FORMAT OF CYBER SECURITY INCIDENCE DISCLOSURE UNDER CORPORATE GOVERNANCE REPORT

I. BACKGROUND:

In terms of Regulation 27 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, listed entity shall submit a quarterly compliance report on corporate governance in the format as specified by the Board from time to time to the recognised stock exchange(s) within twenty one days from the end of each quarter.

Securities Exchange Board of India vide its Notification No. SEBI/LAD-NRO/GN/2023/131 dated June 14, 2023 issued SEBI (Listing Obligations and Disclosure Requirements) (Second Amendment) Regulations, 2023 and inserted sub clause 27(2)(ba) wherein it has specified that the details of Cyber Security incidents or breaches or loss of data or documents shall be disclosed in the Corporate Governance Report and shall be submitted by the listed entities to the stock exchanges on a quarterly basis which is effective from July 14, 2023 onwards.

In reference to this, BSE vide its circular dated September 29, 2023, has revised the existing Corporate Governance Report utility by adding new fields.

II. EFFECTIVE DATE:

This circular shall be effective from the filing of Corporate Governance report for quarter ended September 30, 2023, and onwards.

III. KEY HIGHLIGHTS OF THE CIRCULAR:

Following new fields have been added to the existing Corporate Governance Report utility:

Details of Cyber Security Incidence		
Whether as per Regulation 27(2) (ba) of SEBI (LODR) Regulations, 2015 there has been cyber security incidents or breaches or loss of data or documents during the quarter		Yes/No
Date of the event	Brief details of the event	

IV. CACS VIEW:

As per SEBI Consultation Paper on Review of disclosure requirements for material events or information under SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, the rational of insertion of provision in SEBI LODR requiring the Companies to report the cyber security incidents were as follows:

"With the advancements in technology and the companies adopting such newer technologies, cyber security incidents or breaches and loss of data / documents have become a major concern. Such incidents may impact the operations and/or performance of the listed entity. Disclosure of such events are necessary for investors to understand the associated risks and impact.

However, immediate disclosure of such events may not be desired since the entity may be vulnerable to further attacks. Hence, the disclosure with root cause analysis and remedial measures taken, etc. may be mandated under the quarterly compliance report on corporate governance required to be submitted by listed entities under regulation 27 of LODR Regulations."

In view of above rational, it appears that SEBI intended the listed entities to disclose the incidents of cyber security incidents or breaches and loss of data / documents and such incident may impact the operations and/or performance of listed entity in quarterly Corporate Governance Report.

Hence, It is very subjective for the listed entities to identify the reportable incidents / breach and it may vary from Company to Company based on their nature of business operation and the impact suffered by them.

It is further to note that as referred by SEBI in consultation paper, the meaning of key terms **"Cyber Incident", "Cyber Security Incident"** and **"Cyber Security beaches"** are defined in Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Function and Duties) Rules, 2013 and reproduced as under for quick reference:

(g) "Cyber incident" means any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation;

(h) "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(i) "Cyber security breaches" means unauthorised acquisition or unauthorised use by a person as well as an entity of data or information that compromises the confidentiality, integrity or availability of information maintained in a computer resource;

Disclaimer: There is no official clarification from SEBI / BSE / NSE on the manner of reporting and what kind of information should be reported. Hence, the Company is to consider the incidents which had impacted the operations / performance of the Company and the same may or may not be material for the Company. The above view is just our interpretation. The Compliances are to be ensured by the listed entities in its letter and spirit.

REFERENCE:

https://www.bseindia.com/markets/MarketInfo/DispNewNoticesCirculars.aspx?page=20230929-26

*****

Suggestions may be sent to rupesh@cacsindia.com

Rupesh Agarwal| Managing Partner| Chandrasekaran Associates | Company Secretaries 11-F, Pocket Four | Mayur Vihar Phase One | Delhi - 110 091 | Tel. +91-11-2271 0514 rupesh@cacsindia.com | info@cacsindia.com | www.cacsindia.com