



CYBER SECURITY POLICY

Thomas Cook (India) Limited (hereinafter referred to as "TCIL / the Organization") recognizes that information is a critical business asset. Our ability to operate effectively and succeed in a competitive market with several legislative and regulatory requirements depends on our capability to ensure that business information is protected adequately through appropriate controls and proactive measures. Accordingly, TCIL is committed to the implementation of Information Security by establishing comprehensive processes through-out the Organization.

Business information must be protected from loss, theft, destruction, unauthorized alteration and unauthorized access. We are all aware of the internal / external threats from computer viruses, malwares, ransomwares, hackers and industrial espionage to information systems. Such incidents can have a serious impact on our competitive position and result in substantial damage to business and reputation.

The policy sets out the Management's strategy to address Information Security concerns and the responsibilities of employees to prevent breaches of security. You will be aware that your contract of employment requires you to maintain confidentiality of all the Organization's information. This requirement extends to protecting Organization's information stored on electronic systems and printed copies and hence you are responsible for the integrity of such information, whilst in your possession. It shall also be ensured that all legal, regulatory and statutory obligations are met. The Management is committed to provide the necessary guidance and support for the successful deployment of this Information Security Policy.