Navigatr Group

Email Usage and Security Policy

This report contains 11 pages

Revision History

Version	Author	Date	Revision
1.0	Norm Crooks	4th August 2014	Initial document created.
2.0	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 March 2018
5	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 Purpose

This primary purpose of this document is to provide policy and guidelines/standards for usage and management of e-mail system for Navigatr Group.

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 establish prudent and acceptable practices regarding the use of email; and
- To educate individuals on using email with respect to their responsibilities associated with such use.

This document is intended to provide guidance to end users to ensure e-mail services and operations remains secure and efficient while communicating within intranet as well as through internet.

All users should familiarise themselves with this e-mail usage policy and violation of this policy will lead to a disciplinary action.

1.2 Scope of the policy

This document addresses policies and guidelines/standards related to e-mail usage and management of e-mail System.

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 should familiarise themselves with this e-mail policy and any violation of this policy will lead to a disciplinary action as deemed appropriate by the Navigatr Group.

2 E-Mail usage and security policy

It is the policy of Navigatr Group

- To develop effective systems and procedures to ensure that e-mails are used as an efficient mode of business communication;
- To implement appropriate security control procedures so that e-mail facility is not misused; and
- To implement appropriate security management practices and controls when maintaining and operating a secure e-mail system.

In accordance with the above policy statement, this security policy has been established to provide good practices, procedures and controls over the e-mail usage and management.

Detailed security guidelines/standards for the e-mail usage and management of e-mail system are set out below.

3 E-mail usage guidelines

3.1 Individual usage

3.1.1 The e-mail service is to be used for business purposes as a productivity enhancement tool. Incidental personal use is permissible so long as it does not consume more than a trivial amount of resources, does not interfere with worker productivity, and does not pre-empt any business activity.

3.1.2 In no event should any user create or transmit e-mail messages that include offensive or personal material or material that could be considered as harassing, discriminatory, defamatory, disruptive, illegal, or criminal, or that involves obscene, vulgar, or sexually explicit content.

3.1.3 Electronic mail systems and all messages, including back-up copies, are property of Navigatr Group.

3.1.4 Unauthorized use of e-mail software is prohibited.

3.1.5 The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:

- Sending or forwarding chain letters via e-mail;
- Sending unsolicited messages to large groups except as required to conduct Travel Edge's business;
- Sending excessively large messages; and
- Sending or forwarding email that is likely to contain computer viruses or other malicious software.

3.1.6 Individuals should not send, forward or receive private, confidential or sensitive information through non-Navigatr Group email accounts. Examples of non-Navigatr Group email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).

3.1.7 Individuals should not send, forward, receive or store confidential or sensitive Navigatr Group information utilizing non-Navigatr Group accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants, two-way pagers and cellular telephones.

3.1.8 Confidential information (e.g. pincodes, passwords, proprietary company information, etc.) should not be sent via email in clear text. Such information should be transferred to the recipient in an encrypted format, or provisioned via a SFTP account.

3.2 Privacy

3.2.1 Employees should structure their electronic communications in recognition of the fact that Navigatr Group reserves the right, from time to time, to examine the content of electronic communications. Contractors should be aware that while their communications are not routinely reviewed, in the event that Navigatr Group is compelled by subpoena or other legal means to disclose the content of emails for a particular user of the system we will comply.

3.2.2 Navigatr Group cannot guarantee that electronic communications will be private. Users should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, electronic communications can be accessed by others in accordance with this policy.

3.2.3 Navigatr Group is responsible for its communication networks. It may be necessary to intercept or disclose electronic communications. Other logging and monitoring may take place in order to support operational, maintenance, auditing, and investigative activities. Navigatr Group is committed to respecting the rights of its employees, including their reasonable expectation of privacy.

3.2.4 All user activity on Navigatr Group's information resources is subject to logging and review.

3.3 Access control

3.3.1 Users are prohibited from allowing anyone else to use their electronic mail account (including family, friends, and other users).

3.3.2 Users should be assigned minimal privileges that will allow them to perform the tasks that are necessary to perform their duties. For instance, not all users will be allowed to add members to a Navigatr Group created and approved e-mail distribution list.

3.3.3 Users are prohibited from reading or attempting to read any other user's electronic communications (mail, calendars, and folders).

3.4 Confidentiality

3.4.1 Users should exercise caution when forwarding messages recognizing that some information is intended for specific individuals and may not be appropriate for general distribution.

3.4.2 Users should treat electronic mail as they would any other company communications. When an email is sent, both the sender and the reader should assure that the communications complies with normal communications guidelines such as proper etiquette excluding remarks that contain profanity, obscenities or derogatory remarks, even if made in jest. Content should be business related and should be encrypted when appropriate.

3.4.3 A legal recipient disclaimer should be automatically added to all external electronic mail messages.

3.4.4 All sensitive information transmitted over external network should be encrypted

3.5 Integrity

3.5.1 Users may not misrepresent or falsify their identity on the Internet or in any communication as related to Navigatr Group. The user name, organization and other company specific information should be included in the message or posting.

3.5.2 Users should refrain from opening electronic mail or suspect attachments from which they do not know the sender or when the subject of the message seems inappropriate. Users should not respond to the sender. Users, however, should notify their electronic mail administrator who will take appropriate action.

3.6 Storage/Retention

3.6.1 Mailbox sizes for user email accounts will be enforced as necessary to prevent critical production impacts. In compliance with the mailbox size policy, electronic messages stored on the network mail systems will be automatically deleted by systems administration staff after a certain period of time. Therefore, users should take the following precautions:

- Official records communicated through electronic mail should be identified, managed, protected, and maintained as long as needed for ongoing operations, audits, legal actions, or any other known purpose;
- Any electronic mail containing a formal approval or constituting any commitment by Travel Edge to any outside organization should be copied to the appropriate file or sent (in hard copy if required) to support accountability and audits; and
- Messages no longer needed for business purposes will be periodically purged by users from their personal electronic message storage areas, including personal and local folders.

3.7 Discovering and reporting security problems

3.7.1 If sensitive, confidential, and/or private information is suspected to be lost or disclosed to unauthorized parties, the concerned authorities should be notified immediately.

3.7.2 If unauthorized use of Navigatr Group information systems has taken place or is suspected, the concerned authorities should be notified immediately.

3.7.3 Whenever passwords or other system access control mechanisms are lost or are suspected to be lost, stolen, or disclosed, the concerned authorities should be notified immediately

3.7.4 All unusual systems behaviour, such as missing files, frequent system crashes misrouted messages, and other similar activities occur, the concerned authorities should be notified immediately

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

3.7.6 Users should not perform any security testing, nor use and possess tools for cracking information security unless express written permission is obtained.E-mail security standards

4 Mail system access privileges and administration

4.1.1 All changes to the mail system configuration will be approved and documented by the IT administrators.

4.1.2 Privileges to modify the configuration will be restricted to a few individuals with business need for these privileges.

4.1.3 The mail system's operating system passwords will be selected and maintained based on the Navigatr Group current password policy.

4.1.4 The mail system management will only be assigned to competent and trained technical staffs who are employees of Navigatr Group or contractors responsible for mail system management.

4.1.5 In case the mail system management is outsourced, a Non Disclosure Agreement (NDA) should be signed with the contractor or service provider and the NDA should be enforced.

4.2 Software updates and change control

4.2.1 All changes to the software and hardware will be in accordance with change management policy of the Navigatr Group and should be approved, tested and documented by the IT administrators before applied to the production environment.

4.2.2 The latest stable operating system that meets the security requirements should be used and configured.

4.2.3 The mail server system will be installed on dedicated machines, which perform no other function.

4.2.4 The mail system and operating system software will be updated regularly to fix known security vulnerabilities, to support new features that allow more advanced security policies or to improve performance. A risk assessment and a change request should be a part of the update process. The changes should be tested and approved before applied to the production environment.

4.2.5 The operating system of the mail system will be enabled with audit features for analysis of any attack, suspicious activities and malfunction in the operating system.

4.2.6 The access to the mail system from the internet will be restricted with appropriate filtering devices.

4.2.7 Navigatr Group will implement security mechanism to protect against:

- Viruses and other malicious code;
- Active content (e.g., ActiveX, Java Applets, JavaScript);
- Spam emails; and
- Extra large files might be parked for delivery at off peak hours.

4.3 Mail system configuration review and assessment

4.3.1 The mail system configuration will be reviewed regularly and verified for compliance with current Navigatr Group IT policy and procedures. All changes to the mail system configuration should be evaluated, documented and approved by the IT administrators.

4.3.2 Periodic vulnerability assessment and penetration testing should be performed to evaluate the effectiveness of the security configuration of the e-mail. The testing process should be approved and documented by the IT administrators.

4.4 Secure backup

4.4.1 The mail system configuration and user mailboxes will be backed up regularly in accordance with the Navigatr Group's backup policy.

4.4.2 The latest configuration files, operating system software and configuration procedures will be maintained.

4.5 Auditing

4.5.1 The mail system configuration and log files will be audited on a periodic basis. At a minimum, this audit process should include access privileges, user accounts, security controls, current administrative practices and adequacy of the deployed security measures.

4.5.2 These audits will be performed by technically proficient personnel other than those responsible for the administration of mail system.

4.5.3 The audit observations will be resolved in a timely manner as recommended in the Navigatr Group IT policy and procedures.

4.6 Physical and environmental security

4.6.1 Mail system will be placed in a physically secure room.

4.6.2 The physical access to the room and to the mail system will be formally logged in a log book for effective tracking of physical access.

4.6.3 The room that contains the mail system will be free of electrostatic or magnetic interference. Also the room should have controls for temperature and humidity.

4.6.4 For availability or criticality reasons, an uninterrupted power supply (UPS) will be installed.

4.7 Documentation

Appropriate documentation will be maintained. The documentation should be updated whenever the mail system configuration is changed.

The following will be developed and maintained to support consistent, reliable implementation of this security standard.

- Mail system Installation and Configuration Procedures; and
- Incident response procedures.