GALLANTT ISPAT LIMITED

(Formerly known as Gallantt Metal Limited)

CYBER SECURITY POLICY

INTRODUCTION

Gallantt Ispat Limited (GIL) demonstrates strong commitment towards cyber security and strives continuously to review and provide necessary means to strengthen the cyber security posture.

OBJECTIVE

The main objective of the policy is to –

- Prepare the business and employees to be ready to handle cyber incidents.
- Understand how to prevent an attack and to identify potential incidents.
- Identify the assets that are important to the business – financial, information and technology assets.
- Consider the risks to these and the steps needed to be taken to reduce the effects of an incident.
- Create roles and responsibilities so everyone knows who to report to if an incident occurs, and what to do next.

APPLICABILITY

This policy is applicable for all business operations of the Company. This is also applicable to all employees, consultants, contractors, associates, suppliers, third parties having access to the Company's information assets.

MONITORING AND DETECTION

The cyber security system of the Company shall be reviewed and monitored at regular intervals by the officials of the Information Technology (IT) Department of the Company. They shall check and identify any unusual activities that may cause damage to business information and systems. Unusual activity may include:

- accounts and your network not accessible
- passwords no longer working
- data is missing or altered
- hard drive runs out of space
- computer systems keep crashing

- customers receive spam from business account of the Company
- receive numerous pop-up ads

REVIEW

The IT Department shall –

- Identify if any systems and processes need improving and make required changes.
- Evaluate the incident before and after, and any lessons learnt.
- Update the cyber security structure of the Company and plan based on the lessons learnt so as to improve the security structure.

POLICY STATEMENT

GIL shall consistently thrive to upgrade the technology, systems, processes to be ahead of the curve from cyber security perspective and continuously protect internal information and information related to suppliers, customers, business partners and other stakeholders from unauthorised access.

GIL shall ensure that all Business/Department heads of the Company are directly responsible for ensuring compliance with the policy.