Navigatr Group

Anti-virus and Patch Management Policy

This report contains 7 pages

Revision History

Version	Author	Date	Revision
1.0	Norm Crooks	4th August 2014	Initial document created.
2.0	Norm Crooks	12th October 2016	Media policy added
3.0	Norm Crooks	12th March 2018	Rebranded

This Document Has Been Reviewed By

	Reviewer	Date reviewed
1	Norm Crooks	8th August 2014
2	Norm Crooks	15th September 2014
3	Norm Crooks	6th October 2015
4	Norm Crooks	12th October 2016
5	Norm Crooks	12th March 2018
6	Norm Crooks	9th June 2020

This Document Has Been Approved By

	Name	Signature	Date reviewed
1	John Hiscock (COO)		20th October 2016
2			
3			
4			
5			

Contents

1 Introduction 1
1.1 Purpose 1
1.2 Scope of the policy 1

2 Antivirus policy 2

3 Removable Media Policy 3

4 Patch Management Policy 5

5 Discovering and reporting security problems 6

6 References 7

1 Introduction

1.1 Purpose

This primary purpose of this document is to provide policy and guidelines/standards protect Navigatr Group against the introduction of viruses and other types of malicious code that can jeopardize information security by contaminating, damaging, or destroying information resources.

This policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of e-mail system at Navigatr Group;
- to prevent infection of Navigatr Group computers and networks by computer viruses and other malicious code and intended to prevent major and widespread damage to assets such as the network, user applications, files, and hardware; and
- To educate staff on risk posed by virus and related malicious code and ensure all users use anti-virus software with respect to their use of IT systems.
- To maintain the integrity of software within Navigatr Group, network environment through a well-defined patch management program.
- To ensure the Patch management process is controlled for deployment and maintenance of interim software releases into production environments

1.2 Scope of the policy

This document addresses policies and guidelines/standards related to antivirus, removable media and patch management.

The following Navigatr Group ‘users’ are covered by this policy:

- Full or part-time employees of Navigatr Group;
- Navigatr Group contractors who are authorized to use company-owned equipment or facilities; and
- Other personnel who have been provided access to Navigatr Group e-mail services.

All users will familiarise themselves with this policy and any violation of this policy will lead to a disciplinary action as deemed appropriate by the Navigatr Group management.

2 Antivirus policy

It is the policy of Navigatr Group that:

- All machines will run the latest anti-virus software as approved by organization management.
- E-mail with attachments coming from suspicious or unknown sources will not be opened, nor will attachments be opened, links followed or other directions in the email followed. All such e-mails and their attachments will be deleted from the mail system as well as from the trash. No one should forward any e-mail which a/he thinks may contain virus.
- Note that modern phishing techniques are very sophisticated and emails may be crafted to appear legitimate, and on first glance may appear to come from a collegue or trusted source. Treat all attachments as potentially dangerous and if you do not know what the attachment of an email is do not open it.
- All removable media from outside the organization (e.g. floppy and others) will be scanned for viruses before being used.
- No pirated software will be used on the corporate network.
- In the case of a virus being found, your direct manager and the IT department will be informed immediately. The IT manager will investigate and take proper measures to avoid the event in future.
- All encrypted material will be decrypted and checked for viruses before being used.
- The e-mail Server will have the antiviral program installed and must check all of the e-mails attachment before sending it to individual mail box.
- All of the updates to the antiviral program will be automatic from the web or from the central server
- The email system will likewise employ a spam firewall (Mail Foundry, Barracuda, or the like)

3 Removable Media Policy

This policy must be followed to safeguard both personal and company information and represents a minimum standard.

- USB ports are essential for most personal computers and are universally allowed to support the connection of keyboards and mice.
- USB ports can also be used for approved peripheral devices.
- The following Removable Media Devices utilized in the workplace must be company owned and issued and likewise controlled through an authorized approval process: flash drives, external hard drives, memory sticks, writeable CD-ROM and floppy disks.
- The controls that apply to connecting devices by USB also apply to other methods of connecting these devices and failure to comply with such controls will also violate this policy. Examples of other connection methods include but are not limited to: Bluetooth, Infrared, Firewire, Serial/Parallel ports, Optical (CD/DVD/Blu-ray), eSATA, or SCSI. 3.
- The type of information stored on removable media is governed by the Data Classification contained in the Data Confidentiality Policy and may not include:

a) **Proprietary Company Data –** Proprietary company data is any information that derives its economic value from not being publicly disclosed. It includes information that Navigatr Group is under legal or contractual obligation to protect. The value of proprietary company information to Navigatr Group would be destroyed or diminished if such information were disclosed to others. Most Navigatr Group sensitive information should fall into this category. Proprietary company information may be copied and distributed within Navigatr Group only to authorized users. Proprietary company information disclosed to authorized external users must be done so under a non-disclosure agreement. (Examples of Proprietary company data include company policies, sales plans, and application source code etc.,.)

b) **Confidential Company Data** – Confidential Company Data is information that is not to be publicly disclosed, regardless of its economic value. The disclosure, use, or destruction of Confidential Company Data can have adverse effects on Navigatr Group and possibly carry significant civil, fiscal, or criminal liability. This designation is used much less frequently. It is used for highly sensitive information whose access is restricted to selected, authorized employees. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know for the information. Company confidential information must not be copied without authorization from the identified owner. (Examples of Confidential Company Data include company strategic plans or cryptographic keys.)

c) **Confidential Customer Data** – Confidential customer data is defined as data that only authorized internal Navigatr Group entities or specific authorized external entities can access. The disclosure, use, or destruction of confidential customer data can have adverse effects on Navigatr Group and their relationship with their customers, and possibly carry significant liability for both. Confidential customer data is entrusted to and may transit or is stored by Navigatr Group (and others) over which they have custodial responsibility but do not have ownership. (Examples of Confidential customer data including customer bank or brokerage account information, cryptographic keys, or other data considered private.)

- Removable Media containing any company data must not be taken off company property except in specifically approved cases, such as for off-site backup processes. Approval must be provided by the employee's direct manager and the V.P. Support & Infrastructure (at time of writing Norm Crooks) or COO (at time of writing John Hiscock).

4 Patch Management Policy

Information security advisory services and technology vendors routinely report new defects in software. In many cases, these defects introduce opportunities to obtain unauthorized access or disrupt services. Information about security exposures often receives widespread publicity across the Internet and other media, increasing awareness of software weaknesses, with the consequential risk that attacker could attempt to use this knowledge to exploit the vulnerable systems.

Patch management policy is essential to Navigatr Group. If the security patches are not applied, the potential risks of attack to exploit know vulnerabilities increases. Hence it the policy of Navigatr Group to ensure all patches are applied on time. The following activities will be followed to ensure adherence to the patch management policy.

Patch/Vulnerability management process including a desired defence/response measure and timeframe based on system criticality, vulnerability severity, exploit complexity, type and delivery of attack. At a minimum, this process includes:

- Monitoring for security vulnerabilities from security intelligence sources;
- Completing an impact assessment on new security vulnerabilities;
- Developing and testing the technical remediation strategy (e.g.: Patch identification);
- Implementing the technical remediation strategy on all affected systems;
- Reporting and tracking of remediation measures implemented; and
- Integrating the patch or configuration changes into the related security baseline and system build.

5 Discovering and reporting security problems

5.1.1 If sensitive, confidential, and/or private information is suspected to be lost or disclosed to unauthorized parties, the direct manager and IT Security Officer will be notified immediately.

5.1.2 If unauthorized use of Navigatr Group information systems has taken place or is suspected, the direct manager and IT Security Officer will be notified immediately.

5.1.3 All unusual systems behaviour, such as missing files, frequent system crashes misrouted messages, and other similar activities occur, the direct manager and IT Security Officer will be notified immediately

5.1.4 The specifics of any possible security problems will be kept confidential to immediate management and security personnel.

5.1.5 Users will not perform any security testing, nor use and possess tools for cracking information security unless express written permission is obtained.

6 References

https://www.us-cert.gov/ncas/alerts/TA16-091A
https://www.us-cert.gov/report-phishing