

Policy – Internet Security

1. Introduction

This policy provides guidance around internet security within the business, and aims to ensure that the confidentiality of client and business information is not compromised through the use of the internet.

2. Policy

It is our **policy** that:

- a. all employees must ensure that the confidentiality of client and business information is not compromised by the use of internet or email;
- b. all internet and email communications remain the property of XYZ Limited, and therefore must be of an appropriate nature, regardless of whether it is a business or personal communication.

3. Procedures

The following **procedures** shall ensure that this policy takes effect:

- a. Employees must not download files from the internet to XYZ Limited computers unless they are certain of the integrity of the sender and have obtained authorisation from the CEO or COO.
- b. Employees are not to open or send emails that contain any files that may contain a virus, and are responsible for any personal information they may enter via the internet or email through a XYZ Limited computer.
- c. Employees must obtain permission from their Manager before sending any client information by email.
- d. XYZ Limited retains the absolute right to monitor all internet and email usage on a regular basis, regardless of its nature.

4. Further References

Refer to the:

1. Email Use policy
2. Confidentiality policy
3. Code of Conduct