ANNEXURE A

Handling of Sensitive/Confidential Information of the Company

- **Data and information relating to the Company is confidential and should be used only for official purpose Employees shall not disclose it or use it for personal gain or for the advantage of any other person or purpose.**

- **Users shall not share any Company confidential/sensitive information with a third party without ensuring that a Non-Disclosure Agreement is signed with the respective third party.**

- **Users shall ensure that all the important and sensitive data related to the Company, are stored on the central file storage drives in order to protect such information from unauthorised access and to prevent loss of information due to hard disk crashes.**

- **If any Company sensitive information is stored in the local hard disk/ removable media, such information shall be stored in an encrypted form to safe guard sensitive information from unauthorized access.**

- **Users shall not forward e-mail to any address outside the Company's network unless the information owner / originator agrees in advance or the information is clearly public in nature. This policy does not apply to personal e-mails.**

- Automatic forwarding of email messages to all external address could compromise the information confidentiality to avoid risks associated with such compromise automatic forwarding of e-mail messages of any user to an external address shall be allowed only for a specific period and shall require approval from the Divisional CEO and CIO for Division/CFO and CIO for Corporate.

- Users shall not forward e-mail containing Company information to personal e-mail ids unless authorized by Line EC/DMC member/Corporate HoD.

Refraining from Computer related offences

- **Users shall not store, process, or transmit material which is unlawful, defamatory, harassing invasive of any individual's privacy, abusive, harmful, threatening, vulgar, pornographic, obscene, or otherwise objectionable, offends religious sentiments, or promotes racism.**

- Users shall not use or attempt to initiate activities using information processing resources or equipment leading to abusive, unethical or inappropriate use of the internet facility provided by the Company

    - Examples of prohibited Internet use include, but are not limited to, the following o Impersonate the identity of another user on the internet or on any of the Company systems

    - Conduct illegal activities, including gambling, access or download pornographic illegal material

    - Introduce material considered indecent, offensive, or is related to the production, use, storage, or transmission of sexually explicit or offensive items on the company's network or systems, using Internet

- **To maintain harmony, e-mail users shall not create or forward e-mail messages that can cause harassment to a certain sex, race and religion.**

- **Users shall not delete/destroy/alter any computer source code or information residing in computer resource with the intent to cause wrongful loss or damage to the Company or any person.**

- **Users shall not deny or cause the denial of access to any person authorized to access any information systems.**

Pre-emption against adverse legal implications

- **Only authorized software shall be installed on the desktop/laptop as per the licensing provisions.**

- **While using internet, users shall not**

    - Upload or download commercial software in violation of its copyright

    - Reveal or publicize Company proprietary or sensitive information and represent personal opinions as those of Company's;

    - Enter into contractual agreements via the internet unless authorized to do so, e.g., enter into binding contracts on behalf of Company over the internet;

    - Solicit for any purpose which is not expressly approved by management

    - Use Company logos or materials in any web page or Internet posting without seeking prior approval as per Corporate Governance

- **Users shall ensure that e-mails addressed to external parties are not addressed to or copied to internal recipients. If there is a need for this mail to be sent to internal recipients, such mail should be separately forwarded to internal users.**

- When a communication containing any claims against the Company is received through e-mail, user should immediately send out a responder message which shall read as follows:
  "Please note that claims of any nature whatsoever will not be accepted on email"

- E-mail users shall not

    - Acknowledge any incoming mail if such user is neither dealing with the subject nor authorized by the Company to do so and instead should forward it to the HoD / Unit Head/Functional Head.

    - Further, in the event that such an e-mail relates to any claims against the Company attached with significant financial implication or penal consequences, HoD/Unit Head/Functional Head shall forward the same to the Company Secretary.

Safe use of E-mail and Internet

- **Originating/ propagating a chain mail, which is not related to the business, is strictly prohibited.** The only exception to this clause shall be the messages sent on humanitarian health grounds of Company employees/families.

- Users while using internet shall not:

    - Intentionally interfere with the normal operation of any corporate Internet gateway;

- Attempt to gain unauthorized access to remote systems on the internet;
- Establish unauthorized internet or other external network connections that could allow non-Company users to gain access into information processing resources and information assets;
- Click on suspicious links or pop-up ads or respond to any prompts requesting for installation/ upgrading of any software or device drivers from unknown sources.

Security of Company's IT Assets

- Users shall pay attention to security warnings. When a system gives a security warning, users shall make sure to read the security warning and report to the IT team. In case of any evidence of or suspicion of security violation, users shall notify the respective Information Security Incident Manager (SIM) immediately of any evidence of or suspicion of security violation.
- Users shall make sure that Desktops/Laptops assigned to them are protected by power-on passwords
- **Users shall be responsible for the physical protection of Portable media and devices (such as laptops, external storage media etc.) containing company information and any loss of such media/device shall be reported as per the laid down process of the Division/Shared Services for handling such incidents.**
- **Password Management**
  Users shall ensure that the passwords are
  - Not shared for individual user-ids;
  - Changed at the first log-on;
  - Not easily guessed or obtained using person related information, e.g., names, telephone numbers, and dates of birth etc.;
  - Not written down or stored electronically without adequate protection;
  - Changed whenever there is any indication of possible system or password compromise;
  - Not stored in automated logon processes like browsers and Forms that allow users to store their credentials for replaying later.

Responsible use of Company's IT Assets & Facilities

- To ensure optimal utilisation of the Company's data storage resources, every user should delete unwanted messages as a practice Housekeeping of mailbox shall be the responsibility of individual user.
- Users shall ensure proper restart of laptops/desktops while connected to ITC LAN at least once in a day to update the security policies.
- **User shall be responsible for the deletion of all the information stored on the local hard disk of a computer issued to him/her, before returning the same to the IT Team.**
- User shall not store sensitive/confidential information on removable media unless absolutely necessary.

- User shall delete the information stored in the removable media after the purpose is over.
- **Users shall not share the Information Assets and facilities provided to them or use Information Assets and facilities extended to other users unless authorized to do so.**
- Users shall not try and test the weaknesses of the information systems unless authorized to do so.
- Users shall switch off the power source for individual workstations and other IT equipment before leaving for the day.

Company's Rights

- Company respects the individual privacy. However, owing to legal and ethical reasons:-
    - Privacy shall not extend to the use of the Company's Information assets/ services Company reserves the right to log, monitor and inspect use of all information assets/ services provided to its employees. The user understands that such monitoring may involve access to any personal data or information that the user may store in such information assets The user by agreeing to accept and use such information assets/ services provides his/her consent and authority to the Company to that affect.
    - In order to ensure privacy to e-mail users, the e-mail administrator shall not scrutinize the contents of the users' mailbox. However, in exceptional circumstances, the Chairman – CITSC may grant the permission to scrutinize the e-mails of a specific user for a specific period.
- To protect the Company's interests, it can initiate necessary action for:
    - suspected misuse that may cause damage to Company's interests and image
    - User's non-compliance with regulations.
- To safeguard the Company's interest, IT facilities provided to an employee can be withdrawn at any time at the discretion of the Company.