Information security policy

Malware (malicious software)

Policy summary

Malware is a serious threat to the organization, therefore effective malware controls are essential. Where technically feasible, approved antivirus software must run continuously on all relevant devices, and be updated frequently. Further technical and procedural controls are necessary to address malware risks, including effective incident response, backups and other business continuity arrangements 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 party employees working for the organization 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, keyloggers, trapdoors, backdoors, adware, spyware, crimeware, scareware, ransomware *etc.*, collectively known as "malware" (a contraction of **mal**icious soft**ware**).

Malware poses a serious threat to the organization because it is commonplace, highly variable, very difficult to detect and – in some cases – almost impossible to block. Modern malware is so technically advanced (*e.g.* remotely controlled, reconfigurable and capable of being redirected to attack multiple targets) that we cannot completely rely on preventive and detective controls. Worse still, malware incidents can be highly damaging, affecting the security of business information leading to serious consequences such as business interruption, privacy breaches and other compliance failures, loss/theft/devaluation of intellectual property, extortion, theft from online bank accounts and safety failures.

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, government agencies and others for various reasons including national security and, potentially, cyberwar.

Policy axiom (guiding principle)

Complementary layers of protection must be used to counter malware:

- All reasonable steps must be taken to **avoid** and **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 avoided or prevented by the other 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. Personally-owned ICT devices may only be used for business purposes if duly authorized under the corporate BYOD (Bring Your Own Device) scheme. MDM (Mobile Device Management) software must be installed and configured to permit remote management of BYOD devices by IT, and where applicable corporate antivirus software must be used and maintained.
3. 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 data storage media.
4. 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.
5. Executable attachments (including those inside archives such as zip files, or with non-standard file extensions) 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.
6. All ICT devices 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 following successful testing. End-of-life software that is out of support and no longer maintained or patched by the supplier should be retired from service.
7. Wherever technically possible, IT-approved antivirus software must run continuously on all applicable IT systems (*e.g.* desktop PCs, servers, laptops, tablets, smartphones and *things*), automatically scanning fixed and removable storage media and isolating 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 or Risk 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.
8. 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, wiped to a forensically sound standard, or physically destroyed.

9. 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 or Risk 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).
10. IT users, IT system administrators, Help Desk workers and other IT support staff must be informed of and remain alert to the malware risk through suitable awareness, training and educational activities, including guidelines and procedures supporting this policy.
11. Workers who discover or suspect malware incidents must report them without delay to the Help Desk and await further instructions.
12. Strong incident management and business continuity arrangements (including resilience, recovery and contingency aspects) are essential in case of serious malware infections, outbreaks and incidents arising. Although these arrangements are being used routinely to some extent, handling relatively minor malware incidents and concerns, realistic exercises must be held periodically to simulate and rehearse the response to more serious incidents involving malware.
13. It is particularly important that workers **do not** disclose or discuss malware incidents with outsiders unless explicitly authorized (*e.g*. official press releases and briefings). To minimize unnecessary stress and anxiety, informing the news media and various concerned parties is best handled as an integral part of the incident management process, at the appropriate point. Until then, say nothing and refer all queries to the Help Desk or Public Relations.
14. Automatic file integrity checks should be used routinely to monitor file systems on critical IT systems for unauthorized changes, including those potentially indicating malware infections.
15. Trustworthy software installation media (ideally the original CD- or DVD-ROMs, or checksum-verified downloads direct from software suppliers) should be retained to enable re-installation of known-good operating systems and application programs in the event that this is the only means of recovery.
16. 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 or Risk Owners. Backups should be retained for *at least* three months to facilitate recovery of uninfected data files if malware infections are subsequently determined[*].
17. Suitable business continuity arrangements must be in place in case of serious incidents or disasters involving malware, covering resilience, recovery and contingency aspects.
18. Malware incidents and related near-misses must be recorded by Help 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.

[*] Note: in most cases, business and compliance requirements dictate that backups and archives be retained for substantially longer than the three-month minimum noted here, sometimes for years.

19. 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.
- **Help 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.
- Specialists from **Risk Management, Incident Management, Business Continuity, Compliance, Public Relations** *etc*. have particular rôles in both implementing and maintaining this policy.
- **Workers** are personally accountable for complying with applicable policies, laws and regulations at all times. Workers who use corporate IT systems or their own IT systems under the BYOD (Bring Your Own Device) scheme are responsible for using, and not interfering with, the antivirus controls outlined in this policy. Prior to any official disclosures, workers must not disclose or discuss malware incidents outside the organization unless explicitly authorized to do so.
- **Internal Audit** is authorized to assess compliance with this and other corporate policies at any time.

Related policies, standards, procedures and guidelines

Item	Relevance
Information security policy manual	Describes the organization's Information Security Management System and a suite of information security controls based on the good security practices recommended by ISO/IEC 27001 and ISO/IEC 27002
Standard on antivirus controls	Provides technical details about the antivirus software and other primarily technical antivirus control measures
Security policy on BYOD	Specifies security controls such as remote management, antivirus software, backups and patching on personally-owned ICT devices used for work

Item	Relevance
Policies, standards and procedures on network and system security, access control and information integrity	Concerns security controls both at the network perimeter and within our internal networks (*e.g.* firewalls and intrusion detection systems) and systems (*e.g.* system integrity checking) used to protect them against, detect and/or recover from malware infections
Policies and procedures for security incident reporting and management	Malware incidents should be reported urgently to the Help Desk; incidents will be managed and resolved promptly by the experts
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 and preparations
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	Additional information and guidance to help implement and fulfil the requirements of this policy

Further information

For general advice on information security including malware, contact the Help Desk or browse the intranet *Security Zone*. Contact Information Security or IT for more specific advice and assistance.

If you think your device may be infected by a virus, don't panic! Contact the Help Desk straight away and take their advice. They know how to diagnose common viruses, Trojans *etc*. and if appropriate will call out the Incident Response Team or PC Support. *Please* be patient and do not try to diagnose or fix it yourself as you may make things worse.

Tip: if for some reason the Help Desk cannot be reached, the safest first step is to disconnect an infected device from the network *e.g.* by removing the network cable. If you are unable to turn off wireless networking on an infected portable, shut it down normally or remove the power (you may need to disconnect the battery).

Important note from IsecT Ltd.

This is neither legal nor security advice. It is a generic policy template that does not reflect your organization's particular information security risks, control requirements and constraints.