Subject: **Advisory – Cyber Security Threats and Privacy Concerns – Cautious Usage of AI Driven ChatBots (Advisory No. 09)**

Context. OpenAl launched ChatGPT in November, 2022; gathering a widespread usage and audience. With this, issues regarding positive and negative aspects concerning cyber security and privacy concerns have come to the forefront. Consequently, an advisory on Chat GPT with emphasis on its cyber security challenges/aspects was shared on 19th June, 2023 and 11th July, 2023. Off late, ChatGPT and other similar models (Bard, CoPilot, MyAi etc.) are integrated in major Social Media platforms, Web Browsers and Smart Phones. Given the exponential rise in usage of Al Driven ChatBots, the safety measures and cautious use of ChatGPT/ChatBots at organizational and individual level are illustrated in the ensuing paras.

2. **Growing Trend – Al Driven ChatBots**. Globally, many organizations are integrating ChatGPT and other Al powered ChatBots/APIs into their operational flow/information systems. ChatGPT accounts signify the importance of AI-powered tools along with the associated cyber risks as it allows users to store conversations. In case of breach, access of a user account may provide insight into proprietary information, area of interest/research, internal operational/business strategies, personal communications and software code etc.

3. **Precautionary Measures**

a. **Users**

(1) ChatGPT/other Al-powered ChatBots and APIs must not be used by users handling extremely sensitive data. Masking of critical information may be utilized where absolutely essential.

(2) Do not enter sensitive data which reveals own capability/held resources etc. into ChatBots. If essential, ensure to disable the chat saving feature from the platform's settings menu or manually delete those conversations as soon as possible.

(3) Use a malware free/screened system for ChatBots. An infected system with information stealer malware may take screenshots or perform keylogging leading to a data leak.

b. **Organizations**. Through best practices at organizations can ensure that ChatBots are used securely and the data is protected. It is also important to note that Al technology is constantly evolving. The key to protection may be that organizations must stay up-to-date with the latest security trends. Few best practices (but not limited to) are as follows:

(1) **Dedicated Online PC for ChatBot Usage**. To ensure data protection and countering pilferage of sensitive official data, separate online PC with no private/official data be used for using Al driven ChatBots.

(2) **Conduct Risk Assessment**. Comprehensive risk assessment of Al Driven ChatBots be performed to identify any potential/exploitable vulnerabilities. This will help organizations to develop a plan to mitigate risks and ensure that their data is protected.

(3) **Mechanism to Monitor Access**. It is important to monitor that who has access to ChatBots. A mechanism be ensured that access is granted only to authorize individuals. This can be achieved by implementing strong access controls and monitoring access logs.

(4) **Implement Zero-Trust Security**. Zero trust security (an approach that assumes that every user and device on a network is a potential threat) be adopted. This means that access to resources should be granted only on need-to-know basis followed by strong authentication mechanism.

(5) **Use Secure Channels**. To prevent unauthorized access to Al Driven ChatBots, secure channels be adopted to communicate. It includes using encrypted communication channels and secure APIs.

(6) **Train the Employees**. Employees be trained on cautious usage of ChatBots and the potential risks associated with its use. It, must be ensured that the employees do not share sensitive data with chatbot and are aware of the potential for social engineering/malicious attacks.