Malware Policy

Policy Summary

Malware is a serious threat to the organisation; 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 organisation 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 organisation whether they are explicitly bound (*e.g.* by contractual term and conditions) or implicitly bound (*e.g.* by generally held standards of ethics and acceptable behaviour) 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, scareware, ransomware etc., collectively known as "malware" (a contraction of malicious software).

Malware poses a serious threat to the organisation because it is commonplace, highly variable and surreptitious. It is difficult to detect and block. Modern malware is technically advanced, making it difficult to eradicate and capable of undermining or negating many forms of 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, 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, identify 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, cyber war.

Policy Axiom

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 minimise 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 organisation from outside should be limited and controlled, yet without unduly interfering with the 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 organisation, and prevent (as far as possible) malware leaving the organisation 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. A suitable IT professional must carry out disinfection or deletion.
4. Executable attachments (including those inside archive files 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 minimise 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. Software that is out of support and is no longer maintained or patched by the supplier should be retired from service.
6. Wherever technically possible, IT-approved antivirus software must run continuously on all applicable IT systems (e.g. PCs, servers, laptops, tablets, smartphones and any other portable device), 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 preventative 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 systems 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. Workers who discover or suspect malware incidents must report them without delay to the Help Desk and await further instructions.
11. It is particularly important workers do not disclose or discuss incidents with outsiders unless explicitly authorised (e.g. official press releases and briefings). To minimise unnecessary stress and anxiety, informing the new 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.
12. Automatic file integrity checks should be used routinely to monitor file systems on critical IT systems for unauthorised changes, including those resulting from malware infections.

13. Trustworthy software installation media (ideally the original CD-or DVD ROMs, or checksum-verified downloads direct from the 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.
14. 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*.
15. Suitable business continuity arrangements must be in place in case of serious incidents or disasters involving malware, covering resilience, recovery and contingency aspects.
16. Malware incidents and related near misses must be recorded by the Help Desk, for statistical reporting and continuous improvement purposes. Post-Incident reviews should be completed to analyse significant malware infections and any others where management feels it appropriate and worthwhile to examine control weaknesses and where necessary improve preventative, detective and/or corrective malware controls.
17. 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 roles 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 organisation unless explicitly authorised to do so.
- **Internal Audit** is authorised to assess compliance with this and other corporate policies at any time.

Signed Dr Adnan Niazi

Date 4/1/2021
Last Reviewed On 05/07/24

Version 1