**[Company Name]**

**Policy**

Last Updated: [Insert Date (Month and Year)]

**1.0 Overview**

This policy is meant to protect [Company Name]'s employees, partners and the company from

illegal or damaging actions by individuals, either knowingly or unknowingly via any company-owned equipment/systems.

**2.0 Purpose**

This Policy covers the security and use of all [Company Name] information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment.

**3.0 Scope**

This policy applies to all [Company Name] employees, contractors and agents (hereafter referred to as ‘individuals’). This policy applies to all information, in whatever form, relating to [Company Name] business activities worldwide, and to all information handled by [Company Name] relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by [Company Name] or on its behalf.

**4.0 Policy**

**4.1 Individual’s Responsibility**

**4.2 Internet and Email**

**4.3 Clear Desk and Clear Screen Policy**

**4.4 Working Off-site**

**4.5 Mobile Storage Devices**

**4.6 Software**

**4.7 Viruses**

**4.8 Telephony (Voice) Equipment Conditions of Use**

**4.9 Actions upon Termination of Contract**

**5.0 [Company Name]’s Rights**

[Company Name] reserves the right to access, monitor, review, and release the contents and activity of an individual User’s account(s) as well as that of personal Internet account(s) used for company business. The company reserves the right to access any company owned resources and any non-company owned resources on company property, connected to company networks, or containing company data. This action may be taken to maintain the network’s integrity and the rights of other authorized Users. Additionally, this action may be taken if the security of a computer or network system is threatened, misuse of company resources is suspected, or there is a legitimate business need to review activity or data. This action will be taken only after obtaining approval from the Chief Information Officer or an authorized company office (e.g. Office of General Counsel, or Office of Audit and Compliance), or in response to a subpoena or court order.

**6.0 Non-Compliance Penalties**

We’ll investigate every breach of this policy. We’ll terminate any employee who willfully or regularly breaches our confidentiality guidelines for personal profit. We may also have to punish any unintentional breach of this policy depending on its frequency and seriousness. We’ll terminate employees who repeatedly disregard this policy, even when they do so unintentionally.

This policy is binding even after separation of employment.

**7.0 Misuse of Information Technology Resources**

Users must report all suspected or observed illegal activities to the Information Technology Department, their direct supervisor and/or an appropriate administrative office such as Human Resources or Security. Examples include theft, fraud, copyright infringement, illegal electronic file sharing, sound or video recording piracy, hacking, and viewing or distribution of child pornography.

Abuse of networks or computers at other sites through the use of company resources will be treated as an abuse of resource privileges.

**8.0 Revision History**

Last Reviewed:

[DATE]

Last Edited On:

[DATE]

By:

[EDITOR]