ISO/IEC 27001:2013 Information security management systems
-Protection from malware-

Security category – 12.2. Protection from malware

Control – 12.2.1. Controls against malware
The organization should have detection, prevention and recovery controls to protect against malware and they should be combined with appropriate user awareness.

ISO/IEC 27002 recommends protection against malware to be based on detection and repair software, awareness, system access control and controlled change management.

ISO/IEC 27001:2013 Information security management systems
-Protection from malware-

Guidance on protection from malware:

- define a policy to prohibit the use of unauthorized software and implement controls to detect the use of such software;
- blacklist suspected malicious websites and prevent their use;
- have a policy aimed to protect against risks associated with obtaining files and software from or via external networks;
- use and regular update of malware detection and repair software and scan computers and media on a regular basis;
- have some plans to recover from malware attacks;
- keep in touch with latest information on malware attacks;
- isolating environments where malware infection can lead to catastrophic impacts for the organization - if there are such environments.

For systems where sensitive information is being processed, the use of more than one vendor's antivirus software may improve detection rate.