NORFOLK SOUTHERN CORPORATION

Terms and Conditions Governing the Use of Norfolk Southern Corporation Information Technology Assets

This document establishes the terms and conditions under which a person (“user”) has access to and makes use of the various information technology assets (“NSITA”) of Norfolk Southern Corporation or any of its subsidiaries or affiliates (collectively “NS”). These terms and conditions are taken from and are a portion of the Norfolk Southern Information Security Policies and Processes Documents (ISPPD). While these terms and conditions govern the access and use of the NSITA by all persons, NS employees and other designated persons remain subject also to the full terms and conditions of the NSISPPD.

By accessing and using the NSITA, the user agrees to be subject to and comply with the following:

I. General

All users have a responsibility to protect NS’ information assets. In addition, all users must comply with all federal, state, and local laws, statutes, and regulations that relate to the control and authorized use of NS’ Information Technology Infrastructure.

Users are authorized access to only the information systems and infrastructure necessary to perform their assigned job duties and to which they have been authorized access by NS.

Violations of these terms and conditions are grounds for disciplinary action up to and including termination of employment, civil action, and/or criminal prosecution. NS will also pursue and prosecute, where deemed appropriate, any user who accesses or uses, or attempts to access or use, any NSITA (including, but not limited to, any NS computer, computer system, application, communications system or network) without proper authorization.

Users entering the NSITA will be presented with a click agreement and warning/notice banner. Users must agree to the terms and conditions specified in the banner before being granted access. Clicking past the banner constitutes agreement to all specified terms and conditions of usage set out in this document.

II. Passwords

- Passwords must have at least eight (8) alphanumeric characters.
- Passwords should contain at least one alphabetic character (a-z), one numeric character (0-9), and should contain one special character such as ‘@’, ‘#’, or ‘$’.
- Regardless of the circumstances, passwords must never be shared or revealed to anyone. This includes sharing passwords of other users.
- In the event a user suspects his/her password is compromised in any way, the user should immediately change the password and notify his/her supervisor, manager, SPOC and NS Information Security.
- Any user must not configure or program any computing device or software package to avoid manually entering their password.
- Users should choose passwords that cannot be easily guessed. Passwords should <u>not</u> be related to the user’s ID, job or personal life. For example, a car license plate number, a spouse’s name, an address, proper names, places, and slang should not be used.

- Users should not construct passwords that are identical or substantially similar to passwords that they have previously employed.
- Users should not construct passwords made up of a certain number of characters that do not change combined with a certain number of characters that predictably change. For example, users should not employ passwords like "X34JAN" in January, "X34FEB" in February, etc.
- Users should memorize their passwords and should not record them in any manner.
- Users must ensure that individual authentication information, such as user IDs, passwords, tokens, and smart cards, are not disclosed to or used by any other person.
- Users must immediately change passwords to systems if compromise is suspected, and notify the Security Point of Contact (SPOC) or the NS Information Security Department.

III. Security

- Users must comply with all controls established by the information asset owner.
- Users must use information only for the purpose intended or expressly permitted by the information asset owner.
- Degaussing will be used to render information unreadable on magnetic storage devices that are to be reused.
- Electronic media not planned to be reused or sold must be physically destroyed, rendering the media unusable and effectively preventing the sensitive information from being extracted.
- Users must ensure that terminals, PCs, or workstations are disabled from unauthorized use. This means that users must log out of or lock systems when machines are left unattended. During off-duty hours, users should log off unless there are processes running on the system, in which case, the system must be locked. In some instances a terminal, PC, or workstation in a restricted area may need to be left in non-logged off and non-locked status. The department that has such a need should obtain a variance from NS Information Security.
- Users must immediately report suspected security violations to their supervisor, Security Point of Contact (SPOC), NS Information Security, or Internal Audit.
- Users should not open suspicious programs or e-mail attachments from any source.

IIII. Restricted or Confidential Information

- Users must not disclose or release to any third party individual or organization any information or data unless such disclosure is authorized as part of the job responsibilities of the user. Furthermore, users must ensure that RESTRICTED or CONFIDENTIAL information (collectively "RESTRICTED information") is not disclosed to unauthorized individuals without the permission of the information asset owner.
- No user may have access to RESTRICTED information without the express permission of the information asset owner.
- Users who accept custodial responsibilities of RESTRICTED information, regardless of the media or presentation method, must safeguard the use and storage of that information. This includes protecting information from unauthorized viewing or physical access.
- Transmissions of RESTRICTED information over non-NS networks, such as the Internet or other public networks, must be encrypted.

- All users are responsible for the proper disposal and destruction of RESTRICTED information regardless of the media containing the information.
- RESTRICTED printed information must not be placed in ordinary wastebaskets for disposal. This information must be accumulated and shredded. Shredding may be accomplished on a local, departmental, building, or other basis.
- Transmitting any RESTRICTED information via electronic communications outside the company is prohibited. Users having a business need to transmit such information must secure prior approval from NS Information Security.

V. Prohibited Transmissions or Content/Emails

- Users of the Norfolk Southern e-mail systems are strictly prohibited from:
    - Sending electronic chain letters.
    - Sending or intentionally receiving harassing, offensive, or obscene messages or material (such as pictures or cartoons).
    - Concealing or misrepresenting their (or anyone else involved) identities. Users are prohibited from sending anonymous (unsigned) mail or from altering the ID on sent mail (spoofing).
    - Making improper solicitations.
    - Intercepting, accessing, or reading another user's e-mail, subject to the exception of users designated by corporate management to perform monitoring.
    - Using e-mail to disseminate rumors or false or misleading information.
    - Forwarding e-mail without legitimate business purpose.
    - Using profane, abusive, scandalous, or threatening language in e-mail.
    - Bypassing e-mail security mechanisms.
    - Automatically forwarding e-mail to other external systems, unless approval is granted by a security variance.

- All e-mail transmissions or receptions are subject to monitoring by authorized NS users. All persons who access NS information systems must expect no privacy relative to the sending or receiving of electronic communications. All transmissions may be monitored and reviewed by authorized users at any time without notification. However, NS does not regularly monitor the content of electronic communications unless a legitimate business reason requires such an effort.
- Users must conform to all NS corporate policies and procedures in their use of e-mail.
- NS reserves the right to terminate a user's e-mail access at any time, or to deny access to users who do not have a legitimate business need for such.
- Any user posting messages to Internet discussion groups, internet relay chat, electronic bulletin boards, or any other public information system that is not authorized by NS to do so on its behalf must indicate clearly that these comments do not necessarily represent the position of NS.

VI. Software

- All software must be properly licensed. Software provided by NS on a PC is the property of NS, is copyrighted, and must not be copied to another PC or computer.
- NS will provide software necessary to conduct NS business in a productive manner.

- All software purchases must be approved by the Manager of the department or designated departmental group that owns and/or supports the software.
- All software installations must be supervised by a system administrator or a departmental group assigned that function.
- Software not provided by NS and not included on the approved software list is not permissible.
- Users must not use any externally provided software or computer code from an individual or organization other than a known and trusted supplier.
- Information Technology must approve external software for use at NS.
- Only system administrators or their designees may download software from external sites such as web sites, electronic bulletin board systems, external electronic mail systems, external communication networks, or other systems outside NS. Prior to its installation or execution, the software must be scanned with an approved and current virus detection package.
- Only authorized users in the conduct of their job duties may use diagnostic monitoring tools, equipment, hardware, or software, such as line monitors, protocol analyzers, and sniffers. Specific written authorization from NS Information Security must be obtained by any others to use this type of equipment/capabilities and network diagnostic tools.

VII. Internet

- All access to the Internet or other online services must be via an NS Information Security approved communication device and gateway.
- Use of all online services, including the Internet, must be authorized by the department head designee who is a SPOC.
- All Internet services must be configured so as to avoid the enabling or rerouting of undesirable services.
- Users may access only those systems, networks, access devices, and data where explicit authorization has been given or rights have been granted to the general public.
- Responsible incidental personal use is permissible so long as it is not excessive or offensive and does not significantly interfere with productivity or preempt any legitimate business activity.
- Users of online services are strictly prohibited from:
  - Transmitting any RESTRICTED NS information via the Internet without the proper authorization. Users having a business need to transmit such information should discuss secure alternatives with NS Information Security.
  - Accessing, downloading, storing, or printing material that is inappropriate, offensive, or disrespectful to others. No pornographic, obscene, or offensive sites may be accessed at any time nor is it allowable to intentionally attempt to access such sites. Users who discover they have inadvertently connected to a site that contains sexually explicit, racist, or other offensive material must immediately disconnect from that site.
  - Access to streaming video or streaming audio that does not disrupt network services is permissible. Users must comply with Network Services' request to discontinue use when disruption is noted.
- The ability to connect to a site does not imply that users are permitted to visit that site.
- Users must not establish or maintain a web site or web page pertaining to NS that is accessible from outside of NS' computing environment without prior written approval of NS. Changes to web pages within the NSITA environment must be approved by the responsible NS management group.

- NS reserves the right to terminate a user's Internet access at any time, or to deny access to users who do not have a legitimate business need for such.

VIII. Viruses

- If a virus or other unauthorized code is discovered in the NS computing environment, the user should discontinue using the PC, contact the NS Help Desk at (404) 529-1527, and notify his/her supervisor, manager, or departmental SPOC.

  - If the virus-scanning program detects a virus on a PC, the user should discontinue using the PC, contact the NS Help Desk at (404) 529-1527, and notify their departmental SPOC.
  - Externally supplied disks must not be used with any PC unless previously scanned for viruses.

IX. Other

- All NS system users should be aware that their actions might be monitored as deemed necessary to ensure proper operation and security guideline compliance. Users should not expect that their inputs, actions, or other system activities are private.
- Users must not add, change, or delete data or information except in the normal conduct of their job assignment.
- Users must take all necessary action to ensure the accuracy of corporate data.
- All electronic communications processed by the NS computing environment, including back-up copies, are considered to be the property of NS and are not the property of users of the computing environment.
- The NS computing environment's electronic communication capability must be used for authorized NS business only. Responsible incidental personal use is permissible so long as it is not excessive or offensive and does not significantly interfere with productivity or preempt any legitimate business activity.
- Only files necessary to perform NS business should be downloaded.
- Users are not permitted to update and/or change system files, such as the operating system, application code, and other restricted system elements, unless specifically authorized.
- Computer hardware and software is provided by NS for users to fulfill their job responsibilities. This hardware and software is the property of NS.
- NS PCs must be used in a secure environment to protect them and the information contained in them from disclosure, misuse, abuse, or theft.
- PCs must be protected from environmental hazards (such as fire, dust, water, etc.).
- PCs should be physically protected to lessen the risk of theft, destruction, or misuse. Special precautions must be taken with portable equipment such as:
  - Locking away laptops when not in use.
  - Securing laptops in high-traffic areas and at night.
  - Leaving laptops out of view in automobiles and hotel rooms.
  - Keeping laptops in possession while traveling (i.e., airports)

- All network components and test equipment are required to conform to the NS remote access procedure regardless of location, department, or function.

- All access paths must be designed and installed so they cannot circumvent security.
- Users are prohibited from connecting dial modems to any devices that are either directly or indirectly connected to NS' network. While laptop computers are permitted to have dial modems, like any other PC, they are not allowed to be simultaneously connected to an NS network and a non-NS network. The purpose of this rule is to maintain a separation between the outside world and NS networks. Should users have a valid business need to simultaneously use a modem connection and a LAN connection, specific written authorization must be obtained by requesting a variance from NS Information Security.
- No user will install, cause to be operable, or otherwise allow an access path that is not approved by the NS Enterprise Architecture Oversight Committee (EAOC).
- "Back door" access paths are prohibited.
- The display or transmission or intentional receipt of sexually-explicit images, messages, or cartoons, or any transmission that contains ethnic slurs, racial epithets, or anything that might be construed as harassment or disparagement of others based on race, national origin, sex, sexual orientation, age, disability, religious or political beliefs is not permitted.
- The transfer of information between two NS computers or between a non-NS computer and an NS computer is authorized for legitimate business purposes only. However, transferring any RESTRICTED NS information in any format is prohibited without the proper authorization. Users are prohibited from uploading/downloading information to/from external computers unless specifically authorized to do so as part of their job function.
- Users must scan all downloaded files for viruses and malicious code.
- Users must abide by license requirements and copyright restrictions associated with any downloaded files.
  - Users must:
    - Protect the hardware/software/data from unauthorized access and use.
    - Use PCs for authorized activities only.
    - Maintain physical control of the PC and control over access to the data the PC contains.
    - Conform to all software licensing agreements.
    - Report immediately any incident(s) involving the PC to either the immediate supervisor, manager, the departmental authorizing office, NS Information Security, or Internal Audit
    - Access only that data for which he/she is authorized.
  - It is the responsibility of every NS user to immediately report any actual or suspected policy violations, including but not limited to:
    - Individuals removing sensitive NS information without approval.
    - Computer hardware/software being removed from NS' premises without authorization.
    - Individuals gaining access to data, systems, or information that is not needed in the normal performance of their assigned job function. This includes access to inappropriate web sites.
    - Individuals introducing unauthorized or unapproved software into the NS computing environment.
    - The viewing and/or accessing of RESTRICTED information by unauthorized personnel.
    - Providing RESTRICTED information to any person, organization or contractor who is not authorized to receive such information both internal and external to NS.
    - Providing access to NS' property, facilities, electronic or physical files, networks, or computers to any unauthorized person, organization, or contractor.
    - Providing any unauthorized person information that would enhance their ability to access NS' computers or networks. (This information includes, but is not limited to, login names, passwords, access numbers, encryption algorithms, etc.)

- Unauthorized modification of NS' computer files, databases, or hardcopy images.
- Unauthorized removal of information in any form.
- Unauthorized destruction of any electronic files or hardcopy images.