Navigatr Group

Data Confidentiality Policy

This report contains 8 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

The primary purpose of this document is to provide policy and guidelines on Data Confidentiality at Navigatr Group.

This policy is established to:

- define prudent and acceptable practices with respect to data classification;
- provide management direction on data ownership;
- ensure that access to data and system resources should be limited to a need to know basis, and that specific users must be specifically allowed such access; and
- educate users with respect to their responsibilities, associated with data confidentiality.

1.2 Applicability

This policy and guidelines related to the data confidentiality are applicable to all users who have access to Navigatr Group's data and information.

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 data/information.

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

2 Data confidentiality policy

Data Confidentiality policy statements of Navigatr Group:

2.1.1 Company Information – employees will to hold in the strictest confidence, and not to use, except as required in connection with my work for the Company, or to disclose to any person, firm or corporation, without the written authorization of an officer of the Company, any trade secrets, confidential knowledge, data or other proprietary information of the Company. By way of illustration and not limitation, such shall include information relating to products, processes, know-how, designs, formulas, source code, object code, programs, methods, samples, developmental or experimental work, improvements or discoveries, plans for research, new products, marketing and selling, business plans, budgets and unpublished financial statements, prices and costs, suppliers and customers, and information regarding the skills and compensation of other employees of the Company. Employees will obtain the Company's written approval before publishing or submitting for publication any material (written, verbal or otherwise) that relates to my work at the Company and/or incorporates any information of the Company.

2.1.2 Former Employer Information – employee will not, during span of employment with the Company, improperly use or disclose any proprietary information or trade secrets of my former or concurrent employers or companies, if any, and will not bring onto the premises of the Company any unpublished documents or any property belonging to my former or concurrent employers or companies unless consented to in writing by said employers or companies. Will use in the performance of my duties only information which is generally known and used by persons with training and experience comparable to my own, which is common knowledge on the industry or otherwise legally in the public domain, or which is otherwise provided or developed by the Company.

2.1.3 Third Party Information – Employee recognizes that the Company has received and in the future will receive confidential or proprietary information from third parties subject to a duty on the Company's part to maintain the confidentiality of such information and, in some cases, to use it only for certain limited purposes. Employees will hold all such confidential and proprietary information in the strictest confidence and not to disclose it to any person, firm or corporation or use it for the benefit of anyone other than the Company or such third party, unless expressly authorizes to act otherwise by an officer of the Company.

2.2 Data Classification

- Develop effective systems and procedures for data classification to ensure that allocation of resources to the protect data assets, as well as determining the potential impact due to loss or damage from the corruption, loss or disclosure of data.
- To ensure the security and integrity of all data the default data classification for any data asset is either Confidential Customer Data or Proprietary Company Data;

All data found in the processing environment must fall into one of the following categories:

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 affects 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 affects 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.)

d) **Public Customer Data** – Public customer data is defined as data that any entity either internal or external to Navigatr Group can access. The disclosure, use, or destruction of Public

customer data will have limited or no adverse affects on Navigatr Group or the customer, and carry no significant liability. Public customer data is entrusted to, and may transit or be stored by Navigatr Group (and others) over which they have custodial responsibility but do not have ownership. (Examples of Public customer data include emails, public key certificates or other customer data that is readily available through other public channels or records.

2.3 Data Ownership

- Management will determine an entity responsible for the classification of data.
- The owner of data is responsible for classifying his/her data according to the classification schema noted in this policy.
- The default classification for all data not classified by its owner must be either confidential customer data or Proprietary company data.
- All information, data and documents are to be clearly labelled so that all users are aware of the ownership and classification of the information.
- All information, data and documents must be processed and stored strictly in accordance with the classification schema noted in this policy.

2.4 Non-disclosure Agreements

- On occasion when data assets that may need to be released to entities outside of Travel Edge or when a legitimate business reason exists for releasing sensitive information, a written Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, must be obtained before disclosing the data.

2.5 Data Security

- Confidential data is to be safeguarded using a combination of technical access controls and robust procedures, with all changes supported by audit trails.
- All users of information systems whose job function requires to create and amend data files must save their work on the system regularly to prevent corruption or loss through system failure.
- Data within Information Systems should maintain confidentiality to ensure it prevents disclosure of information to unauthorized parties while the information is in use or in transit, or while the information is being stored or destroyed.
- When providing access to data and information within Navigatr Group, should be attributable to a specific and unique individual. It should be possible to attribute a responsible individual to every event through an identification service and to verify that the individual so assigned has been properly identified through an authentication service.
- Information created and stored by the organization's information systems must be retained for a minimum period that meets both legal and business requirements.
- Archiving of data must take place with due consideration for legal, regulatory and business issues with liaison between technical and business staff.
- Version control practices should always be applied to documentation related to the organization or its customers.

2.6 Discovering and reporting security problems

2.6.1 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.

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

2.6.3 All unusual systems behaviour, such as missing files and related data and other similar activities occur, the user should notify the designated authorities immediately.

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