ALPHA NERO

# Documents, Confidential Information, and IT Policy

To meet the business objectives and ensure continuity of its operations, Alpha Nero shall adopt and follow well-defined and time-tested plans and procedures, to ensure that sensitive information is classified correctly and handled as per organizational policies. Information is considered as primary asset of the company. Alpha Nero uses different types of information assets. The sensitivity of these information assets may vary and similarly, their handling mechanisms are also different.

The purpose of this policy is to ensure personal information, documents, confidential information and information technology usage is protected from unauthorized use and disclosure. This policy helps to facilitate the identification of information to support routine disclosure and active dissemination of information. It also helps to protect the intellectual property of the company.

## Document Retention

Alpha Nero requires to maintain corporate records and expects all employees to fully comply with our corporate record retention. Employees must preserve those records until the company determines that the records are no longer desirable, needed or looked for. If an employee believes that this exception may apply, or has any questions regarding the applicability of this exception, please contact Operations Manager.

When reduced to written or electronic form, all documents and files shall be marked "COMPANY CONFIDENTIAL." Notwithstanding this requirement, unmarked documents and files may still subject to this Policy and must be protected accordingly

Systems users shall NEVER:

- allow anyone else to use their system privileges;
- share their user names or passwords with anyone else;
- exceed their authorized access;
- copy to a non-Company computer system.

Systems users shall secure their usernames and passwords to prevent unauthorized use, and shall properly log out of systems when they have completed use.

When any Employee leaves the Company, the HR representative shall notify the system administrator to arrange for immediate termination of the Employee's accounts upon his or her departure from the Company.

Documents and electronic files not contained within computer systems (e.g., on flash drives) containing company information shall be properly secured at all times in a locked office, drawer or safe. Such documents and electronic files shall not be left unattended in an accessible location at any time.

Where feasible, a system (e.g. a physical log or computer security program) shall be maintained for tracking access to documents or systems that contain trade secrets such as formulas, production processes and new developments/inventions.

When any physical document is no longer needed, it must be shredded. When any electronic file is no longer needed, it shall be properly deleted so as to be unrecoverable using ordinary means.

**Electronic Communications**

Employees have access to the company's electronic communication system, which includes computers, telephones (including Company-issued cell phones or smart phones), voice mail, e-mail and the Internet when accessed through a company computer. The purpose of this system is to enhance job performance on day-to-day assignments and to facilitate effective business communications. Employees' actions and communications on the company's electronic communication system may be attributed to the company, which could be held responsible for Employees' actions. Therefore, this policy outlines the proper uses of the electronic communication system.

- **Ownership.** The Company's electronic communication system is Company property. All messages, information, and data sent and received by the electronic communication system are Company property. Incidental and occasional personal use of the electronic communication system is allowed, but such use will be subject to this policy and any resulting messages and data are the property of the Company.

- **No privacy**. Even though Employees have unique user log-in identification codes and passwords to access the electronic communication system, Employees have no privacy in the use of any part of the electronic communication system or in any documents, messages or information created on, with or transmitted over the system. The Company has access to the system and maintains the right to access and monitor, consistent with the law, all documents, messages and information created on, with or transmitted over the system, including e-mail and Internet usage, without notice to Employees.

  All such documents, messages, and information can be reviewed by the Alpha Nero.

- **Monitoring.** The Company reserves the right to monitor and access the electronic communication system and all documents, messages or information created on, with or transmitted over the system. These Company rights will be exercised strictly in accordance with applicable law, the Company's business purposes (which include ensuring the appropriate use of the system), and in cooperation with requests from law enforcement. The Company also reserves the right to disclose such documents, messages, or information when consistent with the Company's business purposes and with requests from law enforcement.

- **No offensive use.** Employees accessing the electronic communication system are identifiable as Employees of the Company. Employees therefore must recognize that they may be viewed as representatives of the Company when they access the system and they must conduct themselves appropriately. Employees may not use the electronic communication system in an offensive, harassing, illegal, or defamatory manner.

- **Confidential information, solicitation, and illegal activities.** Employees may not improperly disclose confidential Company information and materials in any manner, including via the electronic communication system.

- **Copyrights, trademarks, and patents.** Employees must not violate copyrights, trademarks, or patents. An Employee may not copy, download, or use any image, text, video, audio material, software, or other copyright-protected, trademark-protected, or patented data without appropriate authorization. This restriction applies to copying copyrighted, trademarked or patented materials from someone else, the local area networks, or the Internet.

- **Software.** The Company expressly prohibits the unauthorized use or duplication of copyrighted software. The Company will provide legally acquired software to meet the legitimate Company software needs in a timely fashion and in sufficient quantities for all Employees.

- **Electronic communication system and data.** Only Company authorized software and related encryption software tools may be used in connection with the Company electronic communication system and all related data. Employees shall not use non-Company licensed or owned software or encryption software tools. The Company prohibits Employees from using any software or encryption software tools to access Company data located on the Company electronic communication system, unless authorized to do so. Employees shall not disassemble, decompile, reverse engineer or tamper with any software or encryption software tools to prevent the Company from accessing or recovering any and all encrypted information.

- **Right to search.** The Company reserves the right to inspect and search all computers, electronic devices, and components of the electronic communication system found on Company property without notice to ensure that Employees are complying with this and other Company policies. Such inspections and searches will be conducted in accordance with all applicable laws.

- **Off duty conduct.** An Employee who maintains a web site must not use Company equipment or working time to maintain the web site. Any off duty online conduct by an Employee must not interfere with the Employee's ability to perform his or her job effectively, and must not adversely affect productivity and positive interactions in the workplace.

**Confidential Information**

During employment and any time after leaving the Company, Employees shall not use or disclose any information without prior authorization of the Company.

Every employee as a result of their lengthy service and involvement in key confidential areas has acknowledged and agreed to sign a Non- Disclosure Agreement (NDA) relating to trade secrets, inventions, and proprietary information which, in the company’s view, binds beyond

the cessation of their employment.

A great deal of what they are involved in falls within the agreement which forbids to disclose or utilize any proprietary, confidential information or trade secrets which you have acquired in respect of any business of the company, its subsidiaries, affiliates and/or relating any other dealing or affairs of the company including and not limited to:

- Clients and suppliers
- Proposals and negotiation
- Customer contracts and communications
- Designs and materials
- Price and structures
- Installations

Every employee is accountable and abide to track the confidentiality agreement while employed with Alpha Nero. Any employee found to have violated the Confidentiality Agreement is subject for disciplinary action which include immediate termination.

Attached in this policy are Procedure for Control of Documented Information and Non-Disclosure Agreement (NDA). Failure to adhere to the requirements of this Policy may result in disciplinary action up to and including immediate termination.

**Simon Hacker,**

Managing Director




ALPHA NERO FZ LLC - Dubai Production City- IMPZ - Plot C 07 – Dubai – P O BOX 485008 Tel : +971 44270592 Fax : +971 44278154 - www.alpha –nero.com