automatic updates of anti-virus and anti-malware software.
9. Each email gateway will utilise approved email anti-virus software and will adhere to industry best practices for the setup and use of this software.
10. For systems thought not to be affected by malicious code or software, periodic assessments must be performed. This is to understand and evaluate evolving malware threats with a view to confirming whether these systems continue to not require anti-virus software.

## Enforcement

Any employee found to have violated this policy may be subject to disciplinary action in line with the HR Policy.

## Exceptions

Exceptions to the guiding principles in this policy must be documented and formally approved by the <role> and <organisation>.

Policy exceptions must describe:

* the nature of the exception
* a reasonable explanation for why the policy exception is required
* any risks created by the policy exception
* evidence of approval by all appropriate parties

Review of this document: annually by <role>.

Next review date: <date month year>.