Navigatr Group

User Management and Password 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	11th 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 User and Password management at Navigatr Group.

This policy is established to:

- define prudent and acceptable practices with respect to user and password management on information systems;
- to ensure access control arrangements are established to restrict access by all types of user unless approved;
- To provide authorised users with access privileges which are sufficient to enable them to perform their duties but do not permit them to exceed their authority;
- To ensure adequate audit trails exits for individual accountability; and
- educate users with respect to their responsibilities, associated with password

1.2 Applicability

This policy and guidelines related to User and Password management are applicable to all users who have access to Navigatr Group's information systems

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 IT systems

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

2 Access control security

2.1 Data access control

Authorities to read, write, modify, update, or delete information from automated files or databases should be established by the designated owners of the information. Individuals may be granted a specific combination of authorities. For example, an individual may be allowed to "read only" or to "Read and Write but not delete" data. Authority to read, write, modify, update, or delete data may be identified at the data element level. Specific access authority should be established at the time an individual is assigned a password.

Controls must ensure that legitimate users of the computer cannot access stored software or data unless they have been authorized to do so.

- Access privileges of all users, systems, and programs to Navigatr Group information systems, communications and assets must be restricted on a need-to-know and need to do basis.
- Access to Navigatr Group sensitive or valuable information must be provided only after express management authorization has been obtained. Access to secret information must be granted to specific individuals and for the required period only.
- All resident information, which is sensitive, critical, or valuable, must have system access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.
- Staff who have been authorized to view information classified at a certain sensitivity level must be permitted to access only the information at this level and at less sensitive levels. Staff must never be authorized to write information classified at a certain sensitivity level unless this action is a formal part of an approved declassification process.

2.2 User identification

- Every user will have a uniquely assigned login name and password to access Travel Edge computer systems.
- Each employee is responsible for the login name assigned to him/her.
- For the issue of a new login name, a signed form indicating the relevant privileges is required, either in hardcopy or as part of the internal workflow software like e-mail.
- User login will be disabled after three unsuccessful attempts and reactivated upon request to the system administrator.
- A password should not be displayed in clear text on the screen.
- The system will be logged off automatically after an inactivity period.
- The unsuccessful login attempt will be logged and reviewed at regular intervals.

- In the case of an employee leaving Navigatr Group, the Department Manager will be responsible for making sure that all the employee's system IDs are revoked prior to final settlement.
- A login ID not used for 90 days will be disabled and later deleted with the permission of the employee's Department Manager.

2.3 Authentication

- Access to classified information without appropriate authentication shall not be allowed
- Authentication shall be performed in a manner commensurate with the sensitivity of the information to be accessed.
- The user will be required then to provide unique authentication (e.g., a password) with something that is known or possessed only by that user.

2.4 User privileges management

- All accounts shall be revoked after a pre-defined period of inactivity.
- User privileges shall be reviewed periodically.
- At the time that a member of the staff is transferred or ceases to provide services to Navigatr Group , all related information systems privileges shall be promptly terminated. The outgoing staff shall be responsible for the handover of computer resources to his/her department head or the incoming staff for business continuity.
- The use of special privileges shall be restricted and controlled.
- User access rights will be established on the basis of validated identification. The user identification code should be traceable to the user for the lifetime of the records and reports in which they appear.
- Division Heads must promptly report all significant changes in user duties or employment status to the computer system security administrators handling the user-IDs of the affected persons.
- Where staff are involuntarily terminated, they must be immediately relieved of all of their duties, required to return all Navigatr Group equipment and information, Staff's immediate management is responsible for ensuring all access privileges of the staff are promptly revoked.
- Division Heads should monitor and review the use of information access authority for each employee as each time a transfer, promotion, or termination from service occurs. Access authority to information should be changed or terminated as appropriate.

2.5 Accountability

- Each staff is accountable for the usage, access privilege and for any type of violations committed by their own user Id.
- Wherever feasible, to maintain accountability and traceability all commands issued by computer system operators will be traceable to specific individuals via the use of comprehensive logs.
- Wherever feasible, to foster user accountability, and to allow expedient systems management, all user activities affecting production information should be reconstructible from logs.

2.6 Privacy and personnel policy

- Navigatr Group reserves the right to examine all information stored in or transmitted by the users.
- Employees will sign the undertaking accepting responsibility for adherence to security policies.
- Hiring manager will ensure that security responsibility is included in the job responsibilities of the employee.
- The Terms and Conditions of employment shall mention the Information Security policy for each employee
- Department manager will ensure that the person has all computer accounts removed prior to his/her final settlement.

2.7 Desktop security

- Automatic protection features (e.g. password protected screen saver, keyboard lock) in servers, computer terminals, workstations or microcomputers will be activated if there has been no activity for a predefined period of time to prevent illegal system access attempt. Alternatively, the logon session and connection will be terminated. Also, user workstation should be logged off, before leaving work for the day or before a prolonged period of inactivity.
- Sensitive Data should be held on LAN and not on “C” drive of the user’s PC otherwise it must be protected by a physical lock or encrypted. Please contact the IT department if you have a question about securing data on the LAN.
- Users must log-off personal computers connected to networks when unattended.

2.8 Password management

- The password shall be used to authenticate a user's identity and to establish accountability to grant access to data.
- All default passwords will be changed by the user prior to use of the system.
- The password must never be shared or revealed to anyone else other than the authorized user.
- A password will not be less than 8 characters made up of a mixture of alphabetic and numeric characters, incorporating upper and lowercase letters.
- A password will be changed every 90 days or whenever compromised.
- No common name or personal information will be used as passwords e.g. date of birth, spouse's name, and pet name or phone number.
- A password will be different from the last 10 passwords for system connected to internet and 6 passwords for other systems.
- All user chosen passwords must contain a mix of alphanumeric characters.

2.9 Design of password system user interface

- The display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties will not be able to observe or subsequently recover them.
- All users must be automatically forced to change their passwords at least once every thirty (90) days.
- The initial passwords issued by a security administrator must be valid only for the involved users first on-line session. At that time, the user must be forced to choose another password.
- The number of consecutive attempts to enter an incorrect password must be strictly limited to four (4) unsuccessful attempts to enter a password. The involved user-ID must be either (a) suspended until reset by a system administrator, (b) If dial-up or other external network connections are involved it should be configured to disconnect.

2.10 Password System Internal Design.

- Storage of Passwords in Readable Form.

  - Passwords must not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover them.

- Encryption of Passwords.
  - To prevent them from being disclosed to wiretappers and other unauthorized parties, passwords must always be encrypted when held in storage for any significant period of time or when transmitted over communications systems.

- Prevention of Password Retrieval.
  - Computer and communication systems must be designed, tested, and controlled so as to prevent the retrieval of stored passwords whether they appear in encrypted or unencrypted form.

2.11 Master passwords ” SUPER USER” password management

- In general users will not have unlimited access to "super-passwords." Such passwords will be carefully controlled by user management and limited to system administrators. Monitoring the use of privileged passwords is Critical.
- All vendor-supplied default passwords must be changed before any computer or communications system is used for Navigatr Group business.
- All Master Passwords will be changed periodically.

2.12 Audit trails and logging

- All computer systems handling sensitive, valuable, or critical information must securely log all significant computer security relevant events like: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and addition/deletion/modifications to system software.
- Logs of computer security relevant events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with security measures.
- Logs of major computer security relevant events must be secured such that they cannot be modified, and can be read only by authorized persons. These logs are important for error correction, forensic auditing, security breach recovery, and related efforts.
- Period of retention of logs should be approved by legal Division.

2.13 Physical and environmental security

- Access control systems will be placed in a physically secure room.
- The room that contains the access control systems will be free of electrostatic or magnetic interference. Also the room will have controls for temperature and humidity.
- For availability or criticality reasons, an uninterrupted power supply (UPS) will be installed.

2.14 Documentation

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

2.15 Discovering and reporting security problems

- If sensitive, confidential, and/or private information is or is suspected to be lost or disclosed to unauthorized parties, the user should notify their manager immediately.
- If unauthorized usage of Navigatr Group's data/information has taken place or is suspected, the user should notify their manager immediately.
- All unusual systems behavior, such as missing files and related data and other similar activities occur, the user should notify their manager immediately.
- The specifics of any possible security problems should be kept confidential and should be reported to immediate management staff and IT personnel alone.