IT Security & Network Policy

1.1 Introduction

1. Information Resources are strategic assets of the company and must be treated and managed as valuable resources. The company provides various computer resources to its employees for the purpose of assisting them in the performance of their job-related duties.

2. TIDE WATER OIL (INDIA) LTD. (hereafter called 'TWOC' or "The Company") management has recognized the need to establish appropriate and acceptable security practices regarding the use of information resources and therefore have formulated this policy which clearly documents expectations for appropriate use of the company assets.

1.2 Purpose

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources in conjunction with its established culture of ethical and lawful behaviour, openness, trust, honesty and integrity.

1. Ultimate responsibility for the execution of this policy rests with the management of the company. Each individual policy shall mention the ownership and implementation responsibilities separately.
2. It is the responsibility of all employee/staff including consultants, third party employees and visitors to adhere to these policies
3. The company reserves the right to inspect any data stored on its computer or systems, or transmitted or received via company's network, in the course of investigating security incidents, or safeguarding against security threats.
4. All breaches of information security shall be reported to the Head of IT and investigated by the appropriate staff. Any violation, non-adherence to this policy shall be viewed seriously and will be liable for disciplinary action that may include termination.

1.3 Scope

1. This policy is applicable to all the users of information assets throughout the company.
2. All employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by the company, or to devices that connect to the company network or reside at the company site.
3. It includes all information resources such as equipment of storage of information, processing of information, network involved in data processing, backup media, servers, file storage equipment, PC's, Laptops, software's and licenses, printers, photo copiers, fax machines, all type of internet connectivity etc.

1.4 General Requirements

1. Individuals using the Information Assets of the company and Information Systems supported by the company have a responsibility to use them in a way that is lawful; in compliance with company policy; and consistent with the purposes for which they were intended.
2. Users are responsible for:
   - Knowing and complying with company policies, procedures and standards relating to the use of Information Assets and systems;
   - Safeguarding the Integrity and Confidentiality of company information as outlined in this and other policies; and
   - Creating, accessing, using and disposing of company information based on its classification.
   - Informing IT regarding exit or absconding subordinates or peers, whether directly or through HR, to ensure IT can block all relevant accesses for the said employee(s) who've exit or absconded the organization. In addition, the informing employee should also provide data to IT for forwarding or re-directing email or similar access to another existing employee, if required.

1.5 System Accounts

1. Users are responsible for the security of data, accounts, and systems under their control
2. Users should keep passwords secure and should not share account or password information with anyone, including other personnel, family, or friends.
3. Users should choose passwords that are easy to remember but difficult to guess. Some of the guidelines for password constructions are:
   - Do not use own name, short form of own name, own initials, names of family, friends, co-workers, company or popular characters.
   - Do not use personal information like date-of-birth, address, telephone numbers etc
   - Do not use common words found in English dictionary.
   - Do not use word or number patterns like aaabbb, qwerty, zyxwvuts,123321, etc
   - Do not use any of the above preceded or followed by a digit (e.g., secret1, 1secret)
4. Users should change their passwords at least once every 30 days
5. Conducting company business that results in the storage of proprietary information on personal or non-company controlled environments, including devices maintained by a third party with whom company does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by the company for business purpose.

1.6 Computing Assets

1. You are responsible for ensuring the protection of assigned company assets. Laptops left at the company overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of Company assets to the Information Security Team
2. All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off and switch off the monitor when the device is unattended.
3. Devices that connect to the Company network must be Company's asset and comply with the Access Control Policy
4. Do not interfere with corporate device management or security system software.

1.7 Network Use for Employees

You are responsible for the security and appropriate use of the company network resources under your control. Only registered TWOC's IT asset can be connected to corporate private network. ITD will ensure effective MAC binding feature for IP allocation and network access. Using company network resources for the following is strictly prohibited:

- Causing a security breach to either company or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.
- Causing a disruption of service to either company or other network resources
- Violation of copyright laws including, but not limited to illegally downloading, duplicating or transmitting copyright pictures, music, video or software
- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and key loggers
- Port scanning or security scanning on a production network unless authorized in advance by Information Security personnel.

1.8 Network Use for Externals (Guests/Business partners/Consultants)

In case of an exchange of information between TWOC and an external party, appropriate agreement will be established addressing the following points:

- Traceability and non-repudiation
- Courier identification standards
- Responsibilities and liabilities in the event of an incident
- Labeling system/cryptography as per the sensitivity of the information

Under no circumstances externals/non-TWOC systems should be connected to corporate private network. ITD can provide public internet connection using third party wifi routers for business use on written request and approval from functional heads.

1.9 Electronic/Email Communications

1. The following are strictly prohibited:
   - Sending spam e-mails, or other forms of unsolicited electronic communication.
   - Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
   - Use of company e-mail or IP address to engage in conduct that violates company policies or guidelines Posts to a public newsgroup, bulletin board, or listserv with a company e-mail or IP address represents company to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.
2. Users shall comply with the company's e-mail security policy on proper and effective use of e-mail
3. Users should promptly report all suspected security vulnerabilities or problems that they notice with the email system to the ITD.
4. The company has the authority to intercept or disclose or assist in intercepting or disclosing email communications.
5. Users will not use any email account other than the one provided by the company for transacting official information unless such exception has been specifically approved.
6. Confidential information will be secured before sending through e-mail by way of compression, password protection or other advanced cryptographic means.
7. Language used should be consistent with other forms of business communications
8. All emails will adhere to the standard email signature policy as per company guidelines.

1.10 Internet Usage

1. Excessive Web browsing unrelated to official business during work hours is prohibited. Users shall not use or access the internet for non-business purposes and restrict personal use to a minimum for educational, knowledge and news sites. The organization has the right to grant or revoke complete or partial internet access based on existing or revised policies from time to time
2. Users should not use Internet facilities to:
   - Download or distribute malicious software or tools or to deliberately propagate any virus
   - Violate any copyright or license agreement by downloading or distributing protected material
   - Upload files, software or data belonging to the company to any Internet site without authorization of the owner of the file/ software/ data
   - Share any confidential or sensitive information of the company with any Internet site unless authorized in writing by a Superior

- Users shall not post any company proprietary information or customer's proprietary information on Internet share drives/Briefcase, public forums, newsrooms or bulletin boards. This is strictly prohibited and any violation will be subject to disciplinary process that includes legal consequences
- Post remarks that are defamatory, obscene or against the company. Also, they should not share company internal information on the internet
- Conduct illegal or unethical activities including gambling, accessing obscene material or misrepresenting the organization
- In case such misuse of the Internet access is detected, the company can terminate the user Internet account and take other disciplinary action

3. Following is prohibited:
   - Access online media streaming sites (e.g. radio, music and video broadcasts), other websites and social networking sites unless they are work-related
   - Create and post to personal blogs
   - Creating personal web pages or
   - Conduct a private online business (including dealing on eBay or similar sites, or share trading)
   - Accessing or installing unauthorized software

2.1 Internet Security

1. Users are responsible for safeguarding any online transactions of a personal or official nature which utilize user identities and passwords.
2. Each user should ensure that they verify the nature & status of any secure site (https:// or ftps://) before entering into any internet based transaction.
3. The organization will not be liable for any personal damages or personal losses suffered by anyone using the Company's Internet access.
4. The organization has provided certain security measures to safeguard the use of Internet from within the organization premises. These security measures will not be in effect if any employee makes use of Internet while disconnected from the Company's network
5. Users should not download any software through the Internet. They should approach ITD for any such downloads. ITD will verify that the software does not pose any security or licensing issues before providing a copy of the downloaded software.
6. Users who have downloaded any programs or software directly from the Internet before this policy came into effect should immediately delete all copies or instances of such software or programs from their desktops or laptops.
7. In case any problems are reported and IT finds that un-secure programs have been downloaded from the Internet the matter will be escalated to the Top Management.

2.2 Internet Monitoring

All Internet usage via the company's Internet access, even those of a personal nature, will be monitored by ITD for adherence to the IT Policy. You must have no expectation of privacy in anything that viewed, uploaded or download using the company's Internet access. Your Internet use can be monitored without prior notification if TWOC deems this necessary. ITD also has the right to perform random audits, without any prior intimation, to verify acceptable use of the Internet by the end user. A report will be submitted to the supervisor and top management in case any exceptions are found during such audits.

3.1 Antivirus

1. All workstations and laptops will have antivirus installed, running and updated
2. User will not change the antivirus settings

3. Users should not disable the installed anti-virus agent or change its settings defined during installation. This includes settings for daily virus scan; anti-virus server address and signature update schedules
4. Users should not disrupt the auto virus scan scheduled on their desktop. If the scan is affecting system performance or if the scan has not executed as it should, users should immediately contact the system administrator / IT helpdesk for resolution
5. All external media will be used only after authorization and will be subjected to anti-virus scan and users are advised to run anti-virus scan when any external media is used
6. Users will report any virus detected in the system to system administrator

4.1 Monitoring

The company reserves the right to monitor, record and audit an individual's use of the company's Systems if there are reasonable or probable grounds to suspect illegal or other Inappropriate Conduct.

ITD will establish proper monitoring mechanism using software, which will gather software deployment details for all connected devices at frequent intervals.

5.1 Enforcement

Any employee found to have violated this policy may be subject to necessary disciplinary actions.