SUBJECT	SECTION – MISCELLANEOUS	NUMBER – 200.80.4	PAGE - 1 of 13
INFORMATION TECHNOLOGY	EFFECTIVE DATE - January 3, 2011	SUPERSEDES ISSUE DATED– June 1, 2006	

POLICY

The Information Technology (IT) resources are the sole and exclusive property of the Company, and are an integral part of the Company's business operations. In order to ensure that these resources are used in a responsible manner, and in the best interest of the Company, all Users (defined below) are required to comply with this policy. Exceptions to the policy may be made by the Chief Information Officer ("CIO") for legitimate business reasons.

IT resources are shared by all Users on a fair and equitable basis. It is the responsibility of the Nabors IT Department not only to provide IT resources to Users, but also to implement safeguards such that the rights of Users are not infringed upon by the use of other Users.

DEFINITIONS

1. IT Resources: Any data or information stored in a digital form, hardware, software and other technologies used to create, store, access or transmit such information, and the computing and/or telecommunication resources or other means (i.e., User Accounts) used to access the information.
2. Computing Resources: All software and hardware related to computers (desktop and laptop computers), computer peripherals (i.e., printers, scanners, etc.), servers, networks, storage devices, databases and applications accessed through the computer or other networked device.
3. Telecommunication Resources: All VOIP phones, Smartphones (PDAs, BlackBerry™, Android, iPhone and other devices), cell/mobile phones, fax machines, voicemail, calling cards, local and long distance phone services, aircards, and any handheld electronic device with the ability to receive and/or transmit voice, text, or data messages without a cable connection.
4. Networks: The Guest Wireless Network, Local Area Networks (LANs), and the Wide Area Network (WAN), sometimes referred to as the Nabors Network.
5. NaborsNet: The Company intranet that provides links to departmental Web pages and other information.
6. Outside Users: All Users who are authorized to connect to a Nabors Network other than permanent employees. This includes temporary and contract employees, visitors, and employees of vendors and customers who access the Nabors Network.
7. Users: Employees and Outside Users who are authorized to connect and log in to access the IT resources on a Nabors Network.
8. User Account: A User Account created to access any of the IT resources.
9. Nabors IT: the IT Department in Nabors Corporate Services and the employees who are in the direct reporting hierarchy under the NCS IT Department.

PROCEDURE

1. User Accounts

A User Account is required to access any of the Company's Computing Resources. Each User Account is identified by a unique account name (User ID). Separate User IDs may be required to access different IT resources.

A. Appropriate Use

User Accounts are provided to eligible Users for access to file storage, printing, electronic mail (e-mail), the internet, the intranet, applications, and activities related to the Company's business. Each account represents an allocation of a valuable IT resource and, as such, is monitored by Nabors IT for appropriate use.

Each User Account is assigned to one authorized User. Sharing of accounts is strictly prohibited.

B. Eligibility

All Nabors employees and Outside Users who have an active employee ID with a valid business reason for an account are eligible upon approval from their Supervisor/Manager. Access to some systems may require additional approvals from the appropriate system owner(s).

C. Obtaining a User Account

Upon hiring, all office-based employees will receive a User Account. This is handled by the employee's HR group when the employee is activated in the system. Employees will be granted access to the H: Drive, Department G: Drive, and an email account. Employees may be given access to certain systems automatically based on their job and department. If an employee requires access to additional systems, a User security access request must be submitted online through the myRequests system to request such access.

To obtain a User Account for an Outside User, a User security access request must be submitted online through the myRequests system. The User security access request must be approved by the Supervisor/Manager before the account is created.

Nabors IT will customize the User computing profile, including access to e-mail, the intranet, network directories, and other Computing Resources, based on the information supplied on the User security access request. Once the account is created, an automated e-mail message containing the login ID, password and e-mail address for the User will be sent to the Supervisor/Manager and the User.

D. Changing the Account Password

Upon logging into the account for the first time, the User is responsible for changing the account password. From that point forward, the system will prompt the User to change the password at various intervals, depending upon the password complexities associated with the User Account.

The User is also responsible for protecting the security of the account by not sharing or exposing the password intentionally or unintentionally.

Users who are locked out of their account or forget their User Account passwords must use the self-service Password Reset application to unlock and reset the password. The Password Reset application can be accessed from the Applications page located on myNabors portal. For User Accounts that are not integrated with MS Windows User Account, the User must call the Nabors IT Customer Service to obtain a new password. The Nabors IT Customer Service personnel will verify the User's identity prior to resetting the password.

E. Deactivation and Deletion of User Accounts

When HR flags a User Account to expire or terminates an employee in the HR system on a given day, the access to that User Account is suspended for 30 days. The information on the H: Drive and the email box assigned to the account will not be deleted. While the account is suspended, the User will not be able access the account and the account will no longer receive emails. If the account remains suspended for 30 days, it will automatically change to "disabled", and the email box and all information on the H: drive will be deleted.

F. Misuse of User Accounts

Activation of a User Account constitutes an agreement that the User understands and will abide by all policies and procedures regarding the use of IT resources.

Misuse of a User Account is strictly prohibited. Examples of misuse include, but are not limited to:

- Storing (e.g., writing) or transferring encrypted or unencrypted password information;
- Writing, transferring, compiling, storing or running programs designed to guess passwords or otherwise gain unauthorized access to User or system accounts;
- Breaking into or using another User's Account, or attempting to impersonate another User;
- Sharing passwords with anyone;
- Not taking necessary steps to protect IT Resources (e.g., not securing your PC when leaving your office)

2. Computing Resources

A. Appropriate Use

Within the Networks, many services depend upon distributed Computing Resources and often upon other network services. These resources include servers, printers, workstations, and the network infrastructure (i.e., hubs, switches, routers, cabling system). To maintain the integrity and reliability of the Computing Resources, all Users must utilize these resources responsibly. Nabors IT reserves the right to terminate any process or break any network connection that it determines is adversely affecting the system or the rights of other Users.

B. Approved Computing Resources

The only Computing Resources that may be utilized in the Nabors environment are those explicitly approved by Nabors IT and purchased by the Company. Users are strictly prohibited from bringing any personal computing resources such as hardware (i.e., personal laptops) or software or removable storage media (e.g., USB drives) into the Nabors environment. Nabors IT will not support any computing resources that do not belong to the Company and has the right to confiscate those that are connected to a Nabors Network and located on Nabors' premises.

C. Unauthorized Installation

Nabors IT is responsible for installing all Computing Resources. With the exception of authorized IT personnel, no User may modify and/or install any Computing Resources. To request the installation of a Computing Resource, a User must submit a request through the myRequests system.

D. Data Storage

The Company does not permit storage of data on local hard drives. All data must be stored on the Network. Local hard drives on individual machines are not backed up and, consequently, data may be lost if a computer crashes. Nabors IT is not responsible for any data loss associated with local, network or removable storage.

E. Network Directories

Several network directories with different access restrictions are provided for document storage. The primary network directories include:

- A home directory associated with each User Account for file storage by the assigned User only. All files stored in the home directory will be automatically deleted upon deletion of a User Account.
- A network directory for each subsidiary, which contains separate folders for each department within the subsidiary. These folders are accessible only by Users within the corresponding department.
- A network directory to which all Users have access for sharing files with Users of different departments and/or subsidiaries. This directory is for temporary file exchange purposes only. All files stored on this directory are subject to deletion without notice, and these files are not backed up.

The storage space on the home directory is limited by an enforced disk quota. Once the disk space limit is reached, the User will no longer be able to save to the disk.

F. File Security

Files stored on the network cannot be password protected due to the fact that password protected files cannot be scanned for viruses. Files that are password protected will be deleted without notice. If additional security is required for a file or folder, a User must submit a request for assistance through the myRequests system.

G. Data Backups and Recovery

Folders and files on the Company network are backed up in accordance with the internal IT System Backup Policy. All backups are kept in a safe off-site location for a period of 35 days.

To request the restoration of a file from a backup tape, submit a request through the myRequests system. The request must contain the following information at a minimum:

- The name of the file(s) that needs to be restored;
- The directory and the folder structure in which the files were located;
- The date (within the 35-day period) from which to restore the file.

The file(s) will be placed in the same directory in a folder named "RESTORED". It is the responsibility of the User to move the file(s) to the appropriate directory and to delete the RESTORED folder.

H. Network Printing Resources

Network printing resources include printers, copiers, scanners and multi-function devices. Nabors IT provides network printing resources throughout Company offices at different locations, such as print/copy rooms, and other central locations. Upon approval by the Supervisor/Manager, some Users may utilize local printing resources.

I. Printing Resource Supplies

It is the responsibility of the individual department in which the printing resource is located to replenish supplies such as paper and toner.

J. Secured Areas

Restricted and secured areas such as the Nabors IT office premises, wiring closets, and IT Data Center are all designated for the exclusive use of IT personnel. All unauthorized personnel are prohibited from being in restricted IT areas and will be asked to leave the premises. Violators must be reported to the CIO.

K. Misuse of Computing Resources

Misuse of Computing Resources is strictly prohibited. Examples of misuse include, but are not limited to:

- Purchasing any non-Nabors IT-approved hardware or software with Company funds;
- Connecting or installing any non-Nabors IT-approved hardware or software into the Nabors environment;
- Installing any Company owned software onto a non-Nabors owned computer;
- Playing electronic games on Company Computing Resources;
- Using User Accounts that are not assigned to you;
- Using Computing Resources for personal monetary gain;
- Removing IT resources from Nabors premises without authorization, with the exception of laptops, Smartphones and cell phones;
- Not returning IT Resources at the end of employment with the Company;

- Copying the Company information into personal storage devices;
- Infringing on licensing and copyrights by copying licensed software and documentation without explicit permission. Copying software to a diskette, or any other media, or to an unauthorized computer is a violation of IT policy and of various state and federal laws and is prohibited by the Company;
- Providing access to your computers using modems or through Internet for anyone other than the authorized Nabors IT support personnel. Under no circumstances are Users with modems and communication software (e.g., ProComm, PC Anywhere, etc.) on their computers allowed to keep their computers in "Receive (Host) Mode";
- Mechanically tape recording, digitally recording, or recording conversations or oral communications with, between, or among other employees or non-employees in any other manner that are in any way related to Company business or operations, whether over the telephone or in person without obtaining authorization in advance from the President of the Company and the business unit as well as receiving approval from the Nabors Law Department;
- Misuse or improper handling of IT Resources (e.g., turning off a PC without shutting down properly);
- Modifying or reconfiguring the software, operating system, or hardware of a computer or network;
- Attempting to use more resources than hardware can handle (i.e., running a large number of I/O or computationally intensive applications or too many applications at the same time);
- Monopolizing shared resources (i.e., excessive printing on network printers, using excessive disk space, sending excessive amounts of e-mail, sending global e-mails without authorization, etc.);
- Running programs that lock the screen or keyboard other than a Nabors IT installed screen-saver;
- Installing or running programs that track key-strokes;
- Copying or loading any executables, games, screen-savers, or audio/video clips onto any network drive. Executables consist of any files with EXE, VBS, COM, DLL, or SYS extensions;
- Writing, uploading, downloading, and/or knowingly proliferating worms or viruses;
- Failing to store Company-related electronic data on the Network;
- Reading, copying, or deleting a file on the Network without permission from the owner;
- Password protecting documents on the Network or PC workstation;

- Attempting to print on any media for which the Network printing resource is not designed to use;
- Any activity that can harm the Network printing resource, print server, or Network;
- Any activity that can deny the service of the Network printing resource to other Users;

3. Electronic Mail (E-mail), the Internet, and the Intranet

A. Appropriate Use

The Nabors Network and all information created, transmitted by, received from, or stored on the Network or any associated resources are the property of the Company, and as such, are to be used for business purposes only. E-mail is covered under the Electronic Communications Privacy Act of 1986. This act provides for prosecution of individuals found secretly capturing, reading, or altering another User's e-mail without permission.

B. Eligibility

All active employees will have access to myNabors portal. Users who have an active network User Account will also have an e-mail account. However, Internet access, with the exception of certain authorized sites, is not automatically granted to each individual with an active User Account.

C. Obtaining Internet Access

To request access to the Internet, a User security access request must be submitted through the myRequests system. The User security access request must include a valid business reason for the User to have Internet access, and must be approved by the User's Supervisor/Manager.

D. Mailbox Quotas

Each e-mail account is restricted by a set storage limit of 75MB. When an e-mail account is getting close to meeting the storage quota, the User will be notified by an automated e-mail message. When the e-mail storage limit is reached, the User will be able to receive e-mail messages, but will no longer be able to send messages. If additional storage is needed, a request can be submitted through the myRequests system.

On a weekly basis, any e-mail message that is older than 183 days since it was received or sent will be automatically deleted.

E. E-mail Message Size Limit

A single e-mail message cannot be greater than 8 MB in size, including attachments. To send a message larger than 8 MB, the User must break the message into smaller, separate messages or compress the attachments using compression software (e.g., WinZip or 7-Zip).

Restrictions also apply to the types of attachments that are allowed to pass through the Company e-mail system. A list of approved attachment types is maintained on the Information Technology site on NaborsNet.

F. Monitoring Content and Usage Patterns

The Company reserves the right to monitor all incoming and outgoing e-mail messages and Internet traffic for content, usage patterns, and/or violations of this policy. All messages created, sent or retrieved through the Company e-mail system are the property of the Company and should be considered public information. The Company also reserves the right to delete emails without notice.

G. Misuse of E-mail and the Internet

The Company strictly prohibits misuse of the e-mail system and the internet. Examples of misuse include, but are not limited to:

- Transmitting, retrieving, or storing any communications of a discriminatory, harassing, sexually explicit, abusive, profane, or offensive nature;
- Creating e-mail messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference;
- Any activity that is illegal, against Company policies, or contrary to the Company's best interest;
- Soliciting non-Company business, or for any purpose intended for personal gain;
- Forwarding Company emails to personal email accounts;
- Using personal email accounts for Company business;
- Transmitting, receiving, or forwarding chain letters or emails;
- Transmitting unauthorized mass mailings;
- Forging communications through e-mail, the internet or other media;
- Blogging, using social networking sites, user groups or forums during work time or through the use of Company provided Computing Resources is strictly prohibited. In addition, all Users are prohibited from mentioning the following in any public groups or forums:
  - The Company in general, either in a positive or negative manner;
  - Company managers, employees or former employees;
  - Company activities, including past, present or future activities;
  - Company information, including sending or uploading such information, including but not limited to pictures and video.

4. Telecommunication Resources

Users with a business need will be assigned appropriate Company-owned telecommunication resources. Nabors IT will select preferred equipment and service providers by evaluating telecommunication vendors based upon quality of service, reliability and cost. The Company retains national contracts with preferred service providers that cover the majority of the

Company's area of operations. The national contract rates enable the Company to obtain volume usage discounts, negotiate the best terms and conditions of service, and consolidate billing. In areas of operation in which the service providers for the national contracts do not provide coverage, service is provided by other vendors that do supply coverage to the area. Nabors IT will conduct periodic reviews of the communication services to ensure suitability and quality of service.

A. Appropriate Use and Privacy

All Company provided telecommunication resources and all information transmitted by, received from, or stored in these resources are the property of the Company, and as such, are to be used for business purposes only. If the Company provided telecommunication resources are equipped with GPS, Company reserves the right to track the location of the resources.

B. Eligibility

All Users who have a valid business reason for needing telecommunication resources are eligible for appropriate Company-provided telecommunication resources upon approval from their Supervisor/Manager. Additional approvals may be required when necessary.

C. Monitoring Content

Company reserves the right to monitor all Company provided telecommunications resources for all incoming and outgoing calls, voicemail, email and text messages, information stored on the Company-provided resources and other telecommunication resources for content that may violate this policy.

Company reserves the right to delete Company-related information on Company-provided or personal telecommunication resources without notice at any time.

D. Requests for Telecommunication Resources

All requests for telecommunication resources should be made through the myRequests system. All requests must include a valid business reason. The approval process for requests is automated through myRequests, which sends the request to the appropriate approver upon creation.

The Company does not support or reimburse Users for the purchase of any Bluetooth enabled headsets and other accessories with the exception of chargers and replacement batteries. Any expense report submitted showing the purchase of a Bluetooth enabled headset or any unauthorized device or accessories will not be processed for payment and will be returned to the manager.

Fax machines are supported by the Office Services Department. All fax machine requests should be made through the myRequests system.

E. Monthly Account Statements

All accounts on the national contract will be processed by Nabors IT and paid by the Accounts Payable department. Users who have a Company cell phone that is not on the Company-wide shared plan may have the cell phone and calling card charges billed to their Company credit card. In such cases, Users are responsible for timely payment of their bills to avoid service disruptions.

F. Personal Phone Number Transfers

Phone numbers issued to Users on Company devices will remain the property of the Company should that User leave the company. Users are not allowed to have their personal numbers ported into Nabors phone accounts. Any number ported into a Nabors account becomes the property of the Company and will not be released.

G. Personal Usage

Users should avoid using Company telecommunication resources for personal reasons during working hours, and such usage should be confined to lunch hours or other breaks. However, urgent calls to/from family members or to make an external appointment, for example, can be made/received as long as they are kept to an absolute minimum. In situations that require special arrangements, Users are required to consult their immediate Supervisor for direction. Personal usage of Company-provided telecommunication resources at other times must be limited and infrequent.

H. Camera Usage

Company provided telecommunication resources may be equipped with built-in camera. The usage of the camera on Company provided telecommunication resources or otherwise is restricted at the work site. Users must seek authorization from their immediate Supervisors for any usage of a camera at the work site.

I. Service Termination

Users in possession of Company telecommunication resources are expected to protect the equipment from loss, damage, or theft. If the device is lost or stolen, Users are required to communicate to the Nabors IT department using the myRequests system with in 24 hours. Nabors IT may suspend the account temporarily and replace the resources accordingly.

Nabors IT will deactivate terminated employees' telecommunications resources immediately upon the employee being terminated in the HR system or upon request by the Supervisor or the HR department. On resignation or termination of employment, or at any time on request, the Users may be asked to produce for return or inspection. Failure to return the Company telecommunication resources may result in payroll deduction for the replacement cost of the resources.

J. Using Telecommunications Resources While Driving

The Company requires all Users to utilize a hands-free device when using a telecommunication resources while operating a motor vehicle. If you have a company cell phone, and you do not have a hands-free headset, you may submit a request using myRequests to receive one. **Employees who use a Company-provided telecommunications resource or a Company-provided vehicle are expressly prohibited to prepare, send or read text or email messages or surf the Internet while operating a motor vehicle.**

K. Unsafe Work Situation

The Company prohibits the use of cell phones or other similar devices while at any work site at which the operation of such device would be a distraction to the User and/or could create an unsafe work environment. Devices must be turned off and secured at such work sites.

L. Public Conversations

Sensitive or confidential business related conversation must be avoided in public places, such as elevators or airport. They should be held in private.

M. Misuse

Misuse of telecommunications resources is strictly prohibited by the Company. Misuse includes, but is not limited to:

- Sharing telecommunication devices;
- Using telecommunication resources to transmit vulgar, profane, insulting or offensive messages;
- Soliciting non-Company related business;
- Downloading or installing applications on the Company provided devices

5. IT Personnel Responsibilities

Nabors IT personnel are held to a higher standard than other Users because they have the capability and responsibility to maintain system integrity. On host systems such as the Microsoft Windows servers, Linux, and all resources located in the Data Center or IT closets, system administrators and other IT personnel possess certain access rights that allow them to read, write or execute any file on the system. All IT personnel are entrusted with the security and privacy of all of the data on the Network. As such, confidentiality will always be maintained.

All IT personnel are required to wear a picture ID provided by the Company during working hours. This ID must be visible to all employees. In addition, IT personnel have the right to ask Users to identify themselves.

A. Privacy and Confidentiality

IT Personnel are required to protect the confidentiality and integrity of all Users' private information and other company-specific information, including system passwords, IP addresses, security configuration and specific hardware/software configuration during and after their employment with the Company.

B. Liability

Every effort is made to safeguard data stored on computers. However, IT systems administrators are not liable for any loss of data or loss of service on the IT network unless it is intentionally deleted by an IT employee.

C. Investigations

IT system administrators are responsible for investigating policy violations and suspected abuse of Computing Resources and information (i.e., files, e-mails, internet access, telecommunications, etc.) on the Network. During such investigations, system administrators may inspect files and emails, and monitor Network traffic. However, IT personnel are not authorized to access individual User Accounts or read files or e-mail messages without prior authorization from the Law Department or the CIO. IT personnel are required to report any policy violation to the CIO or Law Department appropriately.

As a condition of employment, all IT employees must agree to cooperate fully with all of the above and all such investigations. Failure to cooperate, as determined by the Company in its sole discretion, is grounds for discipline up to and including termination of employment.

6. Enforcement

Nabors IT will utilize every means available to detect abuse of IT resources. Abuse includes violating any local, state or federal regulation even though the activity may not be explicitly referred to in this document.

Penalties for abuse include temporary and permanent restriction of Network privileges, employee discipline up to and including employment termination and, in extreme cases, criminal prosecution.

A. Temporary Restriction

Temporary access restrictions are intended to be short-term and usually require the User to contact the appropriate system administrator for reactivation. The investigation of network policy violations may require a number of potentially affected accounts to be temporarily restricted.

Access to a User's Account may be temporarily restricted for a number of reasons, including, but not limited to:

- Maintenance or servicing of the Network;
- Dissemination of information before continued use of an account; or
- Investigation of policy violations or suspected abuse of resources.

B. Permanent Restriction

If it is determined that a User's policy violations are serious enough that continued use of the Network and resources would infringe upon the rights or security of other Users or affect the well-being of the Company, the User's Account may be permanently restricted. The president of the business unit and the CIO and/or Law Department must approve the activation of permanent access restrictions.

C. Prosecution

Users accused of severe abuse may be referred to the Company's President, the Law Department and the CIO for further action, or to the appropriate law enforcement agency.

D. Non-Employees and Recovery of Costs

Non-employees accused of severe abuse will be referred to the Law Department and/or local law enforcement officials. If expenses are incurred during unauthorized use of IT resources, the Company reserves the right to pursue full reimbursement of those costs from the individual.

E. Unauthorized Users

If a User is using an account that is not assigned to them, the User's department head and the CIO will be notified.

7. Reporting Procedures

A. Suspicious Activity and Unauthorized Personnel

Users are required to report any suspicious activity or unauthorized personnel involving IT resources to the Nabors IT Customer Service and/or building security immediately.

B. Hardware or Software Issues

Inoperative or malfunctioning Company network and computing resources should be reported to the Nabors IT Customer Service. Problems associated with a remote login, or accessing the IT network from other offices, should also be reported to the Nabors IT Customer Service.