# NTS INFORMATION TECHNOLOGY POLICY

## Business Communications

NTS utilizes various forms of communication tools to convey business communications to various individuals and entities, including customers, suppliers, independent contractors, and vendors. NTS permits employees to utilize those communication tools upon the condition that such use is business-related and professional at all times. Those communication tools include without limitation: telephones, smart phones, iPads (or similar device), voice-mail, pagers, electronic mail (including Instant Messaging and texting), letters, fax machines, modems, servers, computers, network tools (like browsers and Internet access facilities) and any other means of communication. All communications made on behalf of NTS, whether oral, written, or visual, are business communications. Therefore, the entire communication (including the content, the greeting, the salutation, the farewell, and the signature) shall be business-related and professional at all times. This policy does not prohibit employees from discussing the terms and conditions of their employment.

For example, verses, stories, quotations, sayings, electronic art, mottos, pictures, cartoons, graphics, jokes, chain letters, winners pool, other forms of gambling, or personal religious or political messages shall not be included in any NTS business communication. The Executive Vice President, in his sole discretion, may authorize (in advance) the use of certain quotations, graphics, and electronic art -- for business-related purposes. Additionally, the communication of (including the creating, sending, forwarding, or posting of) profane, sexually-explicit, suggestive, discriminatory or harassing statements or images, any message or image having an illegal or immoral purpose, or any statement/image violative of any NTS workplace policy is prohibited. Finally, NTS' communication tools never shall be used for personal financial gain.

## Electronic Communications

**Introduction**. NTS utilizes computers (including e-mail and the Internet), fax machines, communication devices (e.g., smart phone, iPad) and phone mail systems to transmit and receive business-related information. NTS business shall be conducted on NTS-provided computers, fax machines, communication devices, and/or phone mail systems unless the employee receives prior authorization from the Executive Vice President to conduct NTS business on his personal computer, communication device, fax machine, and/or phone mail systems. If so authorized, the employee's use of those personal communication tools to conduct NTS business shall not violate this policy or any other NTS workplace policy. An effort must be made to ensure that accuracy, security, and control of information are maintained. In that regard, Confidential Information shall never be transmitted or exchanged through instant messaging.

Employees, including those who are provided access to the Internet or other public networks, or access to an NTS-provided communication device, should not abuse the availability of the systems or equipment. Employees shall use NTS' computer and phone systems (including phone mail), communication devices, and the fax machines in an authorized, professional, legal, and ethical manner. They shall not be used to violate any applicable laws or legal requirements including, without limitation, the use of NTS' facilities and/or resources to attempt to gain access to third party systems (e.g., competitors, customers, vendors, suppliers). NTS may terminate any employee's access to such systems and devices and take other appropriate disciplinary action in the event the use of such systems or devices is not in accordance with this policy or other NTS policies. Civil and/or criminal liability may also arise from such unauthorized use. Any employee who witnesses or has information about a possible violation of this policy should immediately report it to the Director of Human Resources or the Executive Vice President.

NTS considers e-mail a form of business communication and the language used in all emails should reflect a business tone. Avoid typographical errors as well as misspelled words and poor grammar. Because they are difficult to read and comprehend, using all capital letters, all small letters, incorrect or nonexistent punctuation, shorthand, idioms, emoticons, unfamiliar acronyms, and slang should be avoided.

**Ownership and Control**. The computer, fax machine, NTS-provided communication devices, and phone systems are owned by NTS. Those communication devices and equipment are provided to employees in conjunction with NTS' business and the employee's job responsibilities. All messages and information communicated through them are NTS property. NTS may monitor, inspect, or access its fax machines, phone mail system, communication devices, and/or computers at any time with or without notice. This includes, without limitation, Internet or other public network sites visited by employees, phone mail, phone usage, screen savers, software, file downloads, news groups, and any and all Instant Messaging and e-mail communications sent and received by employees. NTS also may retrieve and/or disclose any information or material stored on its phone mail, fax machine, communication devices, and computer systems. Whether or not the communication is password-protected, there is no expectation of privacy in any matter, whether business-related or personal, created, received, accessed, stored, or sent from any NTS computer, fax machine, communication device, or the phone mail system.

Additionally, NTS may utilize software that enables it to identify and block access to certain Internet sites and certain incoming e-mails. NTS may also utilize software to monitor Internet site(s) visited, Instant Messaging, and any other use of the Internet or other public network.

**Security**. The Internet is not under either NTS' or the addressee's control. Accordingly, care should be taken in determining whether to transmit information or documents (especially those containing Confidential Information) over the Internet or other public network. Where encryption is required for a particular transmission, employees must follow the encryption procedure. Any questions regarding encrypted transmissions should be directed to the Chief Information Officer ("CIO"). In addition, employees must be careful to prevent computer viruses and unlawful or offensive material from being brought into NTS' network from the Internet or other public networks. All authorized files downloaded from the Internet or other public networks must be checked for possible computer viruses. Employees should never download files from the Internet or other public networks, accept e-mail attachments from unknown outsiders (including customers, suppliers, independent contractors, and vendors), or use disks or other storage devices (e.g., mass storage drives, memory sticks) from non-NTS sources without first scanning the material with NTS-approved virus-checking software. The virus scanning software runs automatically and should not be disabled unless you receive prior written authorization from the CIO. If you suspect a virus has entered NTS' network, immediately notify the CIO.

To enhance the security environment and avoid the spreading of viruses, authorized employees accessing the Internet or other public networks through a computer attached to NTS' network must do so through an approved Internet firewall or other security device. Bypassing NTS' computer network security by accessing the Internet or other public networks directly by modem or other means is strictly prohibited unless the computer you are using is not connected to NTS' network and you have received prior written authorization from the CIO to do so.

Additionally, employees shall not: share any e-mail, computer, or phone mail passwords; provide e-mail, computer, fax machine, communication device, or phone mail access to an unauthorized employee or individual; or access another employee's e-mail, computer, fax machine, communication device, or phone mail without prior written authorization from the CIO. All employees shall password protect access to their workstation computer and/or communication device pursuant to I.T. security protocols. Moreover, unless the prior written approval of the CIO has been obtained, employees shall not establish Internet or

other public network connections that could allow unauthorized persons to gain access to NTS' systems and information. Those connections include, without limitation, the establishment of hosts with public modem dial-ins, World Wide Web home pages and File Transfer Protocol.

Employees also shall not (or attempt to) bypass NTS security to access or alter information without prior written authorization from the CIO. No one is authorized to service or "troubleshoot" or alter NTS' computer system (or permit someone else to do it) without prior written authorization from the CIO.

For confidentiality and conserving resources reasons, all NTS computers (e.g., CPU, monitor, speakers) shall be shut down and turned off at the end of your work day.

**Restrictions on Use**. Access to the Internet or other public networks shall be given only to certain authorized employees based on work requirements. Such Internet or other public networks access authorization shall be approved, in advance and in writing, by the CIO.

**Limited Personal Use**. During your NTS employment, an infrequent and minimal amount of personal use of the computer system or provided communication device – including e-mails (as determined in NTS' sole discretion) is permitted during your work time so long as it does not: (1) interfere with your job performance; (2) violate this policy or any other I.T. security or NTS workplace policy; (3) consume significant resources; (4) give rise to more than nominal additional costs; (5) interfere with NTS operations; or (6) interfere with other employees' work time. Under no circumstances, however, shall an employee utilize NTS' computer system or communication devices to play games or to surf or browse inappropriate or offensive site(s). Even though NTS permits some limited personal use of its computer system or communication devices, and whether or not the communications are password-protected, there is no expectation of privacy in any matter, whether business-related or personal, created, received, accessed, stored, or sent from NTS' computer system or communication devices.

Employees shall choose a screen saver and wallpaper from the choices offered by their workstation operating system or from a NTS-authorized source. Employees shall not load or download images for use as a screen saver or wallpaper on their workstation or NTS-provided communication device (e.g., smart phone, iPad) from the Internet or other public network, CD, diskette, or other medium.

**Unacceptable Use**. The creating, viewing, sending, forwarding, or posting of profane, sexually-explicit, suggestive, discriminatory, or harassing statements or images (including those that violate NTS policies regarding equal employment opportunity, discrimination, or harassment) in or from NTS' computer, fax machine, phone systems, or communication devices is prohibited. This expressly includes all personal political and religious quotes, statements, beliefs or commentary. Inappropriate e-mail messages also include, without limitation: chain letters; blast e-mails; jokes; cartoons; stories; electronic art; lottery, winner pools or other forms of gambling; fund raising; solicitations; or any message or image having an illegal or immoral purpose. NTS' phone, fax machine, computer systems, or provided communication devices shall not be used for personal financial gain or to solicit others for activities unrelated to NTS' operations, or in connection with political campaigns, lobbying, or religious purposes. Loading and downloading software for game playing is prohibited. The phone (including smart phones), fax machine, NTS-provided communication devices, and computer systems are part of NTS' workplace, and NTS' policies on workplace conduct are fully applicable.

**Attachments and Links**. Employees must exercise extreme caution when attachments and links are part of an e-mail message. Only attachments or links from known and trusted sources may be opened. If any doubt exists, employees must not open attachments or links as they may contain a virus.

**Transmittal of Confidential Information**. Phone mail and email may be as permanent as hard copy communications and may be stored indefinitely, forwarded to others, inadvertently transmitted to the wrong person, or copied/printed and passed on, generally without the knowledge or consent of the originator. Disclosure of e-mail messages is subject to the same procedures applicable to other written communications and the sharing of information. Accordingly, Confidential Information (defined in the Employee Handbook) shall only be transmitted or forwarded to the authorized and intended recipient(s). Employees also shall not print e-mail messages unless the message first has been opened, read, and determined not to be in violation of this policy.

**Deleting Items**. Unless instructed otherwise by the Executive Vice President or the CIO, please delete items (e-mails, attachments, links) that are no longer needed for business purposes from your Inbox, Sent, and Deleted Items boxes. Although an item may be "deleted", it may remain in the system and later be retrieved.

**Tampering with NTS Website or Web Pages**. Tampering with or altering NTS' website or web pages, without express prior written authorization from the CIO, is strictly prohibited. Creating unauthorized or unofficial websites, web pages, or social network sites concerning NTS' customers, products, services, vendors, suppliers, independent contractors, or NTS' Confidential Information (as defined in this Handbook) is prohibited.

**Use of NTS' Intellectual Property**. No NTS Confidential Information (defined in the Employee Handbook) shall be placed on any public network, whether from an NTS computer or an employee's personal computer, without the prior written authorization of the Executive Vice President. Confidential Information does not include information concerning the terms and conditions of your employment.

**Copyright**. Employees shall not infringe any party's copyright or other intellectual property rights, and employees should not use NTS' systems to download or distribute copyrighted software or data or programs designed to circumvent the security of other computer systems. Distributing an article electronically may be the same as copying it on a copy machine. Employees shall not copy protected material inadvertently and should pay particular attention to forwarding copyrighted materials to others or printing them for later distribution. Do not ignore copyright notices that appear on documents and bear in mind that even if there is no copyright notice, the materials may still be protected by copyright.

**Software Code of Ethics**. Unauthorized duplication of copyrighted computer software violates the law and is contrary to NTS' Business Code of Conduct. NTS forbids such copying and states the following:

- NTS will neither engage in, nor tolerate, the making or using of unauthorized software copies under any circumstances.
- NTS will provide legally acquired software to meet the legitimate software needs in a timely fashion and in sufficient quantities for all our computers.
- NTS will comply with all license or purchase terms regulating the use of any software we acquire or use.
- NTS will enforce strong internal controls to prevent the making or using of unauthorized software copies, including effective measures to verify compliance with these standards and appropriate disciplinary measures for violation of these standards.

## SOCIAL MEDIA

**Facebook Page.** Each NTS Facebook page promotes its message to a growing network of social media users. Content on any NTS social media site should promote NTS' business, generate revenue, and foster interaction with the general public and our customers. NTS, in its sole discretion, retains the right to monitor, access, change, and/or terminate any NTS-administered social media site.

All NTS-administered social media sites will be approved by the CIO. The CIO will monitor content and questions in addition to active recruitment of new subscribers or "fans." If the CIO is unavailable, a backup Manager (selected by NTS) will be responsible for postings and/or site management.

NTS retains control over its social media sites. It will not publish and/or will remove material (once discovered) that is contrary to its policies and procedures, including without limitation, its policies against workplace harassment, discrimination, and violence.

**Business Use of Social Media Sites.** NTS understands that social media tools such as content-sharing websites, blogs, micro-blogs, online forums, and other digital channels established for online interaction and connection are rapidly becoming popular channels of communication. Examples include Facebook, MySpace, Twitter, LinkedIn, Flickr, Live Journal, Tumblr, and YouTube. If you have a business-related need to use social media sites during your work time, you must secure prior approval from the Executive Vice President.

Social media activity on NTS equipment and devices (e.g., laptops, iPads, and NTS-issued phones) is not private. NTS may monitor and preserve any and all use of social media on NTS devices and equipment, including all posts, communications, and sites visited, whether or not password protected, at any time.

This policy establishes required procedures for authorized NTS employees who have a business-related need to use social media sites to communicate about NTS' products and services, including any NTS-hosted social media site. NTS emphasizes there is a big difference between speaking "on behalf of NTS" and speaking "about NTS." Only certain designated employees have authority to speak on NTS' behalf. This policy is not intended to interfere with an employee's legally protected rights or to prohibit communications protected by law. This "Business Use" section does not apply to your "personal use" of social media sites -- which is discussed in the next section.

- **Follow NTS' Policies**. Do not publish any material that would be contrary to NTS' policies and procedures, including without limitation, its policies against workplace harassment, discrimination, violence, and its policies on Confidential Information and intellectual property.

- **Respect Intellectual Property**. Respect the intellectual property of NTS and others. Do not post or link to any material that violates the intellectual property (including, without limitation, copyright, trademark, trade secrets, and patents) of others or of NTS.

- **Provide Accurate Attributions**. Never claim authorship or ownership of someone else's work product or provide false information regarding authorship or ownership of someone else's work. If you are reproducing someone else's work in compliance with applicable intellectual property laws, you should not alter or remove authorship or ownership information that has been provided in connection with the copy of the work that is being reproduced.

- **Know the Site's Rules**. Every social media site in which you communicate online has its own rules – often called Terms and Conditions. You must respect those site's rules. They may be

more restrictive than you might assume. Therefore, you must be knowledgeable about the scope of your online activities within the context of each site's rules.

- **Confidential Information.** Do not disclose NTS' confidential or proprietary business information and trade secrets ("Confidential Information") to persons outside of NTS without prior written authorization from the Executive Vice President. Confidential Information also can include non-public information about our suppliers, vendors, customers, and business partners that has been disclosed to NTS under obligations of confidentiality. Do not cite or obviously reference NTS' suppliers, vendors, customers, or business partners without their prior approval (confirmed with a signed authorization/release form) from them and the Executive Vice President. Confidential Information does not include information concerning the terms and conditions of your employment.

- **Identify Yourself Accurately and Be Transparent.** Be transparent and honest. If you are speaking on NTS' behalf, then honestly disclose your identity and affiliation with NTS. Never create or use an alias or otherwise communicate anonymously. If you identify yourself as an NTS employee on a social media site, and you have not been specifically authorized by the Executive Vice President to speak on NTS' behalf as a spokesperson, then make it clear your posts (or views) are your own and do not represent NTS' views.

- **Respect Work Time**. Only employees who specifically have been authorized to perform online activity related to their NTS responsibilities are permitted to conduct social media activities during their work time. Personal social media activities should be conducted on your non-work time (e.g., authorized rest and meal breaks) on your personal communication device.

- **Accountability**. Be mindful that what you write will be public for an indefinite period of time – even if you attempt to modify or delete. Take time to make sure your posts are complete and accurate. Never knowingly communicate untrue or deceptive information. Be careful and considerate. Please understand you may be subject to liability if your material is found to violate any applicable local, state, or federal law. Civil and/or criminal liability may arise if your postings include copyrights, trademark, trade secrets, patents, or Confidential Information (e.g., text, videos, music, etc.) belonging to others.

- **Online Comments By Others About NTS' Products/Services.** Even if you are not a designated NTS spokesperson, you may play an important role in monitoring the social media landscape. If you discover positive or negative online comments about NTS' products and services that you believe are important to share, please contact the Executive Vice President. Unless you are a designated spokesperson, do not personally respond to negative posts about our products and services. This ensures accuracy, facilitates a consistent message, and avoids unnecessary confusion concerning who officially is speaking on NTS' behalf.

- **Global Significance.** The way you communicate online might be accurate in some parts of the world, but inaccurate (or even illegal) in others. Keep that "world view" in mind when participating in online conversations. When in doubt, consult the Executive Vice President.

- **Forward Business-Related Inquiries.** If the news media or a blogger contacts you about your business-related posting, please refer that person to the Executive Vice President so the inquiry can be directed to the appropriate and authorized NTS representative.

**Personal Use of Social Media Sites.** Whether an NTS employee opts to create or participate in social media sites for personal reasons is his or her own decision. "Personal" use of social media is any participation that is not authorized by NTS. Your use of social media sites through NTS equipment must be job-related for an approved social media application/project. Personal social media activities should be conducted on your non-work time (e.g., authorized rest and meal breaks) on your personal communication device(s).

While generally what you do on your own time is not NTS' concern, anything you post will ultimately be your responsibility. Your personal online communications are individual interactions, not NTS communications. If you choose to participate in a social media site, please exercise sound judgment and common sense. You should not post anything that would be contrary to NTS' workplace policies, including its policies against workplace harassment, discrimination, and violence. Additionally, note the following:

- **Confidential Information**. Do not disclose NTS' confidential business information and trade secrets ("Confidential Information") to persons outside of NTS without prior written authorization from the Executive Vice President. Confidential Information includes non-public information about our suppliers, vendors, customers, and business partners that has been disclosed to NTS under obligations of confidentiality. Do not cite or obviously reference NTS' suppliers, vendors, customers, or business partners without their prior approval (confirmed with a signed authorization/release form) from them and the Executive Vice President. Confidential Information does not include information concerning the terms and conditions of your employment.

- **Manager "Friending" or "Following" of Employees Prohibited.** Managers must be mindful of the content of their oral, written, and electronic communications with fellow employees. NTS, therefore, prohibits managers from "friending" or "following" (or the language equivalent) NTS employees on Facebook or any other type of social media. Without devoting the necessary thought and focus to them, online communications can be hurried, incomplete, unprofessional, and/or far too casual. As a result, those postings may lead to misperceptions, misunderstandings, and potential conflicts of interest. If an employee expresses disappointment with this policy, please refer them to the Executive Vice President for further explanation.

- **"Friending" or "Following" Customer Representatives.** Employees should be mindful of the content of their personal oral, written, and electronic communications with customers or customer representatives. Without devoting the necessary thought and focus to them, online communications can be hurried, incomplete, unprofessional, and/or far too casual. As a result, those postings may lead to misperceptions, misunderstandings, and potential conflicts of interest. If, for some reason, you choose to "friend" or "follow" a customer representative(s), understand that NTS' various workplace policies may apply.