(Effective 01/01/2000)
(Revised 07/01/2023)

KINDER MORGAN

Information Security User Policy

One of our most important assets is our Company information. This policy is designed to ensure the security and proper use of the Company and its affiliate's information systems resources and services. Therefore, violations of this policy could create serious damage to the Company's business and reputation. This policy may be amended or revised periodically as the need arises.

Monitoring the Environment

We reserve the right to monitor any and all aspects of the computer, network, and telecommunication systems, including your electronic mail and computer usage to ensure compliance with this policy. You should not have an expectation of privacy in anything you create, send or receive on your computer. These systems belong to the Company and are to be used for approved business purposes.

Each time you logon to one of the Kinder Morgan systems the two paragraphs listed below are presented and require you to acknowledge your awareness that your activities may be monitored.

User acknowledges and agrees that Kinder Morgan's Management and its authorized agents reserve the right to monitor any and all aspects of the computer, network, and telecommunications systems, including System Users' electronic mail, voicemail, and Internet usage, for any lawful purpose such as to ensure compliance with KMI's policies, including the Information Security User Policy, and the Harassment Prevention Policy (which may be viewed on KMI's intranet site), without limitation. The computers, computer accounts, and telecommunications systems issued to System Users are to assist them in the performance of their jobs. System Users should not have an expectation of privacy in anything they create, send, or receive on such systems. These systems belong to KMI and are to be used for legitimate business purposes.

User agrees that affirmative acknowledgment means the user understands and consents to terms and conditions described herein. The user has no reasonable expectation of privacy regarding communications or data transiting or stored on the information system the user is preparing to use. At any time and for any lawful purpose, KMI or any authorized agents may monitor, intercept, record, and search any communications or data transiting or stored on this information system. At KMI's sole discretion, KMI may disclose pertinent information to the U.S. Government and its authorized representatives to protect the security of critical infrastructure and key resources, ensure information security, or to comply with any applicable law, regulation, legal process, or enforceable governmental request.

Information Security User Policy

Q&A

Q1: Why does Kinder Morgan monitor its information?

A1: Kinder Morgan monitors its information systems to ensure the proper use of our computer resources and data. The information and the information systems resources are to be used for business purposes and are provided to assist you in the performance of your job. You are responsible for protecting Kinder Morgan information from unauthorized access, disclosure, modification, and destruction.

Q2: What are the Company's information system resources?

A2: Information systems resources and services include, but are not limited to, the following: host computers, file servers, workstations, standalone or networked computers, standalone or networked printers, laptop/notebook computers, smart phones, Blackberries, PDAs, software, and internal or external communications networks (Internet, commercial on-line services, bulletin board systems, and electronic mail systems) that are accessed directly or indirectly from the Company's offices or computing equipment regardless of location.

Q3: Does this policy only apply to Kinder Morgan employees?

A3: No, the Information Security Users Policy applies to all Kinder Morgan employees, consultants, contractors, temporary employees, clients, customers, and other individuals ("System Users") that use one or more of the Kinder Morgan or its affiliate's information systems resources and services.

Q4: Does this policy apply to me if I am working from home on my personal computer?

A4: Yes, this policy applies to all System Users of Kinder Morgan's information systems resources and services, whether on Kinder Morgan property, connected from remote locations via any networked connection, including home personal computers, or using Kinder Morgan equipment in any location.

Q5: Do I put my employment at risk if I violate this policy?

A5: Violations of this policy may result in disciplinary action, including possible termination, and/or legal action.

Information Security User Policy

What is expected?

You are responsible for adhering to all policies, standards and procedures for securing information systems resources and services, including the following:

a) Compliance with all software licenses, copyrights, and all other state, provincial and federal laws governing intellectual property.

b) No fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating, or unlawful material shall be sent or downloaded by any form of electronic means or displayed on or stored in the Company's computers or printed on the Company's printers. If you encounter or receive such material, you should immediately report the incident to your supervisor or the Company's Chief Information Officer (CIO).

c) You may not install software onto company owned individual computers or the network without first receiving express authorization to do so from IT. This includes, but is not limited to, software downloaded from the Internet, shareware, freeware or packaged software. IT personnel will periodically scan for, and remove, unauthorized software.

d) You must not procure hardware devices or software products for connection to or access from the Kinder Morgan network without prior approval from IT.

Included but not limited to:

Any software or subscription services allowing Kinder Morgan users to connect and use over the Internet via the Kinder Morgan network.

Any hardware or software allowing remote connectivity from the Internet to a Kinder Morgan asset (hardware or software) via a method other than the remote connectivity options approved by the Kinder Morgan IT department.

SAAS (Software As A Service)

Vendor provided tools

Computer hardware and or software not purchased by Kinder Morgan brought into the Kinder Morgan offices with the intention of connecting to any Kinder Morgan hardware or network, other than the KMGuest network.

Prohibited hardware includes, but is not limited to, desktops, laptops, tablets, docking stations, monitors, mice, keyboards, thumb drives, smart phones, printers, routers, switches, and networking hubs.

Computer hardware and or software purchased by Kinder Morgan, but purchased outside of the KM IT department.

Any hardware, software, application, or tool used for the purpose of establishing a network connection to or from the Kinder Morgan network and Kinder Morgan assets.

Departments have authority to approve the justification for procurement of hardware and software products, however IT approval is required before purchasing.

e) In order to protect electronically generated information (documents, spreadsheets, presentations, databases, etc.), these files should be saved, if possible, on the network directories. It is your responsibility to backup any data you choose to store on your local hard drive.

f) Kinder Morgan electronically generated information stored on your local hard drive, or accessible to you on a network directory, may allow you to copy the information to portable media (thumb drives, external computer hard drives, CD's, DVD's, etc.) or cloud storage (A model of data storage in which the data is stored on remote servers and accessed from the Internet. The remote servers may not be part of the Kinder Morgan network. When the remote servers are not part of the Kinder Morgan network the data stored on these servers is not subject to the same protections as data that is stored on servers that are part of the Kinder Morgan network.). Your ability to copy Kinder Morgan information to portable media or cloud storage from your local hard drive, or from a network directory accessible to you, does not imply a right to copy the information unless specifically authorized by the owners of the information. Regardless of the storage location (Kinder Morgan network directory, your local hard drive, portable media, or cloud storage), Kinder Morgan information must be secured from unauthorized access, disclosure, modification and destruction.

g) Portable media and cloud storage allows Kinder Morgan information to become easily transportable and taken outside of the protections that are part of the Kinder Morgan network. You should understand that once information is taken outside the Company, it is no longer under Kinder Morgan control. The Company routinely executes agreements with other companies to safeguard the confidentiality of their information in exchange for sharing this information with the Company. This means that you must take special care to ensure there is no inadvertent external communication of either the Company’s proprietary information or confidential information from a third party to which the Company has obligations of confidentiality.

h) Portable media or cloud storage should only be used as storage for Kinder Morgan information for valid business reasons and not for convenience. You are responsible for maintaining your electronically generated information, regardless of where it is stored (Kinder Morgan network directory, your local hard drive, portable media, or cloud storage) in compliance with the Corporate Records Management Policy.

i) The Company provides a standard set of software tools for desktop computing needs. These tools include (but are not limited to) Microsoft Office (Word, Excel and PowerPoint) and Outlook. In the course of day-to-day work efforts, you may use these tools to develop “applets” (an applet is a small or narrowly-focused application, as compared to a full-scale business application) that streamline workflow and enhance their productivity. It is your (and your direct management’s) responsibility to ensure these applets perform accurately (calculations, function, and format), that they are sufficiently documented, and that other users of the applet are trained in its proper use.

j) At locations where IT personnel are available, you are not to move computers or computer-related equipment. IT personnel should move equipment at these locations. Your cooperation will protect you, and your equipment, from damage, while also allowing IT to maintain an up-to-date inventory. When an equipment move is needed, IT should be notified in advance. Identifying the equipment and completion date will allow IT personnel to schedule the move.

k) Your ability to connect to other computer systems through the network does not imply a right to connect (and use) those systems unless specifically authorized by the owners of those systems.

l) Data owners will be responsible for security authorization at the application or data level. Data owners may be the process owner or someone designated by the process owner to be responsible for the data. For example, access to the General Ledger is approved by the G/L Owner in Finance and Accounting.

m) Generative artificial intelligence (AI) tools like ChatGPT, Google Bard, Bing Chat, GitHub CoPilot, Dall-E, Midjourney, and ModelScope are capable of answering questions, and generating texts, images and source code. AI tools can be useful, but they present risk for the company if not used responsibly and appropriately. AI tools retain user data that is submitted during use and may use data submitted by one party to generate responses to other third party queries. Accordingly, when using AI tools you must not provide to the tool any Kinder Morgan, or any customer or third party, proprietary or confidential information to which you may have access. Data privacy laws may also restrict the submission of personal information of employees, contractors, vendors, customers or other users of Company systems to AI tools. Information generated by AI tools may not be correct or accurate. If you are using AI tools to generate text, data or images that will be used in the course of your employment, you must verify that the AI generated information is accurate and correct and inform your supervisor that the work product is generated or assisted by AI. The Kinder Morgan Code of Business Conduct and Ethics (the "Code") applies to all aspects of the work you do for the company including any use of AI tools. You may not use AI tools to engage in any conduct that is unlawful or inconsistent with the Code or Kinder Morgan values. If you have any questions regarding the use of any AI tool, please send an email to ai@kindermorgan.com.

Q&A

Q1: Why is software compliance important?

A1: Kinder Morgan enters into legally binding agreements concerning the proper use of computer software. Using computer software in a manner that violates the software use agreement may put Kinder Morgan at risk for financial penalties and fines.

Q2: Is contacting IT prior to installing software on my Kinder Morgan computer really necessary?

A2: Yes, it is necessary to contact the IT department prior to any software installation so that all licensing concerns can be addressed and to ensure that the software complies with the controls established to meet data integrity, security, regulatory compliance, standardization, and adherence to the Company's Sarbanes Oxley Act of 2002 computer systems controls.

Q3: How do I get assistance when I need help from IT?

A3: The Kinder Morgan Help Desk can be reached at 713-420-3375 or 877-563-3375 (US) or 403-514-6600 (Canada). You can also get assistance from the Help Desk WEB page at http://kmonline/itkb/SitePages/Home.aspx for assistance.

Electronic Mail (Email)

Each employee and contractor who has access to the use of the Company's electronic mail systems must use these systems with professionalism in mind. Electronic mail should only be used for the purpose of conducting Company's and

Company's-related business, and should not be used to send personal announcements, messages, or jokes of any kind. Sending potentially hostile or offensive material containing content relating to race, color, religion, sex, sexual orientation, gender identity, national origin, age, physical or mental disability, status as a veteran, or citizenship of individuals legally authorized to work in the United States or Canada is strictly prohibited.

The electronic mail system may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-Company sponsored activities.

Confidential information, information about confidential meetings, interpretation of contracts, opinions of the Company's obligations to any third party, or the Company's rights against any third party should not be communicated by electronic mail, however, if this type of information must be communicated by electronic mail, then the electronic mail needs to comply with the following: (i) it must be clearly marked "confidential" and may require the marking "privileged information" if it is a legal matter being discussed, (ii) it may require a legal email disclaimer at the bottom if there are legal issues being discussed, and (iii) it must be sent to a restricted distribution list made up of only the people that need to know and are actively assessing or contributing to the confidential subject matter being discussed or assessed.

Never write anything in electronic mail that you would be embarrassed to see introduced in public. Confidential information or confidential faxes should never be transmitted via the internet, unless encrypted.

Electronic mail correspondence is the property of the Company, and, as such, is not private correspondence. It may be inspected at any time with or without your knowledge. You should be aware that information in electronic mail systems, on-line and on backup tapes is a business record and therefore can be subpoenaed by a court of law. You should consider these electronic mail communications to be formal business documents and the same level of care should be taken in creating such communication as would be taken with formal written communication.

Electronic mail messages older than 45 days are regularly purged from the Company's servers. You are responsible for reviewing and purging your electronic mail messages stored in Personal Archive Folders as defined in the HR Policy Manual, listed on the Records and Information Governance webpage found here: http://kmonline/procurement/records_mgmt/Pages/Policies%20and%20Procedures.aspx

Information Security User Policy

You should understand that once information is electronically transmitted outside the Company, it is no longer under our control, because the recipient can resend it to anyone. Additionally, inasmuch as electronic mail should not be considered a secure method of data transmission, discretion should be used when sending confidential information through the electronic mail system. Moreover, the Company routinely executes agreements with other companies to safeguard the confidentiality of their information in exchange for sharing this information with the Company. This means that you must take special care to ensure there is no inadvertent external electronic communication of either the Company's proprietary information or confidential information from a third party to which the Company has obligations of confidentiality.

File attachments via electronic mail communications can potentially contain dangerous computer viruses. A common practice is to use phishing emails (Phishing emails try to obtain sensitive data such as financial information, passwords, ID's, deploy malware, or redirect the email recipient to a malicious false WEB site that appears to replicate a legitimate WEB site, by using an email that **appears** to be from a legitimate organization.) to deliver computer viruses and steal confidential information.

Each person receiving files will be held individually accountable for observing appropriate measures to ensure the safety of such files prior to their introduction into the Company's computer systems.

Dictionary.com defines phishing as

"to try to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one."

(http://dictionary.reference.com/browse/phishing).

Please stop and think before you click:

- Consider the following before clicking on any email.

  - Do you know the sender of the email?

  - Did you expect to receive this email?

  - Does the content of the email seem like it is intended for you?

  - If it sounds too good to be true, it is probably false.

The following Company approved electronic mail disclaimer is provided:

This e-mail is the property of Kinder Morgan, Inc. and/or its affiliates and may contain confidential and privileged material for the sole use of the intended recipient(s). Any review, use, distribution or disclosure by others is strictly prohibited. Kinder Morgan Inc. and its affiliates assume no responsibility to persons other than the intended recipient(s), and do not accept liability for any errors or omissions which arise as a result of e-mail transmission. If you are not *the intended recipient, please contact the sender immediately and delete all copies of the message including removal from your hard drive. Thank you.*

Q&A

Q1: Has Kinder Morgan been required to provide email data during litigation?

A1: Yes, we have been required to provide emails that are related to specific cases. You must be careful of the contents of any email created because emails are subject to discovery.

Using the Internet

The Company has software and systems in place that can monitor, record, and restrict Internet usage and non-business related Internet sites. You should be aware that the computer monitoring systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, newsgroup and electronic mail message which moves in and out of the Company's internal networks and the Company reserves the right to do so at any time. You should not expect use of Company computers to be private as to Internet usage. Company management may review Internet activity and analyze usage patterns, and they may choose to publicize this data to assure that the Company's Internet resources are devoted to maintaining the highest levels of productivity.

The information gathered will only be retrieved and scrutinized by approved IT, HR, Legal and executive personnel on an as needed basis.

Q&A

Q1: Why can't I access social media Internet sites from my Kinder Morgan computer?

A1: The Kinder Morgan Internet circuits are provided for legitimate company business use. Increasing the size of the Internet circuits to accommodate the viewing of social media sites, and other blocked sites, would require an additional expense and expose the Kinder Morgan IT systems to malware that is often present on these WEB sites.

Using the Network

To protect IT networked services, you must not establish any internal/external network connections (i.e. electronic bulletin boards, local area networks, wireless networks, File Transfer Protocol servers, web servers, remote connections to existing networks) that could permit third party users to gain access to Kinder Morgan's IT network, without prior approval of IT management.

You must not bring your own computers, computer peripherals, or computer software into Kinder Morgan facilities without prior authorization from IT management. For third parties, personal hardware and software may be used on Kinder Morgan premises during the course of their engagements provided the equipment is not connected to the IT network.

Q&A

Q1: Why can't I use my home computer at work?

A1: The Kinder Morgan IT department ensures Kinder Morgan computers have software installed to protect against computer virus infection and to provide up to date security patching. The patching status and general health of a home computer presents a risk to the Kinder Morgan network and all attached systems.

Radio Licensing

Most business class 2-way radios and many other wireless devices require an FCC license to legally operate. The license can take many different forms. Devices that likely require licenses are as follows:

- Land based hand-held and vehicle mounted 2-way radios.
- Land based marine radios, including hand-held or permanently mounted radios, used to communicate with water borne vessels.
- Radios used aboard a water borne vessel—generally covered by a license for the vessel or a fleet of which the vessel is a member.
- Wireless remote control devices. These are devices to remotely control overhead cranes, ship loaders, conveyors and other large moving machinery.
- Wireless Call Boxes. Call boxes are typically used at access gates to enable a visitor to contact Kinder Morgan personnel so that the gate can be opened.
- Wireless siren control devices. These are used to remotely activate warning or emergency sirens.

Information Security User Policy

The Telecom Group will obtain, manage, renew and cancel FCC licenses as required. The FCC Team within Telecom can be contacted via email at FCC_Regulatory@kindermorgan.com or by telephone at 866-775-5785. The team is available to answer licensing related questions and to aid in determining if certain radios require a license. Do not order licensing from or allow your 2-way radio dealer to obtain FCC licenses.

The Business Unit shall coordinate with the FCC Team to ensure that all radio facilities currently operating, as well as future installations, are compliant with FCC licensing requirements. A person thoroughly familiar with all radio usage at a given facility shall be designated as the interface with the FCC Team.

As part of purchasing or selling Kinder Morgan assets that utilize any FCC licensed radio equipment, the FCC Team should be notified and will manage the process of either transferring, renewing or cancelling licenses.

Land mobile radios used by Kinder Morgan entities to communicate with 3rd parties, including customers, generally are required to be covered by a **written** agreement with the Licensee when operated on a non-profit basis. Land mobile radios used by 3rd parties to communicate with radios operated under a Kinder Morgan held license are also required to be covered by a written agreement when operated on a non-profit basis. This is an FCC rule described in title 47 C.F.R. §90.179. The agreement serves as FCC authorization to operate the radios. With no agreement, there is no authorization.

Kinder Morgan complies with FCC licensing rules and takes its obligations under these regulations very seriously. An employee’s failure to comply with these requirements can result in discipline up to and including termination.

Laptops

The portability of laptop computers makes them particularly vulnerable to theft, either for resale (opportunistic thieves) or for the information they contain (industrial spies).

The impact of a laptop theft includes not just the replacement value of the hardware but also the value of any Kinder Morgan data contained on the laptop. Information is a vital Kinder Morgan asset. The impact of unauthorized access to important and/or sensitive Kinder Morgan data can far outweigh the cost of the equipment itself.

To reduce the likelihood of your laptop computer being stolen you must take the following security measures.

- Keep your laptop in your possession and within sight whenever possible, just as if it were your wallet, handbag or mobile phone. Be extra careful in public places such as airports or restaurants. It takes a thief just a fraction of a second to steal an unattended laptop.

- Laptop computers should be secured in a locked cabinet at the end of the day's business.
- Never leave a laptop visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk, but it is generally much safer to take the laptop with you.
- Remember that people who steal laptops are looking for an opportunity when no one is watching and know the most likely places to find unattended laptops.

The loss of Kinder Morgan property and information, even in small amounts, presents a significant problem over time. Following sound security measures is important in reducing the theft attractiveness of the property while increasing the potential for detection of criminal activities in our workplace. Everyone is encouraged to remain aware and vigilant and report suspicious activities immediately.

Q&A

Q1: How frequently are Kinder Morgan laptops stolen?

A1: Unfortunately several laptops are stolen on an annual basis. Of those stolen, many were left unattended in a Kinder Morgan vehicle. In addition to the cost of the laptop replacement, the Kinder Morgan vehicle often suffers damage from the break-in and must also be repaired.

Computer Hardware Disposal

The disposal of all laptop, desktop, and server computers should be coordinated through the IT department. These devices have computer hard drives installed that contain Kinder Morgan data.

Other equipment such as printers and copiers may have computer hard drives installed that contain Kinder Morgan data. In addition portable media (thumb drives, external computer hard drives, CD’s, DVD’s, etc.) may also contain Kinder Morgan data.

Prior to any equipment (described above in the section) leaving Kinder Morgan control Kinder Morgan data on the computer hard drive (or other fixed or portable media capable of storing electronic data) should be removed.

Computer hardware and peripherals should be picked up by a reputable environmentally certified recycling company in compliance with all local, state, and federal laws. All fees charged for the removal of the equipment will be charged to the department, whom initially purchased the equipment.

Removal of Kinder Morgan data from hard drives contained within leased equipment should be coordinated with the leasing company.

The IT Security department is available to assist Kinder Morgan departments with selecting the appropriate method for data removal. The IT Security department can be contacted at ITSecurity@kindermorgan.com.

Q&A

Q1: How do I remove the data on a hard drive and whom should I contact for computer hardware pickup?

A1: For assistance with removing data on a hard drive and computer hardware pickup, contact the Kinder Morgan Help Desk at 713-420-3375 or 877-563-3375 (US) or 403-514-6600 (Canada). You can also get assistance from the Help Desk WEB page at http://kmonline/itkb/SitePages/Home.aspx for assistance.

Passwords and User ID's

You are responsible for safeguarding your passwords for each system. Individual passwords should not be printed, stored on-line, or given to others. You are responsible for all transactions made using their passwords. To enhance system security, passwords must be at least eight characters.

The following User ID and password rules are established to provide consistency among systems.

User ID Rules:

1. First 4 characters of the last name if available.
2. First 3 characters of the first name (not nickname) to create a maximum total of 7 characters from last name and first name.
3. One numeric that is a 1 for the first person with that first and last name and a 2 for the second person with the same first and last name and so forth. If there are more than 9 with the same login, an alpha character will be used.

Examples:
smitjoh1 - Smith, John, Employee, 1

Strong Password Rules:

Passwords must be at least 8 alphanumeric characters

- Strong passwords **should** contain characters from each of the following four groups and **must** contain characters from at least three of the following four groups:

  - Letters (A, B, C) (Upper Case)
  - Letters (a, b, c) (Lower Case)
  - Numerals (0, 1, 2)
  - Symbols (~, !, @)

- Strong passwords should include at least one symbol character in the second through sixth positions.
- Strong passwords must be significantly different from prior passwords.
- Strong passwords must not contain your name or user name.
- Strong passwords must not be a common word or name.

Passwords must change every 60 days

Suggestions for Passwords:

What makes a strong password
To an attacker, a strong password should appear to be a random string of characters. The following criteria can strengthen your passwords:

Make it lengthy. Each character that you add to your password increases the protection that it provides many times over. Your passwords should be 8 or more characters in length; 14 characters or longer is ideal.

Combine letters, numbers, and symbols. The greater variety of characters that you have in your password, the harder it is to guess. Other important specifics include:

- **The fewer types of characters in your password, the longer it must be.** A 15-character password composed only of random letters and numbers is about 33,000 times stronger than an 8-character password composed of characters from the entire keyboard. If you cannot create a password that contains symbols, you need to make it considerably longer to get the same degree of protection. An ideal password combines both length and different types of symbols.

- **Use the entire keyboard,** not just the most common characters. Symbols typed by holding down the "Shift" key and typing a number are very common in passwords. Your password will be much stronger if you choose from all the symbols on the keyboard, including punctuation marks not on the upper row of the keyboard, and any symbols unique to your language.

Use words and phrases that are easy for you to remember, but difficult for others to guess.

Create a strong, memorable password in 5 steps

Use these steps to develop a strong password:

1. **Think of a sentence that you can remember.** This will be the basis of your strong password or pass phrase. Use a memorable sentence, such as “My son Aiden is three years old.”
2. **Check if the computer or online system supports the pass phrase directly.** If you can use a pass phrase (with spaces between characters) on your computer or online system, do so.
3. **If the computer or online system does not support pass phrases, convert it to a password.** Take the first letter of each word of the sentence that you’ve created to create a new, nonsensical word. Using the example above, you’d get “msaityo”.
4. **Add complexity** by mixing uppercase and lowercase letters and numbers. It is valuable to use some letter swapping or misspellings as well. For instance, in the pass phrase above, consider misspelling Aiden's name, or substituting the word "three" for the number 3. There are many possible substitutions, and the longer the sentence, the more complex your password can be. Your pass phrase might become "My SoN Ayd3N is 3 yeeRs old." If the computer or online system will not support a pass phrase, use the same technique on the shorter password. This might yield a password like "MsAy3yo".
5. **Finally, substitute some special characters.** You can use symbols that look like letters, combine words (remove spaces) and other ways to make the password more complex. Using these tricks, we create a pass phrase of "MySoN 8N i$ 3 yeeR$ old" or a password (using the first letter of each word) "M$8ni3y0".

Password strategies to avoid

Some common methods used to create passwords are easy to guess by criminals. To avoid weak, easy-to-guess passwords:

- **Avoid sequences or repeated characters.** “12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not help make secure passwords.
- **Avoid using only look-alike substitutions of numbers or symbols.** Criminals and other malicious users who know enough to try and crack your password will not be fooled by common look-alike replacements, such as to replace an ‘I’ with a ‘1’ or an ‘a’ with ‘@’ as in “M1cr0$0ft” or “P@ssw0rd”. But these substitutions can be effective when combined with other

measures, such as length, misspellings, or variations in case, to improve the strength of your password.

- **Avoid your login name.** Any part of your name, birthday, social security number, or similar information for your loved ones constitutes a bad password choice. This is one of the first things criminals will try.
- **Avoid dictionary words in any language.** Criminals use sophisticated tools that can rapidly guess passwords that are based on words in multiple dictionaries, including words spelled backwards, common misspellings, and substitutions. This includes all sorts of profanity and any word you would not say in front of your children.
- **Use more than one password everywhere.** If any one of the computers or online systems using this password is compromised, all of your other information protected by that password should be considered compromised as well. It is critical to use different passwords for different systems.
- **Avoid using online storage.** If malicious users find these passwords stored online or on a networked computer, they have access to all your information.

Although not recommended, if you must write your password down, lock it up in a safe place. Do not write down a password and stick it on your monitor, leave it on your desk or write it in your appointment or address book.

Keep your passwords secret

Do not share your password. If you believe your password has been compromised, change it.

Treat your passwords and pass phrases with as much care as the information that they protect.

- **Don’t reveal them to others.** Keep your passwords hidden from friends or family members (especially children) who could pass them on to other less trustworthy individuals.
- **Protect any recorded passwords.** Be careful where you store the passwords that you record or write down. Do not leave these records of your passwords anywhere that you would not leave the information that they protect.
- **Never provide your password over e-mail or based on an e-mail request.** Any e-mail that requests your password or requests that you to go to a Web site to verify your password is almost certainly a fraud. This includes requests from a trusted company or individual. E-mail can be intercepted in transit, and e-mail that requests information might not be from the sender it claims. Internet "phishing" scams use fraudulent e-mail messages to entice you into revealing your user names and passwords, steal your identity, and more.
- **Change your passwords regularly.**

Information Security User Policy

Q&A

Q1: **The Password section of this policy contains a lot of information. Who should I contact if I have additional questions?**

A1: The Kinder Morgan Help Desk can be reached at 713-420-3375 or 877-563-3375 (US) or 403-514-6600 (Canada). You may also use the Help Desk WEB page http://kmonline/itkb/SitePages/Home.aspx for assistance.