



Information security policy

Malware

Policy summary

Malware is a serious threat to our data, IT systems and networks, therefore effective malware controls are essential. Approved antivirus software must run continuously on all relevant systems, and be updated frequently. Further technical and procedural controls are necessary to address malware risks, including effective business continuity management in case of serious infections.

Applicability

This policy applies throughout the organization as part of the corporate governance framework. It is particularly relevant to IT users and administrators, and applies to all computing and network platforms. This policy also applies to third parties acting in a similar capacity to our employees whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies.

Policy detail

Background

This policy concerns computer viruses, network worms, Trojan horse programs, rootkits, key loggers, trapdoors, backdoors, adware, spyware, crimeware *etc.*, collectively termed “malware” (a contraction of malicious software). Malware poses a serious threat to the organization’s information assets because it is:

- Commonplace, highly variable and surreptitious, hence difficult to detect and block;
- Technically advanced, hence difficult to eradicate and capable of undermining or negating many forms of security control; and
- Potentially highly damaging, affecting the information security (confidentiality, integrity and/or availability) of information and perhaps causing serious consequences such as adverse commercial, privacy and safety impacts.

Malware is being actively developed, traded and used by:

- Individuals for personal reasons (such as spying on their partners and work colleagues or accessing confidential proprietary information);
- Criminals to commit fraud, identity theft, information theft, coercion, blackmail, sabotage *etc.*;
- Unethical adversaries to commit industrial espionage, steal intellectual property, sabotage business processes and commercial bids *etc.*; and
- Hackers, journalists, private investigators, law enforcement, the security services and others for various reasons including “national security” and, potentially, cyberwarfare.

Policy axiom (guiding principle)

Complementary layers of protection must be used to counter malware:

- All reasonable steps must be taken to **prevent** malware infections, including both technical/automated and procedural/manual controls; and
- Appropriate **detective** and **corrective** controls must also be in place to identify and minimize the impacts of malware infections that are not in fact prevented by the preventive controls.

Detailed policy requirements

1. Points on the network perimeter through which malware can enter the organization from outside should be limited and controlled, yet without unduly interfering with legitimate network use. Only IT-approved network firewalls may be used, for example.
2. Further controls are necessary to prevent or at least limit the infection and spread of malware within the organization, and prevent (as far as possible) malware leaving the organization by any route including network connections and computer storage media.
3. Emails traversing the email gateways (both inbound and outbound) must be automatically scanned for malware using IT-approved email antivirus software. Any infected messages must be quarantined pending review and disinfection or deletion by suitable IT professionals.
4. Executable attachments (including those inside archives such as zip files) should be routinely blocked or stripped from both inbound and outbound emails at the email gateways. Given legitimate business needs, email users can request that executable attachments are virus scanned and released from quarantine if uninfected.
5. All computers should be configured, maintained, monitored and patched to minimize operating system and application vulnerabilities, including those that could lead to malware infections. Critical security patches should be applied as soon as practicable (but after successful testing).
6. IT-approved antivirus software must run continuously on all applicable IT systems (e.g. PCs, servers, laptops, PDAs and smartphones), automatically scanning fixed and removable storage media and negating any malware detected. Malware signature files should be updated as often as practicable, ideally by direct download from the antivirus software vendors. In the case of IT systems supporting critical business processes, the corresponding Information Asset Owners may however insist that antivirus updates are routinely tested prior to implementation if the risks of inappropriate changes outweigh the risks of malware infection and compromise.
7. Computer media believed to carry a significantly greater risk of malware infection, including all data storage media (both originals and backups) associated with an infected system and/or its users, should be virus-scanned and ideally disinfected on an isolated and safe test environment.
8. Software intended for business-critical systems may have to be reviewed in detail by technically competent and independent persons for malware if the corresponding Information Asset Owners require it. Further risk analysis and preventive measures may be appropriate within the software development, testing, implementation and maintenance processes. This requirement applies to new software developments and to updates, patches or maintenance releases, whether developed externally or in-house, and allows for code reviews to occur at any time (e.g. by scanning source code libraries/databases for malicious embedded functions).
9. IT users, IT system administrators, IT Help/Service Desk and other IT support staff must be informed of and remain alert to the malware risk through suitable awareness, training and educational activities, guidelines and procedures.
10. Automatic file integrity checks should be used routinely to monitor file systems on critical IT systems for unauthorized changes, including those resulting from malware infections.

11. Trustworthy software installation media (ideally the original CD- or DVD-ROMs, or checksum-verified downloads direct from the software vendors) should be retained to enable re-installation of operating systems and application programs in the event that this is the only means of recovery.
12. Regular data backups should be taken to off-line storage media at frequencies determined by the backup policy, Information Security Management and/or the applicable Information Asset Owners. Backups should be retained for *at least* three months to facilitate recovery of uninfected data files if malware infections are subsequently determined*.
13. Contingency measures must be prepared and maintained by IT to deal appropriately with malware outbreaks, covering aspects such as initial notification, response, escalation and resolution of incidents, declaration of a disaster and invocation of the contingency plans, and of course the contingency measures themselves (e.g. network and/or system isolation, additional malware and configuration checks, 'cleansing' and reinstallation of systems etc.).
14. Malware incidents and related 'near-misses' must be recorded by IT Help/Service Desk for statistical reporting and continuous improvement purposes. Post-incident reviews should be completed to analyze significant malware infections and any others where management feels it appropriate and worthwhile to examine control weaknesses and where necessary improve preventive, detective and/or corrective malware controls.
15. Anybody who deliberately or carelessly interferes with the correct operation of antivirus and related malware controls may be subject to disciplinary procedures or legal measures, particularly if their actions significantly increase the risk of malware infections or actually lead to an infection that causes significant damage.

Responsibilities

- **Information Security Management** is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also responsible for running educational activities to raise awareness and understanding of the obligations identified in this policy.
- **IT Department** is responsible for determining requirements, reviewing, approving, installing, configuring, monitoring and maintaining antivirus software and other technical antivirus controls.
- **IT Help/Service Desk** is responsible for defining and operating the malware incident response procedures in conjunction with various IT technical support staff and Information Security, as well as providing first line support for IT users regarding malware support issues and concerns.
- **All relevant employees** are responsible for complying with this and other corporate policies at all times, for example by using properly and not interfering with the antivirus controls outlined in this policy.
- **All relevant employees** are responsible for complying with this and other corporate policies at all times.
- **Internal Audit** is authorized to assess compliance with this and other corporate policies at any time.

* Note: in most cases, business requirements for backups and archives will be substantially longer than the three-month minimum noted here.

Related policies, standards, procedures and guidelines

Item	Relevance
Information security policy manual	Defines the overarching set of information security controls reflecting ISO/IEC 27002 , the international standard code of practice for information security management
Standard on antivirus controls	Provides technical details about the antivirus software and other primarily technical antivirus control measures
Information security incident reporting and response procedures	Instructions for reporting incidents via the IT Help/Service Desk, and handling them through to resolution and learning-the-lessons
Business continuity management policies and procedures	Malware-related incidents may be common and serious enough to make it worth documenting specific resilience and recovery arrangements (e.g. keeping secure offline backups/archives of all software, permitting systems to be rebuilt from scratch if necessary), as well as all-purpose contingency plans
Network and system security policies and procedures	Concerns security controls both at the network perimeter and within our internal networks, such as firewalls and intrusion detection systems
Data backup and archival policy and procedure	Describes corporate requirements for securely retaining off-line copies of important files that may be needed to recover from malware infections
Information security awareness materials	Briefings and guidelines are available to help you implement and comply with this policy

Contacts

For further information about this policy or general advice on information security, contact the IT Help/Service Desk. Security standards, procedures, guidelines and other materials supporting and expanding upon this and other information security policies are available on the intranet **Security Zone**. The Information Security Manager can advise on more specific issues.

If you think your system may be infected by a virus, don't panic! Contact the IT Help/Service Desk straight away and take their advice. They know how to deal with viruses, Trojans *etc.* and will help you check and fix your system, if necessary calling out the incident response team. *Please* do not try to diagnose or fix it yourself as you may make things worse.

Important note from IsecT Ltd.

This policy is unlikely to be entirely sufficient or suitable for you without customization. This is a generic model or template policy incorporating a selection of common controls in this area derived from our knowledge of good security practices and international standards. It does not necessarily reflect your organization's specific requirements. We are not familiar with your particular circumstances and cannot offer tailored guidance. It is not legal advice. It is meant to be considered by management as part of the security awareness program, ideally as part of the regular review and update of your information security policies.