MALWARE

General Overview

Malicious software, commonly known as malware, is a general expression used by many within information security to describe software created and/or used for the purposes of harming and damaging various systems, such as computer code, files, applications, and other relevant information technology platforms and utilities. Additionally, malware is viewed as a hostile and often intrusive software or program code that can seriously impact the confidentiality, integrity, and availability (CIA) of one's overall information technology architecture. It's a serious threat that continues to grow more and more, requiring significant resources from all parties (i.e., vendors who sell "anti-malware products and services, along with organizations that must constantly protect their systems) regarding effective malware initiatives and solutions. A core component of any organization's information security practices is using anti-malware solutions, most notably anti-virus, but there are also numerous ant-malware software products being offered by many vendors today.

At any rate, the goal of a comprehensive malware program is one that includes highly effective software solutions for fighting this never-ending battle, along with having in place a comprehensive well-written malware policy, specifically, an Anti-Virus and Anti-Malware Policy and Procedure document. As for the various types of malware, common examples include the following: viruses, worms, Trojan horses, rootkits, adware, spyware, rogue security software, keyloggers, dialers, and others. Add to the mix of 0 day virus threats (a previously unknown computer virus or other type of malware in which anti-virus software signatures are not yet available), and one can clearly see the importance of having in place a comprehensive anti-malware platform. Lastly, while most malware attacks are targeted on Microsoft Windows platforms, users of UNIX and Linux systems should nonetheless be taking proactive steps in securing their systems, with the use of anti-virus software and other supporting malwares products.

In summary, anti-malware initiatives – specifically those related to the use of antivirus software – is a relatively simple and straightforward concept to deploy within organizations – and one that yields sizeable security benefits. Because most I.T. security professionals associate the topic of malware with the use of antivirus, the below referenced policy will called such – Antivirus and Anti-Malware Policy and Procedures.

Antivirus and Anti-Malware Policy and Procedures

Title	**[company name] Antivirus and Anti-Malware Policy and Procedures**
Version	Version 1.0
Date	TBD
Language	English
Individual and/or Department Responsible for Distribution of Document	[company name] Information Technology Department
Individual and/ or Department Responsible for Timely Update of Document	[name and title]
Developed by:	[company name]
Subject	Use of Software
Approval Date	TBD
Purpose of Document	To implement comprehensive antivirus and anti-malware policies, procedures, and practices whereby all employees and other intended parties are readily aware of the organization's malware policies.
Distribution of Document	Disbursed to all employees of [company name] and available by request to all other intended parties.

1.0 Overview

In accordance with mandated organizational security requirements set forth and approved by management, [company name] has established a formal Antivirus and Anti Malware policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on a(n) [annual, semi-annual, quarterly] basis for ensuring its adequacy and relevancy regarding [company name]'s needs and goals.

1.0 Purpose

This policy and supporting procedures are designed to provide [company name] with a documented and formalized Antivirus and Anti Malware policy that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of [company name] system resources. Malicious software, commonly known as malware, is a general expression used by many within information security to describe software created and/or used for the purposes of harming and damaging various systems, such as computer code, files, applications, and other relevant information technology platforms and utilities. Additionally, malware is viewed as a hostile and often intrusive software or program code that can seriously impact the confidentiality, integrity, and availability (CIA) of one's overall information technology architecture.

As such, a core component of [company name]'s information security practices is using anti-malware solutions, most notably anti-virus, along with other anti-malware software. Ultimately, the goal of a comprehensive malware program for [company name] is one that includes highly effective software solutions for fighting this never-ending battle, along with having in place a comprehensive well-written malware policy, specifically, an Antivirus and Anti Malware Policy and Procedure document. The subsequent policies and procedures relating to antivirus initiatives for [company name] strive to ensure the overall confidentiality, integrity, and availability (CIA) of the organization's network.

1.0 Scope

This policy and supporting procedures encompasses all system resources that are owned, operated, maintained, and controlled by [company name] and all other system resources, both internally and externally, that interact with these systems.

- Internal system resources are those owned, operated, maintained, and controlled by [company name] and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system resources deemed in scope.

- External system resources are those owned, operated, maintained, and controlled by any entity other than [company name], but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "Internal system resources".

- Please note that when referencing the term "antivirus" and/or "anti-malware", this pertains to the following three (3) core components: (1). The actual vendor supplied antivirus and/or anti

malware software solution(s). (2). System resources for which the antivirus and/or anti malware software solution(s) reside on for purposes of enterprise-wide administration (i.e., AV Server). (3). All "hosts" for which antivirus and/or anti malware mechanisms are deployed onto, such as servers, desktops, laptops, other workstations, etc. Thus, the below referenced policies and supporting procedures have been designed to effectively address various operational, technical, and security measures regarding antivirus and anti-malware initiatives.

- When referencing the term "users", this includes any individual that has been granted access rights by [company name] to various system resources and has went through all required provisioning steps. Users typically include, but may not be limited to, the following: employees, consultants, vendors, contractors, along with local, state, and federal personnel.

- For purpose of this policy, antivirus is defined as the following: Software used for purposes of preventing, detecting, and removing malicious software (i.e., malware), such as computer viruses, worms, trojan horses, etc. Additionally, antivirus is software also used for preventing and removing adware, spyware, and other forms of malware.

1.0 Policy

[Company name] is to ensure that the Antivirus and Anti Malware policy adheres to the following conditions for purposes of complying with the mandated organizational security requirements set forth and approved by management:

Definitions
For purpose of this document, please refer to the following terms and related definitions for more information pertaining to a specific subject:

- **Computer Virus:** A computer program that has the ability to replicate itself and spread from one computer to another. Common viruses include, but are limited to, the following: polymorphic virus, boot virus, macro virus, multipartite virus, web scripting virus, etc.
- **Malware:** Software created and/or used for the purposes of harming and damaging various systems, such as computer code, files, applications, and other relevant information technology platforms and utilities.
- **Antivirus:** Software used for purposes of preventing, detecting, and removing malicious software (i.e., malware).
- **Worms:** A standalone, independent program that has the ability to replicate itself and spread to other computers, ultimately infiltrating programs and destroying data.
- **Trojan Horse:** A harmful piece of malware that facilitates unauthorized access on a computer system by way of social engineering tactics and strategies.
- **Keyloggers:** Unauthorized capturing of a user's keystrokes on a computer system. Note: It is considered malware when it is "unauthorized", as there are legitimate uses of keylogging software.
- **Rootkits:** Software that enables unauthorized access to a computer system and that is also hidden from detection. Rootkits can conceal the altering of files, data, etc. and are a serious form of malware.
- **Spyware:** Software that collects vital information from a computer system regarding data on such system and the associated user activities. Note: It is considered malware when it is "unauthorized" as there are legitimate uses of spyware.

- **Adware:** Programs that facilitate delivery of advertising content and related material to a user through their browser while on the Internet, or through some other type of interface. Note: It is considered malware when it is "unauthorized" as there are legitimate uses of adware.
- **Logic Bomb:** Code that is intentionally inserted into a software system that initiates a malicious function when specified conditions are met.

Essential Anti Malware Detection and Containment Measures

Anti-malware initiatives consist primarily of "detection" and "containment", both of which must be utilized at all times for ensuring the safety and security of [company name] system resources. As for "detection" measures, these consist of using approved antivirus software and other supporting utilities that effectively recognize and detect malware, such as signatures, virus dictionaries, and other policy based recognition. Additionally, the use of behavior based heuristics, and possibly File Integrity Monitoring (FIM) tools are extremely useful also. As for "containment" measures, this is a combination of software safeguards imbedded into the anti-malware solutions, along with users acting proactively in discontinuing the use of an affected system resource, and removing it from the [company name] network altogether.

Antivirus Software Deployment and Distribution

The most important component of any anti-malware initiative for [company name] is the use of anti-virus software on all system resources, such as internal servers, user workstations, along with laptops and other applicable devices. As for the antivirus software itself, it must employ a combination of security measures, such as signature based-detection, heuristics, rootkit detection, along with "real-time" protection. Specifically, antivirus signatures are to be updated automatically and pushed out to all system resources, necessary analysis is to be undertaken for identifying new malware or variants of known malware, while also employing immediate scanning of specific devices for malware. Additionally, antivirus is to be distributed in an efficient, yet expedited manner to all system resources, from initial install for new systems, to automatic updates to existing systems.

The best avenue for distribution of antivirus is a centralized platform consisting of stand-alone antivirus server that effectively "pushes" out all updates to the corresponding host machines. For any standalone machines outside the scope of the centralized antivirus platform, updates must be made accordingly. Antivirus software configured on all hosts must not be altered in any way by end users, and authorized I.T. personnel at [company name] are to configure the antivirus settings in such a manner for ensuring such security. Lastly, a computer may not be connected to the network if it does not have antivirus installed on it.

Antivirus Service and Support

Any antivirus solutions utilized by [company name] must be from an approved vendor, one that offers ongoing customer support pertaining to the installation and maintenance of the applicable software. Specifically, this includes all necessary installation documentation (i.e. manuals, user administrator and setup guides, hardening guides, etc.), "virus support" initiatives, such as providing updates for new detection signatures and the applicable dictionaries, etc. Additionally, the vendor is to also provide training material, and any other helpful documentation for ensuring all [company name] antivirus initiatives are being provided as contracted.

Additional Anti Malware Solutions

Antivirus is without question the foundation for any anti-malware platform, but there are additional software solutions that can greatly assist in such endeavors, such as anti-spyware, and others, thus

[company name] is to utilize such tools as necessary for ensuring the safety and security of system resources. These tools are to go through a comprehensive analysis by authorized I.T. personnel before being placed into any such environments.

Security Awareness Training

Proper security awareness training regarding anti malware initiatives helps ensure that all users understand the basic tenants of malicious software, the intent of it, how it works, and the security measures in place for eliminating such malicious software. The more educated and informed users are on this critical subject, the greater the opportunity for identifying perceived or actual malware threats to [company name]. As such, all security awareness training initiatives undertaken by [company name] are to include provisions for educating all users on the broader subject of malware and the applicable anti malware practices in place.

External Media

External media, such as portable storage devices, and other devices that connect via USB ports are strictly forbidden as viruses can easily enter into the [company name] network from such mediums. If in rare cases external media are an absolute necessity, the applicable devices should be plugged into a test | development server, so that that it may be scanned for any possible malware.

Antivirus Logs

An important component of [company name]'s malware initiatives is the ability to effectively understand the associated threats and attacks, such as the viruses and other malicious files blocked by the antivirus solution and other malware utilities. Comprehensive review of such logs allows authorized I.T. personnel to better assess the future threats and all other associated conditions that may impact the confidentiality, integrity, and availability (CIA) of [company name] system resources. Thus, antivirus logs containing malware incidents are to be to be reviewed on a regular basis, with the following information contained within the actual logs: (1). Date. (2). Location. (3). Malware Name. (4). Associated "actions", "status", etc. of the virus.

Mail Server Security

[Company name] mail servers are to be configured will all necessary mail anti malware solutions, such as antivirus and anti-spam, along with other essential utilities for effectively blocking and containing email born viruses and other malware threats. Specifically, all email communications and web browsing for webmail must be sent through the applicable email filtering systems for ensuring file extensions that are known to contain malware, such as .vbs, .dat, .exe, .pif. .scr, are blocked. Additionally, many commonly used file extensions can also contain malware, thus use caution at all times when opening, saving attachments, or forwarding them also.

Network Security Architecture and Practices

While anti malware software solutions such as antivirus, anti-spyware and anti-spam are highly effective in detecting and containing virus and other exploits, [company name] also understands the fundamental importance of a secure network architecture, along with highly formalized, and documented operational and information security policies and procedures. Specifically, firewalls, routers, switches, Intrusion Detection Systems | Intrusion Prevention Systems (IDS | IPS), load balancers, web servers, and all other supporting system resources are to properly provisioned, hardened, secured and locked-down for further ensuring the confidentiality, integrity, and availability (CIA) of [company name]'s network.

Additionally, following best practices for change control, user provisioning and de-provisioning, and many other common operational and security practices further ensures the safety and security of [company name] system resources. Using a Defense-in-Depth approach – one that relies on a multitude of systems and supporting security initiatives for protecting an organization's network – is to be a cornerstone of [company name] security's practices.

Software Downloads

Downloading of software from the Internet onto [company name] system resources is strictly forbidden unless such software has been approved and deemed safe by authorized I.T. personnel. Very often, downloads contain dangerous malware that may be initially undetected. Common software forbidden includes the following: software advertised and claiming to be free, software from unknown and untrusted sites, software received via email from known and/or unknown parties, software that is unlicensed, software received at trade shows, conferences, or other social or professional forums or gatherings.

Incident Response Measures

Timely communication is initially the most effective incident response measure to take regarding perceived or actual malware threats to [company name]. Authorized I.T. employees responsible for the administration of all anti malware initiatives are to inform users of any real-time threats and the relevant safeguards to implement as threats can occur anytime. Additionally, should a user suspect a malware threat, the following steps are to be undertaken immediately:

- Immediately notify authorized I.T. personnel and inform them of the situation.
- Follow all instructions and guidance as given to a user from such I.T. personnel.
- If no immediate I.T. personal are involved – because of outside of normal business hours or communication constraints, discontinue the use of the system resource in question.
- Provide the system resource in question – such as a laptop or other device – to authorized I.T. personnel for forensic inspection.
- Assist in facilitating the completion of an official "Incident Response Form" regarding the malware threat.
- Undertake measures on the affected system resource for removing all viruses, which may include reformatting procedures, along with possible physical destruction of critical devices (i.e., hard drive, etc.), or the entire system altogether.

Note: Common examples of malware threats include the following: error messages, continuous pop-up advertisements, system performance issues, actual anti-virus warnings, alerts, and other suspicious activities.

Continuous Monitoring for Compliance

[Company name] malware practices are only as good as the initiatives in place for ultimately ensuring the aforementioned policies are adhered to by all appropriate users, both end-users, and authorized I.T. personnel. Specifically, this requires a collaborative effort by all parties – from end-users who clearly understand the importance of the organization's malware initiatives, to I.T. individuals responsible for administering the entire anti malware platform. As such, monitoring and compliance initiatives include a wide-range of practices, conducted by both internal audit personnel, along with possible external entities, such as auditors performing compliance engagements.

Best Practices Measures

As with anything in information security that pertains to the confidentiality, integrity, and availability (CIA) of [company name] system resources, promoting best practices is a critical element of a layered, defense-in-depth approach. As such, the following best practices relating to anti-malware initiatives are highly recommended:

- Authorized I.T. personnel are to undertake a comprehensive analysis for ensuring that [company name] has acquired the best possible anti-malware software solutions, which include antivirus, antispyware, and other necessary utilities. Furthermore, the applicable solutions are to be evaluated on an annual basis for ensuring their adequacy and sufficiency.
- All [company name] system resources that require antivirus must in fact have the latest updates (i.e., virus signatures) on these respective devices, such as auto update features.
- If you are unsure of an email or its accompanying attachment, do not open it under any circumstances.
- If you have suspected your computer or any other related system resource has been affected by malware, stop using the system immediately and notify personnel.
- Use sound judgment – if something looks or seems suspicious and you think its malware and poses a security threat, then stop using the affected system resource immediately and contact authorized I.T. personnel immediately.

1.0 Procedures

[Company name] has developed and implemented a comprehensive antivirus and anti-malware process, which encompasses the following categories and supporting activities listed below. These policy directives will be fully enforced by [company name] for ensuring the antivirus and anti-malware initiatives are executed in a formal manner and on a consistent basis for all specified systems.

Note: The "Policy" sections contained within this specific policy and procedure document simply state general best-of-breed practices that should be in place. However, the "Procedures" sections list and describe the actual steps to undertake for ensuring compliance with the aforementioned policies. As such, look upon the policies as statements, formal guidelines, and the general framework for a particular subject matter.