Navigatr Group

Internet Usage 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	10th 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

The primary purpose of this document is to provide policy and guidelines on internet usage and internet security controls to all users (as defined in the scope) at Navigatr Group.

This policy is established to:

- define prudent and acceptable practices with respect to the usage of internet;
- provide good security controls for restricting and monitoring internet access;
- ensure Navigatr Group's services and operations remain secure and efficient while communicating through external network (internet); and
- educate users on using internet with respect to their responsibilities, associated with such usage.

1.2 Applicability

This policy and guidelines related to the internet usage and security controls are applicable to all users who have requested for and provided with internet access using Navigatr Group's network infrastructure.

The following 'users' are covered by this policy:

- Full or part-time employees of Navigatr Group;
- The contractors who are authorized to use Navigatr Group owned equipment or facilities; and other personnel who have been provided access to Navigatr Group's internet services.

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

2 Internet usage policy

It is the policy of Navigatr Group to:

- develop effective systems and procedures to ensure that internet is used as an efficient mode of business communication;
- implement appropriate security control procedures so that internet facility is not misused; and
- implement appropriate security management practices and controls when maintaining and operating the internet services.

In accordance with the above policy statement, this policy has been established to provide good practices, procedures and controls over the internet usage.

Detailed security guidelines for the internet usage and security management practices are set out below.

3 Internet usage guidelines

3.1 Individual usage

3.1.1 The internet facility in Navigatr Group is provided to users only to conduct the business of Navigatr Group in an efficient and convenient manner. Incidental personal use is permissible as deemed appropriate by Navigatr Group.

3.1.2 Internet access facility will be used in an efficient and ethical manner.

3.1.3 Internet usage will never cause disruption, corruption, degradation, or security breaches over Navigatr Group's information system.

3.1.4 Personal accounts with on-line services such as Google, Rackspace, Microsoft etc who provide their own software to access services should not be used or accessed from Navigatr Group's computer system.

3.1.5 Usage of peer-to peer file sharing software such as BitTorrent, Limewire and Tor that allows remote sharing of files such as MP3, audio/video clips, from external network (internet) is strictly prohibited.

3.1.6 Remote access to external computers (other than company managed and approved remote access) is strictly prohibited. All approved remote access must be channelled through a company owned and managed secure and encrypted channel such as the company mobile user VPN or NetExtender.

3.1.7 Navigatr Group's computer systems will not be used to install personal web pages or web servers.

3.1.8 When users provide information on public forums such as newsgroups, bulletin boards, etc., they will clearly indicate that the opinions expressed are their own and not necessarily those of Travel Edge's.

3.1.9 Navigatr Group reserves the rights to block access to any internet sites as deemed inappropriate. The ability to connect to a specific web site does not imply that users are permitted to visit that site.

3.1.10 Users who discover that they have connected to a web site that contains sexually explicit, racist, violent, or other potentially offensive material will be immediately disconnected from that site.

3.1.11 No files or documents may be sent or received that may cause legal liability or harm the reputation of Navigatr Group.

3.2 Privacy

3.2.1 Users of Navigatr Group's internet services should realize that their communications are not automatically protected from viewing by third parties. Unless encryption and/or other approved security practices are employed, users will not send/post information over the internet if they consider it to be private and/or confidential.

3.2.2 Users are reminded that Web browsers leave “footprints” (or cookies) providing a trail of all site visited by the users.

3.2.3 Navigatr Group may activate logs and reserves the right to examine

- files on personal computers;
- web browser cache files;
- web browser bookmarks and cookies;
- logs of web sites visited; and
- other information stored on or passing through Navigatr Group computers.

Such logging facilitates compliance review with internal policies and assist Navigatr Group with internal investigations, if required at a later stage.

3.3 Access control

3.3.1 Individual dial-up lines (telephone), mobile (GPRS) to access the internet from within Navigatr Group's network is strictly prohibited.

3.3.2 The connection to the internet will be restricted with appropriate access controls devices like firewall, proxy or any packet/application filtering devices.

3.3.3 All software used to access the World Wide Web must be approved by the designated authorities and must incorporate all appropriate/approved vendor provided security patches.

3.3.4 The internet access will be passed through the filtering software to scan and filter the URLs, active content, malicious code, trojans and malicious files etc.

3.3.5 Access to internal services (i.e. web-based mail, remote desktop) from the internet must be via a secure (encrypted) login process and traffic must pass through a secure channel (e.g. Navigatr Group's corporate VPN, SSL or SSH connection). Subsequent transaction processes should be secure as well.

3.3.6 Navigatr Group's designated authorities must approve establishing any new business arrangements via the internet.

3.4 Confidentiality

3.4.1 Sensitive, confidential, and private information will never be stored on systems where unauthenticated access is permitted to the public (Internet).

3.4.2 The documentation, software, and other intellectual property of Navigatr Group must not be sold or transferred to any non-Navigatr Group user unless specific and adequate terms and conditions are agreed with.

3.4.3 Inappropriate electronic postings, which include non-work related postings, to public forums are prohibited. This includes postings which harass, annoy, alarm, or otherwise attack others in a forum as well as postings which might be considered as a threat against a user, group, or an organization or contain profanity, religious or political statements. Navigatr Group reserves the right to remove these and other postings, which are inconsistent with Navigatr Group's business interests and/or existing policy statements.

3.4.4 Security credentials, such as credit card numbers, civil id numbers, logins and passwords should only be sent via the internet through secured means in an encrypted format.

3.5 Integrity

3.5.1 Designated authorities will approve all web pages hosted on Navigatr Group's owned or operated systems.

3.5.2 Approval will be obtained from designated authority prior to posting Navigatr Group's information on the system exposed to internet.

3.5.3 The designated authority should first clear all representations on behalf of Navigatr Group. In addition, users should not release Navigatr Group's information or enter into any transactions such as contracts and including placing orders, until the identity of the individual and organization contacted are confirmed. This may be accomplished by a digital signature or digital certificate. Other acceptable means include letter of credit, third party references, and telephone confirmation.

3.5.4 Users may not misrepresent or falsify their identity on the internet or in any Navigatr Group communications. In all official Navigatr Group's communications, the user’s name, organization and other company specific information should be included in the message or posting.

3.5.5 Any files downloaded over the World Wide Web will be scanned for viruses, using approved virus detection software.

3.5.6 Information obtained via the internet will be considered suspect unless it is from a trusted source.

3.6 Intellectual property

Copying of unauthorised software such as, shareware, freeware from internet in a manner that is not consistent with the vendor’s license is strictly forbidden.

3.7 Discovering and reporting security problems

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

3.7.2 If unauthorized usage of Navigatr Group's information systems has taken place or is suspected, the user should notify the designated authorities immediately.

3.7.3 Whenever passwords or other system access control mechanisms are lost or are suspected to be lost, stolen, or disclosed, the user should notify the designated authorities immediately.

3.7.4 All unusual systems behaviour, such as missing files, frequent system crashes and other similar activities occur, the user should notify the designated authorities immediately.

3.7.5 The specifics of any possible security problems will be kept confidential and should be reported to immediate management staff and information security personnel alone.

3.7.6 Users are strictly prohibited from performing any security testing, possessing/using tools for cracking software license, passwords unless appropriate permission is obtained from designated authorities.

4 Agreement to comply with information security policy

Attached is a copy of Navigatr Group's ***Agreement To Comply With Information Security policy***. In order to receive access to the network or increase privilege access to the network, all users will be required to submit this form along with the access requests. This form is non-negotiable.

Agreement To Comply With Information Security Policy

I have access to a copy of Navigatr Group's information security policy. I have read and agree to abide by this policy, which govern my use of these services.

Internet Usage Policy

I, the user, agree to take all reasonable precautions to assure that Navigatr Group's internal information, or information which has been entrusted to Navigatr Group by third parties (such as customers), will not be disclosed to unauthorized persons.

I also agree to promptly report all violations or suspected violations of information security policy to the designated authorities.

By signing this agreement, I certify that I have read and understood this policy, and I am aware of its impact on my job. As a condition of continued employment at Navigatr Group, I agree to abide by this information security policy. I understand that any non-compliance would cause for disciplinary action including, but not limited to access privilege revocation.

Employee Name: ____

Employee Signature: ___________________________ ***Date:*** ______________

Authorised by ____

Head of Department: ___________________________ ***Date:*** _______________