

# ECOSCIENCE INTERNATIONAL BERHAD

(Registration No.: 202001024633 (1380953-M))

(Incorporated in Malaysia)

## RISK MANAGEMENT FRAMEWORK FOR INFORMATION TECHNOLOGY DEPARTMENT POLICY

### 1. Purpose

- a. This Policy is established to access the Information Technology risks that will potentially bring threat to the company business.

### 2. Scope

- a. It covers all Information Technology risk which directly affect product or work quality.

### 3. Responsibility

- a. HOD of Information Technology (IT)

### 4. Risk matrix

	Description	Extent and category of risk
1.	Low	<ul style="list-style-type: none"><li>Adverse impact of less than 10% of Group profit before tax, Group net revenue, net assets or shareholders' funds, whichever is the lowest.</li><li>Consequences can be absorbed under normal operating conditions.</li><li>No material impact on market share and/or reputation of company.</li></ul>
2.	Medium	<ul style="list-style-type: none"><li>Adverse impact of more than 10% but less than 30% of group profit before tax, Group net revenue, net assets or shareholders' funds, whichever is the lowest.</li><li>Potential impact on market share or reputation of company.</li></ul>
3.	High	<ul style="list-style-type: none"><li>Adverse impact of more than 30% of group profit before tax, Group net revenue, net assets or shareholders' funds, whichever is the lowest.</li><li>Market share, reputation or value of company will be affected in the short-term.</li></ul>

Risk rating matrix

Likelihood

Likely

Moderate

Unlikely

↑  
Likelihood  
↓

M	H	H
L	M	H
L	L	M

← Impact →

Insignificant

Moderate

Catastrophic

L - Low

M - Medium

H - High

**RISK MANAGEMENT FRAMEWORK FOR INFORMATION TECHNOLOGY DEPARTMENT POLICY****5. Risk management framework**

No	Risk identification	Risk measurement and assessment			Risk mitigation	Risk reporting and monitoring	Risk governance
		Likelihood	Impact	Severity			
1	Data breach	Low	High	Medium	Control have been in place to protect the confidentiality, integrity and availability of the data. Among all, adequate IT security layer, encryption protocols, virus scanning tools are in place.	In case of data breach identified, the IT rep will immediately report to management for the next action	Risk reduction
2	Back up data missing	Low	High	Medium	The data is back up in server and external hard disc on weekly basis	Total server failure report to be presented to management on yearly basis in case of any	Risk reduction and avoidance
3	Virus attack	Low	Medium	Low	Anti-virus is installed and updated frequently	Total failure report to be presented to management on yearly basis in case of any	Risk reduction
4	Data hacking / cyber attack	Low	High	Medium	Firewall is available to prevent system being hacked. Company IT system recovery in case cyber attack	In case of cyber-attack identified, the IT rep will immediately report to management for the next action	Risk reduction

**RISK MANAGEMENT FRAMEWORK FOR INFORMATION TECHNOLOGY DEPARTMENT POLICY**

No	Risk identification	Risk measurement and assessment			Risk mitigation	Risk reporting and monitoring	Risk governance
		Likelihood	Impact	Severity			
5	Downtime or technical failure of the "symphony" software	Low	Medium	Low	Software health check to be scheduled with the outsource vendor, and vendor standby for maintenance in case failure	Total failure report to be presented to management on yearly basis in case of any	Risk reduction and acceptance
6	Internet connection unstable or disturbance from TM	Low	Low	Low	IT team to connect TM in case observance of internet interruption	In case of internet disruption, IT rep will send disclaimer to the users	Risk acceptance

This Risk Management Framework for Information Technology Department Policy is adopted on 1st July 2020.