ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS – POLICY

(Control 5.10)

Introduction

This policy applies directly to all personnel and external party users of 121 BPO. The policy has been issued with the authority of the CEO/Managing Director, and compliance with its principles is mandatory for all users of the Company's information or information systems.

Control

Rules for the acceptable use and procedures for handling of information and other associated assets should be identified, documented, and implemented.

Purpose

To ensure information and other associated assets are appropriately protected, used, and handled.

Scope

All equipment and information (all information systems, hardware, software, and channels of communication, including voice telephony, social media, video, email, instant messaging, internet, and intranet).

Policy

Senior Management understands that there are rules required for the acceptable use of information and of the assets associated with that information and information processing facilities and that these rules should be identified, documented, and implemented. To this end the Company has produced this policy aligned to the requirements of ISO/IEC 27001:2022:

- Personnel are responsible for complying with the Company's policies when using the Company's information sources. If requirements or responsibilities are unclear, please seek assistance from the Information Officer, IT Manager or from Senior Technical Support.

- Personnel must promptly report harmful events or policy violations involving the Company's information or assets to the Information Officer and IT Manager or the Senior Technical Support person. Events include, but are not limited to the following:

    - Technology incident
    - Data Incident
    - Unauthorised access incident
    - Physical security incident
    - Policy violation

- Personnel should not purposely engage in an activity that may:
    - Harass, threaten, impersonate, or abuse others
    - Degrade the performance of the Company's information sources
    - Deprive the Company's authorised personnel access to information resources
    - Obtain additional resources beyond those allocated
    - Or circumvent the Company's computer security measures

- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system.

- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information developed using the Company's information resources will remain the property of the Company.

- Use of encryption should be managed in a manner that allows authorised personnel to promptly access the information

- The Company's information and associated assets are provided to facilitate company business and should not be used for personal financial gain

- Personnel are expected to cooperate with incident investigations

- Personnel are expected to respect and comply with all legal protections provided by patents, copyright and trademarks, and intellectual property rights for any software or materials viewed, used, or obtained using the organisation's information resources

- Personnel should not intentionally access, create, store, or transmit material which the Company may deem to be offensive, indecent, or obscene.

- As a Company we use different methods of system monitoring, both proactive and reactive, they are:

  a) Firewall limits access safe websites and reports on deviations
  b) Anti-Virus installed on each device, which prevents and alerts any threats
  c) Anti-Virus scheduled system wide scan multiple times per week
  d) Prevent access to USB ports for unauthorised personnel
  e) Securing information for authorised personnel
  f) Encryption used on staff devices