PROTASCO BERHAD
CYBERSECURITY POLICY

Policy Statement

At Protasco Berhad, we are committed to prioritising and enhancing data protection and security to ensure the safety and security of our employees' and clients' data. We maintain robust cybersecurity management practices by embedding strong governance frameworks that reinforce our privacy and security controls. Through continuous awareness initiatives and best practices across all business operations, we aim to safeguard against security breaches that could disrupt our operations, lead to significant financial consequences, and damage our company's reputation.

Objectives

Protasco Berhad recognises the critical importance of cybersecurity in safeguarding its business operations. This policy is established to ensure that all activities involving information technology are effectively protected against cybersecurity threats. The objectives of this policy are:

1. **Stakeholder Obligations:** To clearly define the roles and responsibilities of all stakeholders—including employees, customers, contractors, and other authorised users—in protecting the company's technology and information assets. The Cybersecurity Policy Framework outlines the assets that require protection and identifies the various threats to these assets.
2. **User Responsibilities and Privileges:** To specify the acceptable use of company systems, including guidelines on internet access, user limitations, and the consequences of policy violations. The policy also includes procedures for responding to incidents that could jeopardise the security of the company's computer systems and network.

Scope

This policy applies to all permanent and temporary employees of Protasco Berhad, as well as independent contractors, consultants, vendors, suppliers, agents, and any other users of Protasco's IT resources (collectively referred to as "users"). The policy is applicable regardless of the users' location, ensuring that all individuals and entities accessing or interacting with

Protasco's IT systems and information are subject to the same stringent cybersecurity standards.

Governance

Cybersecurity is a strategic priority for Protasco Berhad, extending beyond a technical issue to a core component of the Group's Risk Management framework, which encompasses all business units. The Group Corporate Office is responsible with developing and implementing a comprehensive cybersecurity plan to ensure robust protection across the organisation.

Cyber risks must be regularly reported and updated to operations management, senior management, and the Board of Directors. All levels of leadership should consider these risks when making changes to business processes, including the information and technology environment.

Cybersecurity Risk Management

The Group will develop, maintain, and periodically update as required, an inventory of major types of information and systems on the basis of criticality to the business. This list, on a priority basis, will be used to formally assess the degree of cyber protection that the company has, the target degree of protection as well as the plans that are in place to achieve the desired level as appropriate. The target level will reflect the nature of the information or application as well as the risk appetite.

Cybersecurity Breach

Upon discovering a breach, the Business Unit or Department must take immediate steps to contain it. Detailed procedures will be established and shared across all Business Units within the Group to ensure effective cybersecurity management. Regular awareness and training will be provided to all employees to ensure these procedures are understood and consistently followed.

Legal Compliance

Violations of this policy may result in disciplinary action, up to and including termination, depending on the severity and nature of the breach. Disciplinary measures will be determined on a case-by-case basis, in line with company policies and applicable laws.

This policy will be reviewed from time to time for continuous improvement based on the environment and circumstances the surrounding the Group and its Business Units.