I G PETROCHEMICALS LIMITED
IT SECURITY POLICY

=============================

Policy

The risk of data theft, scams, and security breaches can have a detrimental impact on the Company's systems, technology infrastructure, and reputation. As a result, I G Petrochemicals Ltd. (IGPL) has created this policy to help outline the security measures put in place to ensure information remains secure and protected. The cyber security policy of the Company outlines the guidelines and provisions for preserving the security of the data and technology infrastructure.

Purpose

The purpose of this policy is to (a) protect IGPL's data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the Company's disciplinary process for policy violations.

Scope

This policy applies to all our employees, contractors, volunteers, and anyone who has permanent or temporary access to our systems and hardware.

The Policy deals with protection of Confidential Information, protection of personal and Company's devices, how to keep e-mails safe, managing passwords, security features for transfer of data, remote access, etc. All employees are obliged to protect the data and instructions are given on how to avoid security breaches.

Employees are advised to keep both their personal and Company's devices secured while trying to access official emails. It is also advised to avoid accessing internal systems and accounts from third party's devices or lending their own devices to others. Emails often host scams and malicious software and to avoid virus infection or data theft, necessary guidelines have been issued to counter the same. If an employee isn't sure about the safety of the email, they are to be referred to IT Team.

Transfer of data bears significant security risk to the Company. It is advised to approach IT team to transfer sensitive data to other devices or accounts, share confidential data over the company network/ system and not over public Wi-Fi orprivate connection, ensure that the recipients of the data are properly authorized people or organizations andhave adequate security policies, report scams, privacy breaches and hacking attempts, users are restricted to copy data from Company network to personal devices. Employees are expected to comply with our social media and internet usage policy.

IT Team need to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. IT Team must investigate promptly, resolve the issue and send a companywide alert when necessary.

The IT Team shall take appropriate security measures such as to install firewalls, anti-malware software and access authentication systems, arrange security training for all employees, inform employees regularly about new scam emails or viruses and ways to combat them, investigate security breaches, wherever required, thoroughly and follow this policies provisions as other employees do.

All employees are expected to always follow this policy and those who cause security breaches shall face disciplinary action.

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.