BOARD CORPORATE DISCLOSURE AND CYBERSECURITY POLICY

1. INTRODUCTION

Cabnet Holdings Berhad ("Cabnet" or "the Company") is committed to upholding high standards of transparency and promotion of investor confidence through the provision of comprehensive, accurate and quality information on a timely and even basis and to protect its systems and information from cyber threats, to better manage and reduce cybersecurity risk as well as to uplift Cabnet's group cybersecurity capabilities.

In adopting this policy, Cabnet has taken into account the recommendations contained in the Malaysian Code of Corporate Governance 2021 ("MCCG 2021"), the disclosure obligations contained in the ACE Market Listing Requirements of Bursa Malaysia Securities Berhad and the Corporate Disclosure Guide issued by Bursa Malaysia.

2. RATIONALE AND OBJECTIVES

The primary objectives of Cabnet's Corporate Disclosure and Cybersecurity Policy are:

- To promote and elevate a high standard of integrity and transparency through timely comprehensive, accurate, quality and full disclosure.
- To promote and maintain market integrity and investor confidence.
- To exercise due diligence to ensure the veracity of the information being disseminated is factual, accurate, clear, timely and comprehensive.
- To build good relationship with all stakeholders based on transparency, openness, trust and confidence.
- To align cyber security initiatives to business objectives.
- To establish cybersecurity governance to support cybersecurity initiatives.
- To have in place efficient procedures for management of information, which promotes accountability for the disclosure of material information.

3. DISCLOSURE STRUCTURE AND RESPONSIBILITY

To achieve its objectives, Cabnet has adopted the following structure and responsibility.

3.1 Corporate Disclosure Policies and Procedures (CDPP)

Cabnet has adopted the following Disclosure Policies and Procedures.

- Communicating and responding to all stakeholders in respect of all information relating to the Group through all forms of communication channels as outlined under 3.4 below.

3.2 Designated Spokesperson:

- Chief Executive Officer
- Chief Operating Officer
- Chairman of the Board

3.3 The Designated Spokesperson is responsible for:

- Proper dissemination of information and ensuring compliance with the disclosure obligations under the Listing Requirements.
- Communication, overseeing and co-ordinating disclosure of material information to all stakeholders in accordance with the Listing Requirements and ensuring appropriate security measures are in place to maintain integrity of the information being disseminated.

3.4 **Disclosure and Dissemination Channels**

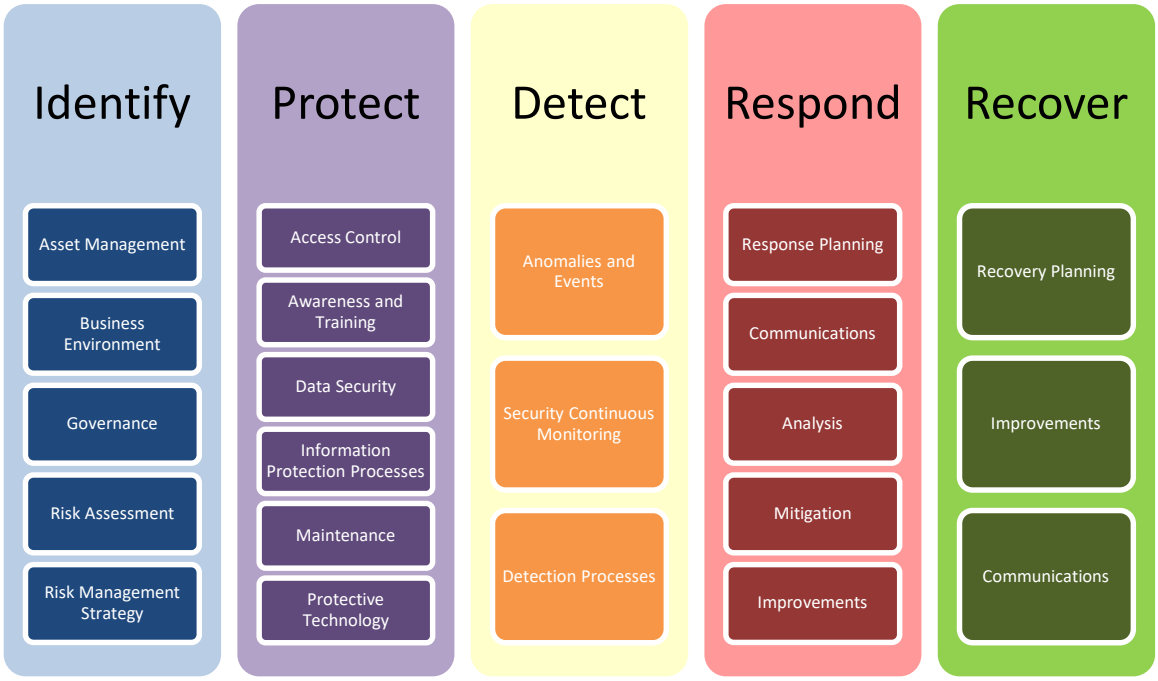
Cabnet is authorised to make use of a broad range of communication channels to disseminate information to its stakeholders and these include :

- Electronic facilities provided by Bursa
- Press releases
- Corporate website
- E-mail
- Road shows, exhibitions, analyst briefings, interviews or events, and
- General Meetings

4. DOCUMENT AND CYBERSECURITY MANAGEMENT

Cabnet has in place a structured and streamlined document management system in place for each of its operating departments.

Cabnet shall implement management of cybersecurity focusing on 5 attributes consistent with NIST Cybersecurity Framework namely Identify, Protect, Detect, Respond and Recover.



These documents are securely stored and where material and sensitive, are restricted in its circulation to authorised personnel and locked away.

Cabnet also has in place, a secured Information Technology system for communication and document management purposes supported and maintained by an in-house IT Manager/Department.

Access to information in the IT system is secured and controlled through password protection and authorised access restrictions.

Financial information and other material price sensitive information access is further restricted to only designated senior management employees in the finance/accounts department. The finance/accounts department's information is not shared or accessible by other departments within the Group.

5. RESTRICTIONS, PROHIBITIONS AND CONFIDENTIALITY

Only the following persons who "need to know" are authorised to have access and become privy to sensitive and material information that has not been disclosed and made available to the public.

a) members of the Board of Directors.

b) the Chief Financial Officer and senior executives in the finance/accounts department designated by the Chief Executive Officer/Deputy Chief Executive Officer/Chief Financial Officer.

c) the Company Secretaries, auditors, reporting accountants, lawyers, consultants and investment advisers on a "need to know basis" to enable such persons to carry out their roles and responsibilities at the appropriate time as may be determined by the Chief Executive Officer/Deputy Chief Executive Officer/Chief Financial Officer.

d) the authorised persons upon coming into possession of such confidential information are reminded :

- Of the need to keep the information strictly confidential
- Of the restriction for insiders who are in possession of unreleased material information not to trade in the Company's securities or the securities of such related third parties, where applicable.
- Tip any third party with such information.

6. WHERE CONFIDENTIALITY IS COMPROMISED

In the event, the confidentiality of the information has been compromised, Cabnet will take the appropriate steps to make an immediate announcement of the information (or clarify the status) to Bursa Malaysia.

Confidentiality is deemed to have been compromised where such information appears in analyst reports, media reports or market rumours accompanied by unusual market activity.

Where Cabnet becomes aware of a rumour or report, the Chief Executive Officer/Deputy Chief Executive Officer/Chief Financial Officer will consult with its Directors, major shareholders and such other relevant persons involved in the matter to determine:

- whether the rumour or report contains undisclosed material information; and
- whether immediate disclosure is required to clarify, confirm or deny the rumour or report.

As a general rule it is not Cabnet's policy to respond or comment on market rumours and speculations, unless they appear to contain elements of undisclosed material information.

This Board Corporate Disclosure and Cybersecurity Policy was approved and adopted by the Board on 23 February 2018.

This Board Corporate Disclosure and Cybersecurity Policy was last reviewed and revised on 24 February 2022.