INFORMATION SYSTEMS ACCEPTABLE USE POLICY

Introduction

Information resources residing at various locations within the Company are strategic and vital assets. These assets shall be available and protected against accidental or unauthorized access, disclosure, modification or destruction. We need to manage the access, availability, integrity, utility, authenticity and confidentiality of information contained therein. This document outlines various aspects of acceptable practices for use of Information Assets. Every employee shall read this document and understand the policies and the implications of misuse/abuse.

Objective

The main objectives of this policy are:

- To ensure that all of the Company's information processing systems, data, other equipment and intellectual property are adequately protected against all threats to maintain the level of service required by GILAC to conduct its business
- To ensure that Company officials and employees are fully aware of the contractual, statutory or regulatory implications of any illegal/unauthorized use of software
- To limit the use of information systems to the business purposes for which such resources are intended
- To create within the Company an awareness of the need for information security to be an integral part of the day to day operation of every employee and ensure that all employees understand the importance of security to the Company and their responsibilities for maintaining security
- To make all the employees aware about, the processes that need to be followed for procurement, upgrade and disposal of IT assets
- To ensure that all intellectual property rights (IPR) of the owners are adequately protected and regulations related to information technology (IT) Security/ Intellectual Property Rights (IPR) and protection of customer data are adhered to

Scope

- This policy applies to all users of GILAC information and information systems within GILAC and non GILAC third party services providers for services related to hosting, SAAS etc. Such users include but are not limited to permanent employees, temporary employees, trainees, vendors, contractors, business partners and other related third party personnel
- In a case where a client/partner provides security policies and guidelines, it will be applicable addition to this Acceptable Use Policy. Where the two policies (the client's/ partner's policy and GILAC Acceptable Use Policy) are in conflict, the more restrictive of the two will be applicable, provided the business is not adversely affected