[Your Company Name]

Anti-Virus & Malware Policy

DOCUMENT AUTHOR:	[Insert Author]
DOCUMENT OWNER:	[Insert Owner]
STATUS:	[Draft/Approved]
DATE CREATED:	[Insert Date]
VERSION:	[Insert Version]
LAST UPDATED:	[Insert Date]
SECURITY CLASSIFICATION:	[High/Medium/Low]

Document Customisation

This page *(to end of the 'disclaimer')* provides template guidance and ***must be removed*** from the finished version. For information on customising this template, please refer to the *'Instructions'* supplied with your order.

It is important to work through the document and customise any areas to ensure that the finished template accurately reflects what your organisation does and the controls that you have in place. You should consider your regulatory and legal obligations and any standards or requirements that apply to your industry or business type when customising the content.

Template Guidance

We have provided a generic template as a starting point for you to develop your own document in this compliance area. You should review and customise the template sections thoroughly to ensure that the finished version accurately reflects your organisations' controls and responsibilities.

This template goes hand in hand with the other information security policies in your pack and should be customised to note the exact anti-virus and malware software and protections that you use on all servers, networks and devices.

Referencing Other Policies

We sometimes reference other policies in a template where relevant *(i.e. refer to Anti-Bribery & Corruption Policy in conjunction with AML).* Referenced documents are **only** included in your pack if you have ordered them separately or you have purchased a Toolkit or Bundle that includes them.

Licence Terms

Purchased documents are for use within the ordering company **only** and cannot be used, sold or transferred elsewhere without written permission from Know Your Compliance Limited. Please refer to the *'Instructions'* document for more information on our T&C's and licence options.

Disclaimer

Know Your Compliance Limited has created this template for you to use in developing and implementing your compliance program requirements. Whilst every reasonable care is taken to ensure that the content is relevant, compliant and up to date; it is **your responsibility** to ensure that the finished policy complies with any regulatory and/or legal requirements and standards.

It is important that you customise the content to suit your industry needs and business type. Know Your Compliance Limited makes no claims or guarantees about the compliance or adequacy of the template content and accepts no responsibility or liability for any loss, damage or expense incurred as a result of reliance on our documents. If you are unsure of your obligations, you should obtain legal or professional advice before publishing, using or relying upon your finished policy.

Revision History

VERSION	REVISION DATE	SECTION REVISED	REASON FOR REVISION	DESCRIPTION OF REVISION

Table of Contents

1 Policy Statement 5
2 Purpose 5
3 Scope 5
4 Objectives 5
5 Responsibilities 6

1 POLICY STATEMENT

This policy helps [Your Company Name] (hereinafter referred to as the "Company") to deliver how it protects the devices, people and information under its remit through the use of malware and anti-virus software and applications. The Company installs malware and anti-virus protections on all devices that can access external networks and secure through secure configuration that risks and threats are minimised.

We recognise our obligations to protect not only the intellectual property of the Company, but also any personal or confidential information relating to our customers and employees. Users are made aware that they are not allowed to access the malware or anti-virus applications and are bound by the objectives and content of this policy.

2 PURPOSE

The purpose of this policy is to define the Company standards for installing and configuring malware and anti-virus software on all of its devices **[and employee's personal devices where they are used for business purposes].** The Company understands the threat posed by viruses and malicious software and have strict measures and controls for minimising the risk of its devices being infected or affected.

This Policy sets out the responsibilities of all users to ensure that they adhere to this policy and take every reasonable precaution when accessing, using or opening websites, emails, files, USB or other removable media or other systems that may pose a risk or threat to the Company's information systems.

3 SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4 OBJECTIVES

The Company recognises that virus or malware infections are extremely damaging in multiple ways. There is both a monetary and reputational cost when a device or network is infected, and the Company has an obligation to ensure that every reasonable measure is taken to reduce the risk of such infections happening.

As viruses and malicious software is constantly evolving, so are the Company's controls and approach to protecting our devices and networks. We have a number of objectives in place to ensure that our business, information, employees and customers are protected from virus and/or malware infections, including: -.

- Install anti-virus and malware applications or software on all devices that are connected to *(or can be connected to)* external systems and the internet
- Regularly update malware and anti-virus software and ensure that where applicable, automatic updates are enabled
- Known malicious sites or email addresses *(spam)* must be blacklisted where possible to prevent unauthorised access
- All devices and servers used by the Company utilise a supported operating system version with the latest patches and updates installed and applied
- Any personal devices *(i.e. smartphones, laptops)* that are utilised for business purposes are to be given to the **[IT Team/Named Person/IT Manager]** to ensure that effective, adequate and up to date anti-virus and malware software has been installed and correctly configured
- [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
  - [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

5 RESPONSIBILITIES

It is the responsibility of the **[IT Team/Named Person/IT Manager]** to oversee; implement; configure; monitor and maintain all anti-virus and malware software applications. However, all users are expected to understand the importance of preventing access to devices from malicious sites or email attachments and are responsible for following the objectives in this policy.