Acceptable Use Policy

1. Overview

Nicholas Financial Inc.'s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Nicholas Financial's established culture of openness, trust and integrity. The Company is committed to protecting employees, partners, customers and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Nicholas Financial. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Nicholas Financial employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Nicholas Financial. These rules are in place to protect the employee, our customers and Nicholas Financial. Inappropriate use exposes Nicholas Financial to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Nicholas Financial business or interact with internal networks and business systems, whether owned or leased by Nicholas Financial, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Nicholas Financial and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Nicholas Financial policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Nicholas Financial. This policy applies to all equipment that is owned or leased by Nicholas Financial.

4. Policy

4.1 General Use and Ownership

4.1.1 Nicholas Financial proprietary information stored on electronic and computing devices whether owned or leased by Nicholas Financial, the employee or a third party, remains the sole property of Nicholas Financial. You must ensure that proprietary information is protected.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Nicholas Financial proprietary information.

4.1.3 You may access, use or share Nicholas Financial proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. The Company is responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems.

4.1.5 For security and network maintenance purposes, authorized individuals within Nicholas Financial may monitor equipment, systems and network traffic at any time.

4.1.6 Nicholas Financial reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with Nicholas Financial's access procedures.

4.2.2 System level and user level passwords must comply with the company's password policies. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from a Nicholas Financial email address to newsgroups are prohibited.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Nicholas Financial authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Nicholas Financial-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Nicholas Financial.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Nicholas Financial or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting Nicholas Financial business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Nicholas Financial computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Nicholas Financial account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to Nicholas Financial's IT department is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the Nicholas Financial network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, Nicholas Financial employees or customer to parties outside Nicholas Financial.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Questions may be addressed to the company's main corporate mailing address or web site.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within Nicholas Financial's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Nicholas Financial or connected via Nicholas Financial's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using Nicholas Financial's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Use of Nicholas Financial's systems to engage in blogging is prohibited.

2. Nicholas Financial's Confidential Information policy also applies to all social media. As such, Employees are prohibited from revealing any of Nicholas Financial's confidential or proprietary information, trade secrets or any other material covered by Nicholas Financial's Confidential Information policy when engaged in blogging or social media posting of any sort.

3. Employees shall not engage in any social media posting or blogging that may harm or tarnish the image, reputation and/or goodwill of Nicholas Financial and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when using social media or otherwise engaging in any conduct prohibited by Nicholas Financial's *Non-Discrimination and Anti-Harassment* policy.

4. Employees may also not attribute personal statements, opinions or beliefs to Nicholas Financial when engaged in social media posting or blogging. If an employee is expressing his or her beliefs and/or opinions in social media posts or blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Nicholas Financial. Employees assume any and all risk associated with social media posting or blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Nicholas Financial's trademarks, logos and any other Nicholas Financial intellectual property may also not be used in connection with any social media or blogging activity

5. Policy Compliance

5.1 Compliance Measurement

The Company team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the company's management in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Processes

- Nicholas Financial Email Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

I understand and agree to terms and stipulations set forth in this Acceptable Use Policy statement.

_____

Employee Printed Name

_____

Employee Signature Date

PLEASE RETURN THIS FORM TO THE HUMAN RESOURCES DEPARTMENT.

IT WILL BE PLACED IN YOUR PERSONNEL FILE.

7. Revision History

Date of Change	Responsible	Summary of Change