



Information Security and Cybersecurity Policy

Introduction

Express Power Solutions (M) Berhad and its Group of Companies (“the Group”) recognize the importance of information and technology in supporting the Group’s business operations, continuity, resilience, and long-term growth.

As the Group increasingly relies on information systems, digital technologies, networks, cloud services, and electronic communications, it is exposed to evolving information security and cybersecurity risks, including unauthorized access, malware, phishing, ransomware, data breaches, system disruption, and other cyber threats.

The Group is therefore committed to maintaining an effective information security and cybersecurity framework to protect its information, systems, networks, applications, technology assets, and the interests of its stakeholders. This Policy establishes the Group’s principles and requirements for managing information security and cybersecurity risks and supporting the secure, resilient, and continuous operation of the Group.

Objective

The objective of this Policy is to establish a consistent and effective framework for managing information security and cybersecurity risks across the Group and to ensure that appropriate measures are in place to protect the confidentiality, integrity, and availability of the Group’s information and technology resources.

The Policy aims to:

- protect the Group’s information, systems, networks, applications, and technology assets from unauthorized access, disclosure, alteration, destruction, misuse, disruption, and loss;
- identify, assess, manage, and reduce information security and cybersecurity risks that may affect the Group’s operations, assets, and stakeholders;
- prevent, detect, respond to, and recover from information security and cybersecurity incidents and threats;
- support business continuity, operational resilience, and the secure delivery of the Group’s business activities;
- promote security awareness and accountability among personnel and relevant third parties; and
- ensure compliance with applicable legal, regulatory, contractual, and industry requirements.



Scope

This Policy applies to Express Power Solutions (M) Berhad and its Group of Companies ("the Group") and covers all information and technology resources, including information systems, networks, applications, devices, cloud services, and related technology resources owned, managed, leased, or authorized by the Group, regardless of their format, medium, or location.

This Policy applies to all directors, employees, contractors, consultants, service providers, and other third parties who access, process, or manage the Group's information or technology resources.

Governance and Responsibilities

The Board of Directors and Senior Management provide oversight and direction on information security and cybersecurity matters and ensure that appropriate governance, resources, and controls are established to support compliance with applicable requirements.

The Administration department, or other function designated by the Group, shall coordinate the implementation, monitoring, and continuous improvement of this Policy and related information security and cybersecurity activities, with support from relevant functions as appropriate.

All directors, employees, contractors, and relevant third parties are responsible for complying with this Policy and protecting the Group's information and technology resources within the scope of their roles and responsibilities.

Relationship with Other Group Policies

This Policy shall be read together with the Group Personal Data Protection Policy and other applicable Group policies, procedures, standards, and guidelines.

Where information security and cybersecurity matters involve the protection of personal data, the relevant requirements under the Group Personal Data Protection Policy shall also apply.

Access Control and Handling of Information

Access to information and systems shall be appropriately controlled based on job roles, responsibilities, least privilege, and need-to-know principles.

User accounts and access rights shall be established according to job responsibilities, reviewed periodically, and promptly modified or revoked when no longer required, including when personnel change roles or leave the Group.

Appropriate authentication and access controls shall be maintained to prevent unauthorized access. Privileged and administrative access shall be restricted and reviewed, and shared accounts shall be avoided unless necessary and appropriately controlled.



Confidential and sensitive information shall be appropriately protected and accessed only by authorized personnel. Information shall be securely handled throughout its lifecycle, including storage, transmission, use, retention, and disposal.

Information and technology assets that are no longer required shall be securely disposed of in accordance with applicable Group procedures.

Cybersecurity and Technology Protection

The Group shall implement appropriate measures to protect its information, systems, networks, applications, and technology resources against cybersecurity threats, unauthorized access, misuse, disruption, and other security risks.

The Group shall take reasonable and risk-based measures to prevent, detect, respond to, and recover from cybersecurity threats and incidents.

Personnel shall use the Group's information and technology resources responsibly and shall not intentionally disable, bypass, or circumvent established security controls.

Personnel shall remain vigilant against common cybersecurity threats, including phishing, malware, social engineering, and unauthorized access, and shall promptly report any suspected cybersecurity incident or weakness.

Security Updates and Vulnerability Management

The Group shall take reasonable and appropriate measures to identify and address security vulnerabilities that may affect its information systems, applications, networks, devices, and other technology resources.

Security updates and patches shall be applied within a reasonable timeframe based on the nature and severity of the vulnerability, the associated risk, and the operational requirements of the affected system.

Where vulnerabilities cannot be immediately addressed, appropriate risk mitigation or compensating measures shall be considered.

Third-Party and Supplier Security

Third parties and suppliers with access to the Group's information or technology resources shall comply with applicable Group security requirements.

Where appropriate, information security and cybersecurity requirements shall be incorporated into relevant contractual or service arrangements.

Third-party access to the Group's information and technology resources shall be appropriately authorized and controlled and shall be removed when no longer required.



Incident Management

Any actual or suspected information security or cybersecurity incident, security breach, unauthorized access, malware infection, phishing attack, loss of information or device, or other security event shall be reported promptly through the designated reporting channel or to the Administration department or designated person, as applicable.

Personnel shall not conceal or deliberately take actions that may compromise evidence relating to a suspected security incident.

The Group shall establish and maintain appropriate processes for identifying, assessing, responding to, and recovering from information security and cybersecurity incidents.

Where required, incidents shall be escalated to Senior Management, the Board of Directors, relevant authorities, or other affected parties in accordance with applicable laws, regulations, contractual obligations, and Group procedures.

Business Continuity and Recovery

The Group shall maintain appropriate measures to support the availability and recovery of critical information, systems, and technology resources in the event of a disruption, cybersecurity incident, disaster, or other adverse event.

Critical information and systems shall be appropriately backed up, and backups shall be protected against unauthorized access, alteration, destruction, or compromise.

Where appropriate, recovery and business continuity arrangements shall be periodically reviewed or tested to assess their effectiveness.

Training and Awareness

The Group shall provide appropriate information security and cybersecurity training and awareness activities based on personnel roles and responsibilities. Personnel shall participate in relevant activities and remain vigilant in protecting the Group's information and technology resources.

Training and awareness activities shall cover relevant topics such as secure password practices, phishing and social engineering, protection of confidential information, safe use of Group technology resources, incident reporting, and other emerging cybersecurity threats.

Monitoring and Compliance

The Group shall monitor compliance with this Policy and relevant information security and cybersecurity requirements. Where non-compliance, weaknesses, or gaps are identified, appropriate corrective and preventive measures shall be implemented and monitored.



Policy Approval and Review

This Policy shall be reviewed periodically and whenever significant changes occur to the Group's business operations, technology environment, information security or cybersecurity risks, legal or regulatory requirements, or applicable industry standards.

This Policy was adopted by the Board of Directors on 19 Aug 2026.